Securing Technologies of Freedom after the Arab Spring:
Policy Entrepreneurship and Norms Consolidation Practices in Internet Freedom Promotion

Muzammil M. Hussain

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

University of Washington

2014

Reading Committee:

Philip N. Howard, Chair

W. Lance Bennett

Kirsten A. Foot

Patricia Moy

Program Authorized to Offer Degree:

Department of Communication

University of Washington

Abstract

Securing Technologies of Freedom after the Arab Spring:
Policy Entrepreneurship and Norms Consolidation Practices in Internet Freedom Promotion

Muzammil M. Hussain

Chair of the Supervisory Committee:
Professor Philip N. Howard
Department of Communication

This dissertation is an investigation of the aftermath of the Arab Spring protests of 2011-2012 and their consequences for impacting contemporary discussions and efforts to promote "internet freedom" by Western democratic states. This study focuses on the key stakeholder communities that have emerged to compete, define, and consolidate the norms and frameworks surrounding internet freedom promotion: *state-based*, *private sector*, and *civil society* actors. This dissertation also describes the rise and failed attempt of civil society stakeholders to infuse democratically-oriented frames for approaching digital infrastructure management with the primary interests of protecting citizen rights and political activists in autocratic states. The political economy of global digital infrastructure regulation is also examined, and the positions of state-based and private sector influences within it are articulated. In doing so, this study identifies a key tech-savvy community of practice that has delineated the most comprehensive opportunities and pitfalls of using digital media tools for democracy promotion, and is struggling to consolidate and enact these practices and norms into policy frameworks. However, these efforts are cast against the competing interests of the technology providers in colluding with repressive and democratic state powers to provide functionally equivalent anti-democratic technocratic capabilities. Thus, this story is parts network analysis, part policy analysis, and part event analysis. Throughout, the proto-regime formation approach to technology policy is emphasized in contrast to existing state-sponsored telecommunications regulatory bodies.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

FOC: Freedom Online Coalition

GNI: Global Network Initiative

ICANN: Internet Corporation for Assigned Names and Numbers

IETF: Internet Engineering Task Force

IGF: Internet Governance Forum

ISOC: Internet Society

ITU: UN's International Telecommunication Union

NSA: US's National Security Agency

NSF: US's National Science Foundation

UN: United Nations

WSIS: ITU's World Summit on the Information Society

ACKNOWLEDGEMENTS & DEDICATION

I would like first of all to express my heartfelt thanks and appreciation to Professor Phil Howard, whose endless patience, support, commitment and open-mindedness have been a constant source of inspiration for me throughout my years of graduate study at the University of Washington. I have also benefitted much from Professor Doug McLeod, at the University of Wisconsin, who first enrolled me into the curious world of praxis-based learning and discovery. I have little faith that those two sentences will convey my sentiments in full—so I offer them my most sincere gratitude and an intention of paying it forward.

I also wish to thank my hard-working committee: Professors Patricia Moy, Kirsten Foot, and Lance Bennett. Throughout my program, Dr. Moy consistently set high standards for me and pushed me to develop the quality of my ideas alongside my skills in demonstrating them effectively. The seeds of this particular project were planted early on while I was enrolled in Dr. Foot's cutting-edge methods course, and I am also grateful for her exposing me to new theoretical pastures since. Dr. Bennett's sharp guidance has been hugely beneficial for this project and my overall development; I am particularly grateful for my time spent at the CCCE pursuing parallel projects with a bright community of researchers.

For better perspective, this project has actually been a small part of a much larger unlikely (and at times uncertain) journey through three fine public institutions: the University of Washington, the University of Wisconsin, and the Strongsville High School. During this trek, my friends from graduate studies—Jason, Eike, and Shawn—extended their honest friendships and good company in this labor we love, something I have considered sacred. My friends from the MSA shaped me in more ways than they know, and their most valuable gift has been their community. But at Strongsville, David and Linda Lackey deserve special mention for being first to blur the boundaries between the honest joy of learning and the beneficial task of friendship. They also deserve blame for my incurable bouts of marginalia.

Along every step of this project, all that has come before it, and is presently blossoming today, my family has been my most selfless source of support, inspiration, and motivation. I have dedicated this project to them as a small token of my appreciation, and I thank The Guide, The Friend, The One for these gifts.

Mohamed Muzammil Hussain
Ann Arbor, Michigan, USA

Chapter 1 – Internet Freedom Promotion after the Arab Spring

This dissertation is the first in-depth study of the transnational networks of *technology-savvy activists*, *communications corporations*, and *foreign ministries* behind the Arab Spring and several ensuing democratization movements currently in play in global politics. Since the Arab Spring of 2011, these stakeholders have been publicly and transnationally engaged in the challenging work of synthesizing policy norms to better monitor, promote, and regulate the political uses and consequences of information and communication technologies (ICTs) in, but not limited to, nondemocratic countries. In this investigation, I examine the emergence and activities of several competing technology policy arenas, debates, and stakeholders sponsored primarily by Western democratic regimes since the aftermath of the Arab Springs protests of 2011-2012. To couch these phenomena conceptually, I ground them under the rubric of "proto-regimes" in formation, where the involved stakeholders are engaged in introducing competing norms and goals and are struggling to synthesize them under a coherent system (Young 1989). The task of this investigation is to examine this regime construction process, and the new communities of practice that are informing its ideological origins and strategic frameworks.

To do so, I investigate the ongoing efforts and social construction of new policy norms and frameworks by multistakeholder communities of actors that have agitated since the Arab Spring protests of 2010-2011. These actors have competing intersections, understandings, and practices but have converged in intending to govern the political attributes and capabilities of the digital infrastructure undergirding recent episodes of digitally enabled social change. To study these transnational multi-stakeholder actors I conduct a transnational and multi-method "network ethnography" (Howard 2002) by combining primary *archival*, *interview*, and *network* data from connected arenas of exclusive meetings, background debates, and public negotiations that were sparked and organized as a response to the lessons and mishaps observed during the Arab Spring protests and revolutions. In doing so, this study also identifies and traces a small Silicon Valley-based community of policy entrepreneurs—those who "from outside the formal positions of government, introduce, translate, and help implement new ideas into public practice" (Roberts and King 1991). They include technologists and activists who have since 2008 worked diligently to articulate many of the new norms, vocabularies, and frameworks now being referenced by

officials, activists, and journalists, internationally. These experts have been instrumental in driving the surrounding ideas and discussions about promoting "internet freedom" and are increasingly important in setting the agenda for what constitutes meaningful and effective policies for securing digital infrastructures in the public's interests.

In the aftermath of the 2011 cascades of revolts and uprisings, this band of technology-savvy *civil society activists* originating from Silicon Valley (but based transnationally) have become more vocal and confident in propagating their ideological commitments towards governing technologies to promote both human and democratic rights. Furthermore, in doing so, these technology activists have also realized their limitations in facing authoritarian state powers' impunity in overtaking digital infrastructure. Therefore, these technology activists have also helped lobby support from advanced Western democracies to produce alternative communications policy regimes – a domain of policy entrepreneurship they refer to as promoting internet freedom. The ushering of this new normative policy agenda has come about through the active brokering of *advanced Western democracies* to involve the *private technology corporations* that ultimately produce the digital infrastructures used by citizens worldwide.

Given the complexities of the transnational political setting and challenges these diverse stakeholders (activists, corporations, and governments) are addressing, their efforts have been both foundational and lacking. Their policy efforts have been foundational because the period of activities observed in this study (January 2012 to December 2012) contains the first major collective effort by which a coalition of primarily Western nation states has publicly formed a consensus to protect internet freedom globally. In doing so, the broader elements comprising internet infrastructure have been acknowledged as sites for the contentious exercise of authoritarian state power, as well as important public goods for democracy promoters to secure in the public's interest. This is why it is necessary to trace the rise of this emergent policy regime, not by assuming that it is either effective or coherent, but rather because it is intending to impact fundamental aspects of the modern global communication system under the auspices of promoting democratic and human rights.

1.1 How Consequential are Digital Technologies for Political Communication?

The coalition[1] of Western nation states referenced previously broadly represents advanced-industrialized democracies, and is supported most substantively (i.e., both politically and materially) by the United States Department of State. Although the United States is the most influential sponsor, ideological and material commitment towards promoting internet freedom has also been provided by The Netherlands Ministry of Foreign Affairs, the Swedish Ministry for Foreign Affairs, and the Foreign and Commonwealth Office of the United Kingdom, to name three key state backers. The network of Western democratic states working on the promotion of internet freedom was formally launched soon after major Arab Spring protests subsided, in December 2011, at The Hague by Dutch foreign minister Uri Rosenthal. The coalition, titled the "Freedom Online Coalition" (hitherto referred to as the FOC[2]), was a clear response to the Arab Spring protests that began in December 2010. For example, during the December 2011 launch of the FOC in The Hague, then- Secretary of State Hillary Clinton offered the coalition its opening keynote remarks[3] and acknowledged Foreign Ministers Rosenthal (The Netherlands) and Carl Bildt (Sweden), corporate representative Eric Schmidt (Google), and civil society NGO leader Leon Willems (Free Press Unlimited) as "coconspirators" of the FOC—acknowledging the intimate involvement of state, private sector, and civil society stakeholders during its early moments.

In addition to the coalition of twenty-one member states, the United States has been this coalition's most prominent sponsor. In coordination, the United States, since 2008, has similarly invested more than 100 million USD to promote internet freedom-related research, development, and intervention projects. In sponsoring dialogues and negotiations to bring together disparate digital infrastructure stakeholders, the United States and the FOC provide material support to

---

[1] State-based coalitions are often referred to as international treaty or policy regimes; but this coalition is not a formal "international regime." Rather, a core component of this investigation is to unpack the political economy of this coalition, help make explicit its implicit norms, and evaluate its operational utility in achieving its normative goals.

[2] The "Freedom Online Coalition" (FOC) is formally endorsed by the governments of: Austria, Canada, Costa Rica, Czech Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Kenya, Latvia, the Republic of Maldives, Mexico, Mongolia, The Netherlands, Sweden, Tunisia, the United Kingdom, and the United States.

[3] Full-text available here: http://www.humanrights.gov/2011/12/09/secretary-clinton-on-internet-freedom-transcript/

global internet users and activists under threat for exercising their fundamental human rights through new and cutting-edge technologies. According to the informational materials published and propagated by the FOC, this is primarily done with the help of funding programs from member states exceeding 2.5 million euros. The FOC, then, is a key example illustrating the infusion of activist, state, and corporate interests in the ambiguous domain of internet freedom promotion work involving several types of stakeholders.

But there are also reasons why the FOC is neither the central case or site of study for investigating all the important norms and actors involved in internet freedom promotion—particularly with regards to the emerging proto-regime in question. We should be careful here to not conflate the FOC as *the* internet freedom proto-regime. There are at least three reasons why. First, in order to investigate internet freedom promotion efforts, focusing solely on the activities of the FOC is not an ideal or conceptually valid strategy. This is because the diverse stakeholders working in the internet freedom arena(s) often disagree and often misunderstand each other—consensus is not a core characteristic of internet freedom work; consensus formation is actually this issue-area's core problem and challenge. Second, the transnational context of the investigative phenomena (i.e., internet freedom promotion) necessitates that we triangulate and corroborate its distinct understandings being provided by the involved stakeholders coming from multiple sectors and contexts. For example, proponents of internet freedom work are situated within governmental agencies, communication corporations, transnational civil society organizations, as well as loose-networks of political-minded technologists who tinker with and manipulate digital tools and infrastructure (for an activist's perspective, see MacKinnon 2013). Third, because internet freedom promotion fits under the broader category of regulating or governing the global internet infrastructure and all its surrounding and undergirding elements (i.e., what I refer to as *digital infrastructures* – see section 1.3 for a defining discussion), we must also recognize the influence of preexisting regulatory agencies and regimes that have existed long before the Arab Spring of 2011 and how discussions about internet freedom have both increased in maturity and incoherence. Indeed, a large body of scholarship already exists within the corpuses of telecommunications policy and internet governance. This tradition has developed a vast knowledge base about the influential bodies and policy coalitions including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Internet Governance Forum (IGF), the Internet Society (ISOC), and the UN's

International Telecommunication Union (ITU), to name a few. Moreover, given the heavily politicized and commercialized stakeholders and the lack of effective focusing arenas to consolidate these eclectic interests, a presiding internet regime has not yet emerged, though several of these regimes continue to compete for a dominant position in the transnational policy arena. Broadly, then, it is conceptually problematic to refer to the FOC as "the" internet freedom policy arena or treaty regime that is, or should, worthy of singular examination. Indeed, there are many venues and arenas where the norms surrounding internet freedom promotion are being defined and debated. However, it is because of the FOC's formal coalition of committed and prominent member states, and the coalition's peculiar launch as a direct *response* to the aftermath of the Arab Spring, that justifies the FOC both as an interesting case both conceptually distinct and empirically novel for deeper analysis.

To elaborate, investigating the FOC and all its related networks of actors and their activities surrounding internet freedom promotion in the time period after the Arab Spring is empirically novel because of its unique historical importance. Second, investigating the FOC and its affiliated internet freedom stakeholders is conceptually important because no focused research has to date evaluated this particular set of stakeholders that are vigorously justifying the establishment of an internet regime to globally protect the democratic rights of citizens beyond citizenship and state boundaries. For both these reasons, then, we must investigate the activities of the FOC and connected internet freedom promotion activities because this represents a unique case *found* in the empirical world, as well as theoretically interesting case *made* due to its nature of being an anomaly in the existing scholarship (Ragin and Becker 1992).

Thus, this investigation progresses by using the FOC as a starting point for discussing the broader internet freedom proto-regime being shaped since the Arab Spring of 2011-2012 to identify the potentially new infrastructure stakeholders surrounding internet freedom concerns. By tracing the emergence of these novel stakeholders and their contemporary cooperating and conflicting interests I also identify connected and parallel policy arenas where substantive internet freedom work is also being conducted that the existing scholarship must incorporate and theorize. By doing so, a key contribution of this investigation is the incorporation and identification of important new communities of practice that have been under-examined in telecommunications scholarship since the rise of participatory digital media platforms (Jenkins 2006).

Infrastructure Politics Undergirding Digitally-Enabled Political Change

This study addresses a significant gap in comparative political communication scholarship. On the one hand, there have been several recent advances in the study of transnational collective action and technology-enabled social change that seem to seamlessly transcend state boundaries (Bennett and Segerberg 2013; Howard and Hussain 2013). Across disciplines, political scientists, political sociologists, and political communication scholars are (re-)assessing the technological and cultural processes enabling contemporary political participation in the most advanced media systems (e.g., the Occupy Wall Street protests). On the other hand, comparative politics and democratization scholars are also taking detailed note of similar trends in developing societies and non-democratic states (e.g., the Arab Spring revolutions). But neither trajectory has yet substantively reconciled the claims surrounding these new digitally enabled processes because they are agnostic to the reality that these new activities require a shared and global *digital infrastructure* upon which social media platforms and digital media technologies exist. Incorporating the global political economy of digital infrastructure is a significant gap in studies of comparative political communication.

It is necessary to expand the domain of scholarship in political communication to include contemporary infrastructure politics. We need to understand how the technological affordances that have come to empower (and sometimes threaten) mediated political participation also depend on the complex transnational political economy that undergirds digital tools and online environments. This is a critical gap in communication scholarship because most media and communication environments are being established on a shared and transnational internet backbone that is radically different from the broadcast infrastructure of previous decades. In this arena, it is states and multinational technology corporations that are involved substantively in designing and regulating digital infrastructures. But most scholarship tends to focus on the experiences of citizens and civil society actors and how they use digital media, and remains agnostic to the more influential stakeholders' structural influences.

To address this gap, I begin with the premise that digital infrastructures have empowered both democratic movements and recalcitrant rulers in observed and causal ways. I clarify that the central research problem is not whether or not digital technologies are of political consequence, but rather how these consequences are being managed and perhaps could be managed more effectively in the democratic interest of the users. To do so, communication scholarship must

begin to identify the forces by which advanced Western[4] technologies have been made politically significant in nondemocratic settings, and the new challenges being faced by the stakeholders[5] attempting to govern the democratic impacts of these technologies. This is why we must expand the domain of focus beyond the users and uses of digital technologies, to critically investigating the stakeholders shaping digital infrastructures. These diverse infrastructure stakeholders are participating in the promotion and designing of important social and political affordances for their users by shaping the *norms, frameworks* and *policies* that undergird the eventual construction of digital social and political environments.

Investigating the ongoing developments surrounding internet freedom policy promotion is not the only starting point for doing so, but there are several reasons why it is a logical one to begin with. First, internet freedom promotion is important for understanding how the new digital infrastructures that support political communication and participation in both democratic and nondemocratic regimes emerge as a consequence of transnational political economic forces. Second, it is necessary to advance our research agenda to anticipate and critically assess the developments of this broad policy arena by understanding the actors doing this work. Third, doing so will allow us to go beyond describing how our modern public communication systems are, towards better understanding how these systems come to be through historical conditions, political perspectives, and the intentional and powerful actors constructing them (Hallin and Mancini 2004). The recent period of transnational activity surrounding internet freedom promotion reflects both a historically significant moment and a conceptually novel case for critical examination. In sum, we must do more than theorize the ways in which digital media and digital technologies shape or effect political participation for users and citizens; we must also understand how important political communication environments are sometimes shaped in powerful ways by small groups of social actors and their vested interests.

For those reasons, this chapter proceeds by synthesizing and summarizing the most recent findings on the causes and consequences of digital media and ICTs used for political participation from an international and transnational perspective. Because this is a study focused

[4] "Western" because they have been produced there, and the political economy shaping them continues to be based there.

[5] Again, I begin with the premise that these stakeholders are also based in advanced industrialized Western democracies, but empirically investigate the transnational network later in the study.

on the efforts sparked to promote internet freedom policies as a result of the Arab Spring, I do not conduct a comprehensive review of all of the literature on all country cases where technologies have been observed to play a role. Instead, I offer a more focused review of the most recent and relevant contours of the debates surrounding ICTs and democratization that has arisen *because* of the Arab Spring revolutions. I argue that the underlying political conditions of the technological infrastructure upon which media systems are established have not received critical attention. However, the events of the Arab Spring have illuminated this agnosticism regarding the politics of digital infrastructures.

This agnosticism about infrastructure politics in current political communication scholarship is partially due to the limitations in place on the restricted technical knowledge contained in related domains, like telecommunications research. Telecommunications scholarship is often utilized in studies interested in economic aspects of globalization, but is often mired in specialized debates and discussions about pricing protocols and complicated, sometimes insular organizations like the International Telecommunications Union (ITU). As such, this highly specialized body of research is not well-connected in its significance to other fields, like explaining modern processes of political change. But providing some foundation for making these connections by showcasing the consequences of digital infrastructure for political participation is necessary in order to advance this investigation about internet freedom.

Because this study is explicitly focused on the problem of understanding the new policy arenas, norms, and regimes being formulated to secure digital infrastructure, the remaining discussion develops by following these three steps: First, I review how ICTs have been observed to play a role in mobilizing political change. I argue that ICTs have had causal consequences both for and against democratic entrenchment, even in the most repressive political contexts. Second, I review the most current evidence to argue that the political uses of ICTs (both for and against democratic purposes) have ultimately been dependent on the undergirding transnational digital infrastructure that has enabled global communication and mediated participation. Third, I illustrate how digital infrastructures have come to be the object of political contention for democracy promoters and recalcitrant rulers alike. In doing so, I conclude by identifying the new sets of actors and stakeholders who have agitated in transnational arenas to fight over that infrastructure in the name of promoting internet freedom: technology-savvy *civil society* activists (the civic users generating new technology policy norms), multinational *technology corporations*

(the private actors providing digital infrastructures), and advanced ***democratic states*** (the state actors necessary for effectively enforcing new policy frames).

By following this line of argumentation, the remaining discussion helps to justify the conceptual importance of updating our understanding to go beyond the established internet regimes that are well-investigated (e.g., the ITU vs. ICANN). Doing so also requires that we critically examine the emergence of the internet freedom proto-regime that is being championed by Western democracies since the Arab Spring. In the next section I begin by reviewing recent evidence about the consequences of digital infrastructures during periods of political crisis.

1.2 What has the Arab Spring taught us about the Political Internet?

Immediately following the Arab Spring revolts, the July-August 2011 issue of *Foreign Affairs* reflected on the central question puzzling comparative scholars today: "Why Middle East Studies Missed the Arab Spring: The Myth of Authoritarian Stability" (Gause III 2011). Other events soon to follow, like the Occupy Wall Street (2011) movement in North America and Western Europe, the Greek protests against EU austerity measures (2011), collective mobilizations during Russia's elections (2011), the Spanish Indignants protests (2011-2012), and, more recently, Turkey's Gezi Park protests (2013), have all paid symbolic homage to the Arab protests and revolutions for inspiring the organizational strategies of movement leaders and bolstering the courage of participating activists. Indeed, several waves of protests across the globe have taken place since in sub-Saharan Africa, Europe, Asia, and the Americas, and reflect the structural connective and transnational features observed during the Arab Spring (Bennett and Segerberg 2013). Even far-off Oceania has been impacted, where, during the period when Libya was embroiled in protests and civil war, a group of Sydney-based Fijian democracy promoters organized to challenge the military junta in Fiji while citing the Arab Spring protests as the inspiration or trigger.

These waves of unprecedented global protests have collectively provided political scientists and political sociologists with an important call to update their frameworks, theories, and assumptions about how political change is being organized today. While comparative researchers have been quick to acknowledge the novel aspects of these transnational and consecutive protests, investigating the mobilization tools necessary for organizing them is a more challenging task. There still exists considerable skepticism about drawing critical attention to the

emergence of new communication technologies and digital infrastructures as serious ingredients in the causal recipes for contemporary democratization. Uncritical labels offered by enthusiastic journalists and observers, like "Facebook revolutions" and "Twitter revolutions," have also served to stall the intellectual foundation for more seriously observing technological interferences in contemporary international politics.

Some of the skepticism about taking ICTs and digital infrastructures seriously comes from disagreement on how to define the political moment itself. Some argue that "there has been—and there will be—no serial collapse of authoritarian regimes leading to a democratic future. Instead of 'revolution', the talk now is of 'uprisings', 'revolt' or even simply 'crisis'" (Dalacoura 2012: 63). This concern rests on whether the Arab Spring was democratic enough, or whether it is too soon to define some of the processes and attributes of the mobilizations as sufficiently democratizing. In some ways, this skepticism is justified. The long-term process of political change and institutional democratization must be measured by studying the complex series of regulatory and institutional changes in the political systems and procedural practices that meaningfully engage citizens in democratic acts. Other concerns also rest on consistently documented challenges, such as the corrosive power of oil wealth (Ross 2008), and the deeply-rooted gender inequity in many Arab societies (Meyer, Rizzo, and Ali 2007) – conditions which cannot painlessly be overturned in the immediate aftermath of popular protests. In other words, many Arab societies may have ousted their ruling dictators, but the controlling interests and structural conditions embedded in the maintenance of authoritarian power have not.

Despite these reasons to remain critical, it is also necessary to account for the important ways in which ICTs and digital media use have changed the processes of democratic entrenchment and authoritarian power. Recent studies assessing the Arab Spring also find that ICTs do have a causal influence on processes of democratization, and that some recipes actually help explain democratic entrenchment in some of the most repressive political systems across the span of years, not just after momentary protests (Howard 2010). The opposition movements and civil society actors in Egypt and Tunisia may not have had much practice in organizing real elections and relevant opposition parties before the Arab Spring (Langhor 2004; Posusney 2002). But since the gradual and exponential introduction of internet infrastructure long before the Arab Spring, they somehow slowly gained new capacities to mobilize powerfully with new communication tools around shared grievances, again and again.

Yet most comparative observers still do not pay serious attention to the radical ways in which Arab states and societies had been impacted on all levels (economic, social, and political) by the introduction of new ICTs and digital infrastructures over the past two decades. These perspectives that do not account for the impact of digital technologies on state-society relations and opportunities for organizing political change point to the authoritarian resilience of oil-rich monarchies as counter-factual examples (Ehteshami 2003; Ehteshami and Wright 2007). States like Bahrain, Qatar, and Saudi Arabia had used those resources efficiently to better fund, secure, and co-opt new technologies to bolster their authoritarian capabilities – suggesting that digital media was having an antidemocratic impact on those societies. But a more discerning interpretation would also make note of the fact that technologies had enabled *both*: 1) the empowerment of pro-democracy movements and the entrenchment of civil society on the one hand, and on the other hand, 2) refined the powers and practices for exercising censorship and surveillance by nondemocratic regimes (Hussain and Howard 2013).

To emphasize the last point, interpretations of the Arab Spring that do not take into account digital technologies and new forms of organizing political change risk re-telling an incomplete and inaccurate story about authoritarian exceptionalism in the 21st century (Kamrava 1998; Bellin 2004; Posusney 2004). These presiding digital infrastructures-agnostic analyses no longer resonate as strongly with events on-the-ground today. If we are to have a more accurate understanding of why modern cascades of political change were different and unexpected, we must account for the unexpected forces and novel practices related to digital-enabled organizing observed before and during the period of rapid mobilizations across several countries.

Today, with the peak of the Arab Spring behind us, several countries including Tunisia and Egypt are struggling to develop long-term and sustainable democratic institutions. But it does not reduce the level of scholarship to investigate the new patterns of political change and modern recipes of democratization being observed after the widespread diffusion of internet infrastructure. In response to the growing chorus of voices asking whether we need to rethink the logic of authoritarianism in the Arab world, or even broadly, authoritarian persistence writ large, Bellin (2012: 127) has answered in the affirmative by identifying several new puzzles: the dynamics of military defection; the logic of social mobilization; and *the importance of social media and satellite television's structural capabilities* in the mobilization process.

In summary, a more complete understanding of contemporary political change, even in the most stalwart nondemocratic regimes, requires unpacking both: 1) the infusion of digitally-mediated political participation by democracy promoters in their organizational practices, and 2) the counter efforts by repressive rulers to contain and repurpose the new infrastructures and tools that facilitates such practices. Activists and dictatorships have come to see digital technologies as political goods that can be used (and constructed) as both democratic scaffoldings and as authoritarian panopticons. In all these cases, the common struggle has been one pitting citizens and civil society actors against dictators and their security forces to control the political uses and affordances of digital infrastructures. But the important thread linking these opposing stakeholders (state powers vs. civil society) has been the technology companies (i.e., the private sector) that own and maintain key pieces of digital infrastructures. So it is the case that unpacking the politics internet freedom promotion requires investigating at least three core categories of stakeholders: *state powers*, *civil society*, and the *private sector*.

With the benefit of some necessary hindsight, this different retelling of the story about the Arab Spring should acknowledge, even privilege, the real ways in which dissent was organized. We must do so by paying close attention to the interactive relationships between the new arsenals of communication tools and strategies used by protesters to outmaneuver their dictators. Furthermore, because the infrastructure that supports these mediated political practices was located globally and transnationally to begin with, the experiences and lessons from the Arab Spring have taught us that we must begin to see digital infrastructures as an important arena for exercising state power and for international politics itself (Hussain and Howard 2013). As I will demonstrate in the next section, the democratic activists who exploited the political capacities of digital infrastructures have, since the Arab Spring, done more than just recognize it themselves as an important good to secure in the democratic interest. Since the Arab Spring, they also begun to agitate and organize transnationally to implement better support and policies to protect their digital infrastructures in the name of human rights.

Transnational Actors and Politics behind Infrastructure Activism

A digital media-focused analysis of modern political change is importantly unique from analytical perspectives that are agnostic to the intimate and important ways in which global communications systems have come to impact societies. Mainly, a digitally-centered analysis

shows that the central puzzles surrounding contemporary political change have embedded in them the strategic uses and unexpected pitfalls of digital media and digital infrastructures (Howard and Hussain 2013). So if we were to reassess the lessons learned from the Arab Spring and acknowledge the observable ways in which contemporary communication tools and strategies were intimately tied to the process of organizing political change, how might we retell a slightly different version of events? More importantly, what might this tell us about internet freedom politics today?

Ben Ali ruled Tunisia for twenty years, but in early 2011, digitally-enabled protesters tossed out their dictator in less than two months. Emboldened and inspired by neighboring events, the April 6 youth movement in Egypt mobilized to organize sustained protests to challenge the thirty-year-old Mubarak regime through surprisingly disciplined and largely peaceful demonstrations. Watching and learning from these creative strategies, discontent spread over digital media networks of family and friends to Algeria, Jordan, Yemen, and other authoritarian states in the Arab world. These important political moments consistently drew diverse networks of people, many of whom had not been political before: young entrepreneurs, government workers, women's groups, and the urban middle class. Digital media networks consistently enabled activist networks in the Arab region to voice shared grievances and nurture transportable strategies for mobilizing against their dictators. Across the Arab Spring protests, defections from censored media and security agencies were announced on social media, mobilization tactics were shared on Facebook pages and activists' blogs, and desperate calls for global sympathy and support were spread by citizen journalists on Twitter.

But it is also myopic to tell the causal tale of digital media and political change in the Arab Spring as if it had started in 2011. In Egypt, the April 6 youth movement was cautiously testing strategies for peaceful resistance as early as 2008. In late 2009, armed with mobile phones and digital cameras, international activists from London with transnational support networks flew into Tahrir Square and demonstrated against the Egyptian-Israeli blockade of the Gaza Strip. Through innovative hybrid media campaigns relying primarily on microblogging, the conjoined networks of European and Arab activists engineered an international media event that eventually pressured Egyptian authorities to temporarily lift the blockade so humanitarian aid could pass through to Gazans. Lebanon also experienced the first stirrings of its Cedar Revolution as early as 2005—a chain of massive demonstrations in Beirut that critically limited

Syria's stronghold on Lebanese political liberalization. Because of this decisive victory, in the ongoing Syrian civil war Beirut's internet infrastructure, as well as Israel's neighboring internet backbone, continues to serve as a critical node and relative safe zone for sympathetic "hacktivists" and "fixers" to secure the flow of political information to international news agencies and human rights organizations.

There is also evidence that some important strategies for peaceful democratic change came from international NGOs like the Centre for Applied Nonviolent Action and Strategies—a Serbian organization led by Srđa Popović, who in 2000 helped mobilize the resistance to end Milošević's rule, trained protesters in 2003 for Georgia's "Rose Revolution," followed by the Lebanese protests of 2004, Ukraine's 2005 "Orange Revolution," and the Maldives' revolution in 2007, and eventually moved down to train Egypt's April 6 movement in 2008. Popović's book *Nonviolent Struggle: 50 Crucial Points* is a best seller in terms of free online downloads by activist organizers, totaling more than 17,000. Thus it is not easy to pinpoint exactly when the digitally enabled revolutions of the Arab Spring first began. Tunisia's unexpected revolution may have sparked this latest round of events, but it is worthwhile to recognize that a particular breed of "information activists" were working transnationally across the Arab world and the European Neighborhood (with assistance from political diasporas in Western democratic states) as early as 2005. These activists, and their notable focus on securing and applying the political potential of digital technologies, helped enable activists in Tunisia, Egypt, and beyond with the experience and sophistication of using ICTs and new media tools for organizing peaceful and effective resistance against experienced authoritarians and their well-funded security and surveillance practices.

Based on these rich case histories, telling a digital media history of the Arab Spring is important because many of the new characteristics and processes being documented in current comparative politics are in important ways being mediated by the new communications infrastructure made possible since 1995, when the US National Science Foundation effectively privatized the internet as a consumer good. For example, observations that a different public sphere was being encoded into the fabric of Arab societies, even in the most repressive political systems, have had a long history of scholarly recognition, but one thus far sequestered in the new fields of digital politics and cybercultural studies. Early on, it was Al-Saggaf's (2006) study of the online public sphere in the Arab world that first documented the important ways in which

civic engagement was being nurtured in the news and discussion spaces of online news organizations. Recent work has also documented the growing importance of participatory networking sites which provide a relatively open and safe space for youth to experiment with a wide range of social and political issues (Omoush, Yaseen, and Alma'aitah 2012; Shirazi 2012). In sum, tools like Facebook, Twitter, blogs, and other internet applications have been strongly linked with the broadening of political engagement opportunities in cases across Arab authoritarian regimes (Al-Kandari and Hasanen 2012). So it is more than plausible that the long-term and infrastructural diffusion of ICT tools and online services are important precursors for the cultivation of discussion and deliberation, shared grievances and opinion formation, and even mobilization and social action in digitally mediated spaces.

Weighing multiple political, economic, demographic, and cultural conditions, then, it is components of digital infrastructures that consistently appear as key ingredients in parsimonious models helping to explain the conjoined combinations of causes behind regime fragility and social movement success in this Arab Spring (Hussain and Howard 2013). Therefore, to understand the successes and failures of contemporary political protests, we must also assess how civil society leaders and authoritarian security forces treated communication technologies as politically consequential. This important perspective draws attention to the idea that it is not enough to observe the uses of digital media and ICTs—it is more important to question *how these tools come into existence in the first place*. Not doing so risks continuing to develop an intellectual understanding of media use and political change that remains agnostic with respect to the digital infrastructures that supports contemporary mediated practices of political participation and engagement.

But digital tools and ICTs are not static and unchanging structures; they are constantly being shaped and reshaped by both technology designers and users—a perspective well recognized by work on the social shaping of technology (Neff 2012). Digital media platforms and their forms and frequency of uses are structured and afforded by various transnationally distributed stakeholders, including engineers and regulators. Therefore, the broader internet infrastructure that supports digital media platforms like Facebook, Twitter, etc., exists in a complex political economy of transnational conditions governed, regulated, and contested by a highly complex set of actors, including state powers and private commerce stakeholders. To illustrate this, consider the fact that the US State Department–supported Alliance of Youth

Movements network has since 2009 designed and deployed social media protest strategies to activists in Egypt's Arab Spring, G20 protests, and others, combining digitally enabled strategies like "smart mobbing" for political, marketing, and artistic causes. Democratic activists and political users of digital media tools and ICTs have also increasingly intervened in the construction of these tools and the underlying information infrastructure they exist on. For example, both Egyptian and Tunisian youth were involved in an organization called Takriz, a self-described citizen "cyber think tank" established in 1998 that also provided activists in the Arab Spring with technical training in countercensorship and surveillance software (Pollock 2011). So even though it was the state, in this case Ben Ali's regime, that brought internet infrastructure to its citizens, it was the activist community involved in Takriz that exploited the regime-sponsored infrastructure to cultivate safe spaces and digital strategies for antiauthoritarian activists to turn against the regime's interests (Khondker 2011).

Furthermore, the democratic uses of digital media are not inherently afforded by online technologies—they can, as has been observed across democratic and authoritarian regimes since 1995, be used against civil societies (Howard, Agarwal, and Hussain 2011). When the Arab protests began in 2011, dictators and their authoritarian regimes did not stand idly by. In Tunisia, Egypt, Libya, Algeria, and elsewhere, regimes came down forcefully to try and shut down communication networks. Some were successful, as in the case of Egypt shutting down London-based Vodafone, while others, like Algeria, did not have centralized management to easily coerce technology providers. But surprisingly, even when unfriendly governments were successful in shutting down communication networks, transnational networks of sympathetic "information activists" skillful in technology-savvy activism also activated to redesigned tools for political use and waged hacktivism wars to negatively affect dictators' communication capacities. This particular breed of activists was further supported by technology policy NGOs, like US-based AccessNow (which is now referred to as Access) and the Bay Area-based Electronic Frontier Foundation (EFF). Both launched effective lobbying campaigns to pressure ICT companies like Vodafone to turn connectivity back on and launched investigations to hold Western software companies accountable for selling censorship technologies to the repressive governments of Syria and Bahrain.

Considering these compelling narratives drawn directly from the experiences of the Arab Spring, it seems then that we must say more than just that technologies are sometimes socially

shaped and perhaps politically consequential. Based on the above events, it seems that technologies are often (re-)engineered with political affordances for very intentional and political outcomes, sometimes by their designers, but also by their users. Unfortunately, perspectives that go beyond treating ICTs and digital infrastructures agnostically to bring critical attention to the political economic conditions which help give rise to new digital safe spaces and provide civil society actors with digital scaffolding to do their work are still limited. Most often, these perspectives are also relegated to scholarship in associated fields of telecommunications policy and mired in technical language about engineering standards that do not easily illustrate or explain the intimate political conditions, ideologies, and experiences shaping their use by and impact on citizens and activists (see: Mueller 2010, Denardis 2009).

But since the aftermath of the Arab Spring, political activism and policy debates surrounding digital infrastructures have become highly visible and contentious at the international level. These events and negotiations are novel because they have been new additions to the existing forums and arenas that have traditionally existed surrounding internet governance (e.g., the ITU, the IGF, ICANN, etc.). Between the period during which major protests of the Tunisian, Egyptian, and Libyan revolutions concluded (October 2011) and when the UN's ITU organized in Dubai (UAE) to revise its quarter century-old global telecommunications treaties at WCIT-12 (December 2012), there have been at least 10 major stakeholder summits focused explicitly on defining and promoting internet freedom (see Table 1). These policy conventions and conferences have been brokered by the foreign policy offices of key Western democratic nations (e.g., The Netherlands) and others, including respected civil society organizations (e.g., Access) and influential multinational technology corporations (e.g., Google).

Access, the main organization that pressured technology companies to stop selling software tools to dictators in its aftermath of Iran's Green Revolution (2009), and lobbied corporations to keep digital networks running during Egypt's national internet shutdown (2011) has taken an international leadership role in organizing networks of civil society activists around issues of "internet freedom." In October 2011, immediately following the Arab Spring protests, Access launched its first Silicon Valley Human Rights Conference. Though organized by a civil society group, this event was also sponsored and funded by Google, Facebook, Yahoo!, AT&T, Mozilla, Skype, and other key multinational ICT corporations, and brought together corporate

leaders and foreign policy officials of major Western democratic nations to design policies for corporate social responsibility with respect to international human rights.

Similarly breaking with convention, the governments of the United States, the Netherlands, Sweden, and the European Union also publicly followed suit, creating formal funding programs of over $100 million to support digital activists working within repressive regimes under the auspices of the Freedom Online Coalition (discussed previously in section 1.1). Most of the competitive and winning responses to their requests for proposals (RFPs) dealt centrally with issues connected to digital infrastructures and ICTs, like helping to create secure and anonymous internet access points for activists working within nondemocratic states to communicate freely and safely on their laptops and internet-enabled mobile devices. One of the most publicized and celebrated outcomes of these funding initiatives and state backing was a proxy internet access protocol called *Tor*. Tor has been used across the world in places like China, Saudi Arabia, and elsewhere by activists and citizens to access content securely and anonymously. Furthermore, member states of the FOC have also organized independent, but coordinated, internet freedom arenas to bring together global stakeholders physically in Berlin, Dublin, London, Stockholm, Vienna, and elsewhere (see Table 1).

The most recent efforts have also extended internet freedom promotion work to include citizens and stakeholders in emerging powers, like Brazil, and more events have been scheduled to extend reach to the Asia-Pacific region, starting with South Korea. However, since the period when major protests of the Arab Spring subsided the most active supporters of internet freedom focused organizing have been a core collective representing technology activists and policy makers from advanced industrialized Western democracies (reflected in the membership of the FOC). Altogether, then, between the conclusion of Arab Spring protests (October 2011) and the UN's historic quarter-century ITU treaty negotiation in Dubai (December 2012), these stakeholder meetings and negotiations have worked to highlight and elucidate the complex issues surrounding the digital infrastructural politics from the perspectives of activists, governments, and corporations. Because these stakeholders and their activities reflect a convergence around technology-based political activism, the remaining discussion in this chapter introduces the analytical frames and conceptual tools necessary to investigate this important new domain of transnational activities and conflicts involving global digital infrastructures.

Table 1: Post-Arab Spring internet freedom Multi-Stakeholder Meetings, 2011-2012

Summit	Location	Date	Organizer
Silicon Valley Human Rights Conference I	San Francisco	Oct. 2011	Access
London Conference on Cyberspace	London	Nov. 2011	UK Foreign and Commonwealth Office
Our Internet – Our Rights – Our Freedoms	Vienna	Nov. 2011	Council of Europe
Freedom Online Conference I	The Hague	Dec. 2011	Freedom Online Coalition
Stockholm Internet Forum	Stockholm	Apr. 2012	Swedish Ministry of Foreign Affairs
Human Rights and Technology Conference II	Rio de Janeiro	May 2012	Access
Dublin Conference on Internet Freedom	Dublin	Jun. 2012	Organization for Security and Co-operation in Europe
Internet at Liberty Conference: Promoting Progress and Freedom	Washington DC	Jul. 2012	Google
The Internet and Human Rights: Building a Free, Open and Secure Internet	Berlin	Sep. 2012	German Federal Foreign Office
Freedom Online Conference II	Nairobi	Sep. 2012	Freedom Online Coalition

Note: List prepared by author based on interview and fieldwork data collected from informant interviews and snowballing between March 2011 and December 2012. List excludes informal side-events, "hackathons," and major internet governance summits that did not focus centrally on promoting the internet freedom discourse or agenda.

1.3 Inside the Internet Freedom Proto-Regime: An Investigative Framework

The discussion arc thus far has taken two broad steps. First, I argued that many elements of digital infrastructures are consequential to political communication, and this is particularly true in non-democratic political systems (section 1.1). This is because digital infrastructures are the scaffolding upon which contemporary forms of digitally-enabled political organizing are taking place. To that end, the Arab Spring experiences as well as several recent waves of protests have shown in myriad ways that both political activists and state powers are struggling to secure different kinds of digital affordances. More importantly, these examples often share a common narrative where both users and rulers increasingly target internet service providers (who facilitate digital access) and digital media companies (who facilitate digital content). Users, particularly political activists, are increasingly pressuring these access and content providers to keep both open and flowing during periods of political crisis. Simultaneously, repressive rulers and state powers are increasingly coercing the same digital infrastructure providers to monitor and/or censor political uses of digital media for their political interests. In many extremely repressive political systems, like those of Qatar or Saudi Arabia, the state itself is the internet service provider and has near total control of all aspects of its digital environment. However, even in less extreme examples, the technocratic skills and necessary technologies to dominate digital infrastructure often originate from the advanced industrial economies of Western democracies.

Second, as a consequence, I also provided several novel examples of policy initiatives that have opened up in the international policy arenas since the Arab Spring related explicitly to issues and agendas promoting internet freedom (section 1.2). These policy arenas are sponsored, often independently, by several[6] advanced industrialized Western democracies interested in better supporting and regulating digital infrastructures in the global public's democratic interest, or at the very least for the purpose of establishing more socially responsible standards for managing their technological exports. More importantly, these initiatives currently exhibit a surprising lack of consensus because a vast array of interests and frameworks has been championed by the diverse community of stakeholders invited into these discussions. So what internet freedom means and how it should be promoted within the realms of policy making, adoption, and implementation is hitherto unclear and needs to be clarified so that an effective

[6] Again, the Freedom Online Coalition (FOC) is the most public and cohesive expression of this policy phenomena, but is not the sole proprietor of internet freedom concerns. See Table 1 for a complete list.

policy regime might emerge. The likelihood of this eventuality depends on the consolidation and establishment of a coherent norms system that respects the various invested stakeholders' goals and needs.

Because this discussion and reflections on recent events have collectively illuminated a complex set of contentions and politics about digital infrastructures that are taking place at the international level and includes multiple stakeholder communities, I will now clarify a conceptual framework with a three-part analytical utility to advance this study. *First*, the approach must be able to unpack the complex political economy of the involved stakeholders in the transnational arenas and their connected interests surrounding digital infrastructure. *Second*, because the policy interests of these actors are often conflicting, the approach should view policy formation as a process that is socially constructed through debates, negotiations, and norms consolidation taking place in and across various communities of practice (Lave and Wenger 1991; Adler 2008). *Third*, because in its current manifestation internet freedom refers to a broad domain that hasn't effectively been consolidated into a coherent policy regime, the framework and investigation should serve to illuminate some opportune avenues for pragmatic consolidation.

For these reasons, I propose adopting the notion of *proto-regime formation* from international relations theory—a corpus of scholarship invested in understanding how new policy regimes are established by networks of policy entrepreneurs who transcend local contexts to solve complex transnational challenges that require knowledge exchange from different institutional backgrounds (Roberts and King 1991). Transnational policy regimes matter because they provide the forum or medium by which state powers cooperate to solve shared problems or allocate public goods in the transnational or global environment (Haggard and Simmons 1987). Regimes are necessary policy apparatuses because international activities today rely increasingly on overseas investment and trade, and the channels of global communication which make these interactions possible are "more numerous, decentralized, and diverse than ever" (Haas 1980: 357).

Effective regimes require complex negotiations and consolidations of norms in multi-stakeholder environments to take place in order to be established. Attempts to coordinate behavior among a group of countries around shared challenges, for example by setting up global telecommunications infrastructure, are often governed by numerous semi-voluntary bilateral

agreements that it is often extremely complex to form agreements around because of the number of autonomous states and stakeholder communities involved. Examples of these regulatory regimes and challenging issues include: the International Telecommunications Union (ITU), the International Monetary Fund (IMF), the Kyoto Protocols, the Geneva Convention, and various weapons-trade control agreements designed to coordinate transnational cooperation between several states (Neumayer 2005).

All established regimes must go through formation periods dealing with the work of aggregating and consolidating conflicting norms, disagreements, and impasses between different communities of stakeholders. These "proto-regime" period (i.e., regimes that have not yet been consolidated, and therefore lack enforceable coherence) can take many forms and directions in its advancement, but can be described as having an *eclectic, rational, skeptical, or pragmatic* direction (Haas 1980).

- *Eclectic* regimes tend to link issues in a tactical manner. The key actors involved do this by manipulating technical information for their strategic needs, and because of the overt self-interests driving their functions and participation, these types of proto-regimes will likely not emerge, and instead devolve into disagreement.
- *Rational* regimes substantively link issues on the basis of agreed doctrines—but because of the dependency on shared doctrines, the success of these regimes depends on finding simple issues with clear doctrines or clarifying issues to achieve joint doctrines.
- *Skeptical* regimes are often fragmented and only held together by the will and capability of powerful states and partners paying off their opponents. Because of this, skeptical regimes tend to be weak and unstable.
- Finally, *pragmatic* regimes attempt to narrow the scope of the regime down to a mutually beneficial range of interests acceptable to all important stakeholders. This often eventually results in a more limited but fairly stable regime that is also able to adapt and adjust to the evolving challenges and issues being addressed.

The internet freedom proto-regime investigated in this study can be currently described as being in a current period of stasis best encapsulated as an *eclectic regime* where state actors, technology providers, and digital activists are all bringing contrasting norms and interests regarding digital infrastructure. The involved stakeholders are also engaged in the pragmatic task

of nurturing a more focused (and coherent) policy framework to secure digital infrastructures. However, what they mean when working to promote internet freedom and whom they intend to serve in doing so has not been defined clearly or consensually. But it is precisely this definitional period of impasse and conflict that is critical to examine because important decisions are being made by the involved stakeholders to chisel the scope of the regime. In order to do this, we must also investigate the stakeholders, understand their norms and motivations, and identify which actors or communities of practice are producing the most viable and innovative policy ideas (Lave and Wenger 1991).

In order to do this, it is important for this investigation to look beyond the obvious and influential actors, like governments and established policy institutions (the main focus in internet governance and telecommunications policy scholarship). By recognizing that state powers and powerful institutions from the top down are not the only relevant actors exerting forces on periods of regime formation, we can account for newer and nontraditional stakeholders entering the mix. These could include: transnational advocacy networks, global civil society members, nongovernmental organizations, and global citizens and "international public spheres" from the bottom up that seem to be more agile and important in recent studies of international relations and regime formation (Cochran 2002). In this approach, new "communities of practice" and their production of expert knowledge have become useful analytical perspectives for understanding how regimes evolve throughout their formative periods:

> "Regimes are not simply static summaries of rules and norms; they may also serve as important vehicles for international learning that produce convergent state policies. This role for regimes has been seriously underestimated in the theoretical and empirical literature, which has tended to focus on two correlates of regimes—political order and economic growth—rather than on the *transformative processes that regimes may imitate or foster*. The literature has also paid little attention to the fact that some *regimes stem from communities of shared knowledge* and not simply from domestic and transnational interest groups." (Haas 1989: 377; emphasis added)

These growing references to "communities of shared knowledge" in international relations work refers to a concept introduced by Lave and Wenger's (1991) called "communities of practice." In their early formulation of communities of practice, this referred to the forms of learning taking place outside of highly structured institutional environments. Rather, communities of practice

referred to the more haphazard social contexts in which learning itself was a social activity co-created by the interactions of experts and novices—what Lave and Wenger call "Legitimate Peripheral Participation" (LPP).

Through their grounded ethnographic analysis of a range of sophisticated professions, like midwives, tailors, navy quartermasters, supermarket butchers, and more, LPP has allowed orthodox social psychological traditions studying the process of learning and innovation to incorporate a social constructionist approach, in contrast to a behaviorally deterministic one. Legitimate peripheral participation has also provided a coherent framework to concretely examine the various informal, and therefore flexible and innovative, networks of social actors, who include both advanced professionals and amateur enthusiasts, engaging in transformative and long-term interactions that lead to new standards and practices (i.e., communities of practice). In this view, social actors and their levels of expertise and ideological traits are not the only sources for explaining how new standards and practices are produced. Lave and Wenger argue that group cultures *created by* communities of practice, embedded across formally structured institutions and loose epistemic networks, are a critical lens to understand the process of learning and innovation. Examining peripheral participation in these communities of practice has provided fields as diverse as education research (Cobb and Yackel 1996), innovation management (Brown and Duguid 1991), and urban sociology (Deakin, Lombardi, and Cooper 2011), to change the unit of analysis from "knowledge in the heads of individual" experts to their interactions in groups engaged in social practices and cultural production. *In this investigation, because we are examining the formation of new policy frameworks surrounding internet freedom, it is equally important to examine the new social spaces and social practices where internet freedom is being promoted, in addition to examining the ideas surrounding internet freedom promotion itself.*

Engaging the communities of practice framework also allows me to move the focus away from the narrow learning that happens in the head of individual experts. Instead, I can also delve deeply into the peripheral zones of stakeholder interactions where the new challenges and unanticipated problems of internet freedom work are addressed in a far more observable and rich manner. Identifying important and understudied communities of actors, then, provides an important opportunity to illuminate and demystify esoteric policy-making efforts because it widens the analysis beyond the conventional focus on state powers or private interests

(Moravcsik 2000). Broadening the definition of involved stakeholders to include nontraditional actors and their interaction spaces makes it possible to examine interesting cases of civil society networks and citizen advocacy organizations that seem to be newly organizing since the Arab Spring around the critical politics of digital infrastructure management.

Thus, it is important to investigate the transnational politics of digital infrastructures sparked since the Arab Spring because the negotiations taking place between stakeholders debating internet freedom seem importantly distinct and disconnected from the local activists and indigenous autocrats that are traditionally examined by democratization studies or the institutional and governance stakeholders studied in telecommunications studies. In the recent aftermath of the Arab Spring, the transnational stakeholders and arenas related to promoting internet freedom are importantly new and distinct from the internet governance politics of the past. But it is not very clear what it means to promote internet freedom yet because the label is "like a Rorschach inkblot test: different [stakeholders] look at the same ink splotch and see very different things." (MacKinnon 2013: 188). This leads to some important questions to be examined in the following chapters of this dissertation:

1. Who are the new stakeholders involved in and being engaged to define the issues and contours of internet freedom policy? (Chapter 3)
2. Of these various stakeholders, where is the substantive intellectual and experiential knowledge being drawn from to construct new norms and types of policies and understandings about digital infrastructure? (Chapter 4)
3. How coherent and coordinated are these norms when it comes time to promote internet freedom on the global stage of policy making and treaty negotiations? (Chapter 5)
4. Finally, what are further opportunities and new challenges facing internet freedom promoters to implement a more cohesive and democratically-viable internet freedom policy regime? (Chapter 6)

Digital Infrastructures: Critical, Consumer, or Civic?

Creating technology policy is the core issue that several distinct stakeholders have begun to orbit around with regards to internet freedom promotion. So why not simply draw on the existing literature focused on internet infrastructure and internet regulatory regimes? What exactly is the analytical utility of focusing more broadly on digital infrastructures, and what material and

conceptual properties differentiate its core components? In this investigation I specifically engage with elements of digital infrastructures because each community of the stakeholders brings to the internet freedom arenas different vested interests and ways of valuing the back-end internet infrastructure, the consumer ICTs, or the web-based social media environments they make use of or themselves provide. In short, all aspects of infrastructure related to the internet and the World Wide Web are involved when dealing with internet freedom promotion.

To elaborate, depending on the stakeholders involved, internet freedom can refer to very different components, and therefore be valued and understood differently. For example, these digital components can include or be referred to as: 1) a *critical infrastructure* mediating state power and the affairs of the state (i.e., internet infrastructure), 2) *consumer technologies* facilitating individual's access to digital communications networks (i.e., ICTs), or 3) a *civic scaffolding* allowing political organizers meaningful content and discussion and organizing spaces (i.e., web content). State-based actors often view digital infrastructure as a critical infrastructure which focuses narrowly on issues of national security (cyberterrorism and cybercrime). Technology companies, because they are often tasked with providing and maintaining it, often view digital infrastructure as a consumer technology they are providing to "users" in the form of *access* (e.g., internet and mobile service providers) or *content* (e.g., Google, Netflix, Facebook, etc.). Activists, because they are most concerned about the communicative affordances that digital tools grant them to facilitate digitally-mediated political communication and social mobilizing, often define digital infrastructure as a civic media technology, privileging concerns around censorship and surveillance.

Thus, "digital infrastructures" in this study is an overly encompassing object and concept to be examined and unpacked in the context of different stakeholder communities. Adopting this notion of a multilevel digital infrastructure enables us to move beyond the limitations of traditional internet governance approaches to address the broader domain of internet freedom norms being discussed in this new proto-regime that go beyond the politics of the internet backbone (the standard site of investigation for existing internet governance scholarship). How are the identified stakeholders likely to approach defining "digital infrastructure" and why?

States often view digital infrastructure as an issue of national security. For example, since the mid-1990s (the same time the NSF effectively privatized the internet) the United States

government has established a wide-ranging program[7] on critical infrastructure referring to all "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." These systems and assets, managed by several federal agencies, include:

- Agriculture and Food [Departments of Agriculture and Health and Human Services]
- Banking and Finance [Department of the Treasury]
- Chemical Industry and Hazardous Materials [Department of Homeland Security]
- Critical Manufacturing [Department of Homeland Security]
- Defense Industrial Base [Department of Defense]
- Emergency Services [Department of Homeland Security]
- Energy [Department of Energy]
- Government [Department of Homeland Security]
- Information and Telecommunications [Department of Commerce]
- National Monuments and Icons [Department of the Interior]
- Post [Department of Homeland Security]
- Public Health [Department of Health and Human Services]
- Transportation and Shipping [Department of Transportation]
- Water [Environmental Protection Agency]

Since 2001 then, steadily growing concerns about the threat of international terrorism and global financial crime have led to state actors narrowing their understanding of digital infrastructure as a fundamental communication backbone to be protected from internet crime and cyberterrorism. Here, digital infrastructure for state-based stakeholders simply refers to governmental information systems that utilize parts of the internet's network layer. Therefore, the norms surrounding digital infrastructure and internet freedom promoted by state actors entail concerns about **national security** and **cyber terrorism**.

In contrast to state actors, technology companies' definitional approaches to digital infrastructure can often be understood as focusing on the two parallel types of services they deliver: provisioning *access*, and *content*, to both individual users and national markets. Access

[7] 42 U.S. CODE § 5195C – Critical Infrastructure Protection: http://www.law.cornell.edu/uscode/text/42/5195c

providers are often internet service providers that give public consumers subscriptions to log onto the global internet via a personal computer, or mobile service providers that also provide data access through mobile phones to the global internet (e.g., Comcast and Verizon). In contrast, content providers are the large private corporations that rely on the access terminals that users make use of, but provide content in the form of textual and audiovisual information for users to consume on the World Wide Web (e.g., Google and Facebook). For technology providers, digital infrastructure also refers broadly to all ICTs that interface users with data on the network, including laptop computers and mobile phones (e.g., Nokia mobile phones and Dell laptop computers). To private actors, digital infrastructure, then, refers to both the network layer of the global internet backbone and the interface layer of consumer ICTs. Therefore, the norms surrounding digital infrastructure and internet freedom promoted by private actors entail concerns about net neutrality, and **data traffic** and **data pricing** tiers.

Finally, in contrast to state actors and technology providers, civil society stakeholders understand digital infrastructure to mean the quality and reliability of content and access to digital media and consumer ICTs that they use for their social and political organizing. These digital media users define digital infrastructure in ways that combine both states' and providers' definitions, but with consideration to the normative utility of applying these tools for their political work. For example, they agree with states actors' narrow focus on digital infrastructure referring primarily to the internet's backbone, but in doing so add qualifiers about wanting freedom from surveillance and monitoring on the network layer. Similarly, like private actors, they also define digital infrastructure to more broadly include the digital content and the consumer ICTs used to access this content, but in doing so add qualifiers about wanting freedom of censorship mechanisms which limit data transmissions for specific political content. In summary, political activists and civil society members define digital infrastructure as having reliable and safe access to consumer ICTs free from surveillance and censorship *both* on the internet's network layer (e.g., cables and servers), and the user-level interface layer where they access digital content (e.g., computers and phones). Therefore, the norms surrounding digital infrastructure and internet freedom promoted by civil society actors entail concerns about **political surveillance** and **political filtering** of their digitally mediated experiences.

In summary, a useful definition of digital infrastructure for this investigation must remain an intentionally interchangeable and pluralistic one because the involved stakeholders

themselves disagree on its scope and focus. In the next section, I expand on the norms and concerns that each of the three stakeholder communities seem to be championing based on these differing approaches towards digital infrastructures. The purpose of doing so is to describe how internet freedom is understood differently by stakeholders because focusing on different pieces of the digital infrastructure necessitates distinct norms specific to its context.

Stakeholder Norms: States, Providers, and Activists

A starting point for analyzing which norms are being promoted in internet freedom work is to identify core issues shared across actor categories that can be meaningfully compared and contrasted. These factors include unpacking different definitional approaches for describing the objects of contention (i.e., digital infrastructures) and the associated problem issues (i.e., national security and terrorism; data traffic and data pricing; and surveillance and filtering). To understand why, it is necessary to identify the communities of practice or categories of stakeholders behind these different focusing issues, norms, and definitions. In this study there are at least three main communities of stakeholders worth unpacking: state powers, technology companies, and political activists.

1. *Democratic State Powers* are the conveners of the important arenas that have been cultivated for discussing and debating internet freedom concerns. Democracies are not the only state powers involved, but they are the necessary stakeholders for brokering interactions between multinational technology providers and digital activists. Western democracies are also the most explicit pack of international states collectively backing the promotion of internet freedom, which I have described in the formation history of the Freedom Online Coalition (FOC).
2. *Multinational Technology Providers* are the producers who deploy new communication systems internationally and provide technocratic expertise to governments (including to authoritarian regimes) to implement new communications infrastructure according to their needs and demands. In addition to providing basic internet infrastructure to support digital communication, they are also the stakeholders who have cultivated the large user-base of global citizens who are being directly impacted by different politically aimed manipulations of digital infrastructures by repressive governments.

3. *Transnational Civil Society* includes the broad international community of technology policy experts and political activists who have come together to championing new types of reforms in the regulation of digital infrastructure at all levels (i.e., the network-layer and the interface-layer) being used for political participation across the world. These stakeholders are the most novel and important set of actors because they are introducing new ways of thinking about and valuing technologies that have recently become politically consequential, particularly during the Arab Spring.

State powers are an important set of stakeholders because they have the political power to organize and broker interactions among all stakeholders. Although the private sector and civil society have also brokered their own multi-stakeholder gatherings (such as Google, and Access, respectively), advanced Western democracies have been the most frequent organizers of these arenas pertaining to internet freedom. But promoting internet freedom is not the only way in which state power is an important presence, or the only motive when state actors are involved. For example, authoritarian governments have done their own organizing and sharing of technical expertise, such as Russia, China, and Saudi Arabia who have supported each other in pushing for nation-based definitions of telecommunications policy in recent internet governance gatherings (such as at the December 2012 ITU meeting in Dubai). Similarly, developing countries and emerging democracies also seem to sometimes find common ground and coordinate around their shared needs, like protesting the dominance of primarily US-based technical standards on the global internet. For example, Brazil and India have often voiced intentions to develop their own Global South-to-South internet cables in protest of the US government's NSA surveillance scandals. However, when speaking specifically of the debates surrounding "internet freedom," this issue area remains explicitly under the sponsorship (and leadership) of advanced industrialized Western democracies.

The United States is the core global leader of this pack of states, and the United Kingdom and Germany are important international allies legitimizing the issue. Smaller states dependent on their high-tech industries (including Sweden, the Netherlands, and Ireland) have also pursued ambitious involvement in the US-led internet freedom work because their domestic economies rely heavily on exporting ICTs and infrastructure internationally, but often follow and borrow the agendas of internet freedom work promoted by the US. The membership of all these countries is

reflected in the pack of 21 states composing the Freedom Online Coalition (also led by the US), launched in The Hague during the immediate aftermath of the Arab Spring. So for the purposes of this investigation, when referring to and investigating state powers involved in promoting internet freedom, by "state actors" I refer specifically to those working for the interests of advanced industrialized Western democracies—unless explicitly noted otherwise.

The core norms that seem to dominate these states' perspectives when discussing internet freedom promotion includes focusing on defining digital infrastructure as referring to "critical infrastructure" wherein core concerns relate to protecting their nations' governmental communication systems from threats of cyber-terrorism and cybercrime, and specifically cyber-spying from hostile nations. This induces state actors to approach internet freedom promotion with the goal of regulating the export of technocratic expertise and digital technologies to hostile nations. They do this by supporting export controls on hardware and software for surveillance and censorship by technology companies based within their borders. A prominent example of this includes the case of Google's struggle in the Chinese market, where the search engine leader has relied on the US Department of State's support to negotiate terms of use involving the censoring of search content in China. Similarly, Canada's Research in Motion, which produces the popular Blackberry smart phone, has struggled with the governments of Saudi Arabia and the UAE to resist having to give access to its data servers to these nations with the possibility of political surveillance and censorship. State powers are very important in another way, because they are the key stakeholders opening doors to civil society leaders and digitally savvy political activists, inviting them to attend internet freedom forums. In other words, state actors are the key conveners of internet freedom arenas that bring together civil society and technology providers to the same table. Thus, clarifying the interactions and outcomes of the relationships between civil society and state actors is an important focus of this study.

Second, beyond state actors, the private sector, or ***technology providers***, is another core category of stakeholders involved in internet freedom promotion. These stakeholders are the high-tech sector of multinational corporations who innovate and implement digital infrastructure across the globe. They also have the core user base of millions of digital media users, which include the civil society actors who use these providers' digital infrastructures to engage in digital political communication and political organizing work. The norms that seem important to technology providers include concerns about losing valuable intellectual property rights when

they export their proprietary technologies and software outside of their home countries. For example, software companies that develop censorship tools to block pornography domestically face risks when they export these tools which are easily adapted in nondemocratic contexts to block political content. On the other hand, these stakeholders have also been complicit in these activities, particularly when their desire to enter profitable emerging markets requires them to provide such services to gain new customer bases. Because such exports have not clearly been defined as abuses of human rights, as is the case in exporting weapons, technology providers both benefit from and seek to clarify standards by which to shape their international activities.

When observing technology providers in internet freedom forums, their incentives to participate stem from public pressure exerted on them by digital activists documenting their involvement in human rights abuses. In other words, their incentive to join the tables set by state actors is primarily an outcome of public shaming and lobbying work done by civil society and human rights watchdogs—otherwise they have little incentive for pursuing internet freedom discussions. Technology providers rarely organize their own internet freedom events, but do cosponsor many for public relations purposes to exhibit their support for social responsibility concerns. For example, Google is an active financial supporter of several internet freedom policy conventions. Still, this stakeholder community cannot arrive at standards for regulating its own export of ICTs and technocratic services, and instead seems to be involved as a conditional outcome of the pressures they are facing from transnational civil society and digital activists. Civil society actors face a key challenge with this category of stakeholders because they lack the power to enforce norms and policies, unlike state powers.

Finally, the most dynamic and important community of stakeholders is the energetic technology-savvy transnational ***civil society*** activist network that has recently arrived on the international policy scene. These relatively new set of actors seem to have agitated rather recently, particularly during the aftermath of the Arab Spring protests. Earlier in this chapter I provided several narrative sketches and examples including the tactics of digital rights organizations like Access and the Electronic Frontier Foundation (EFF). Access was formed after the 2009 Green Revolution in Iran, while the EFF has a longer history in the Bay Area protecting US citizens' bill of rights in digital environments. But when dealing with internet freedom promotion, these stakeholders do not appear to be congregated in any particular nation-state, but rather seem to be constituted by a vast transnational network of issues-based experts

and political activists who have found digital rights to be an important domain for them to address. Their core norms seem to entail cultivating a public discussion around what are usually esoteric technical standards often negotiated between governments and corporations, but these new stakeholders want the public to recognize why these decisions are important and consequential to their civic lives. In the words one civil society activist, their core normative motivation is driven by questions like, "How do we make internet governance politics about ICANN and the ITU sexy and relevant to the Twitter activists in Riyadh?" (Interview in Stockholm, April 2012).

This stakeholder community of infrastructure activists is also the only set of actors attempting to inject the internet freedom discussion into the news agenda of international media and journalistic coverage. The common story, then, is that the Arab Spring seems to have given these civil society activists rich experiences and examples to raise awareness about esoteric infrastructure politics with the lay public. Furthermore, civil society actors also seem newly charged with advanced technical expertise about the inner workings of digital tools and infrastructure that is surprisingly sophisticated and unexpected. Where did they acquire such technocratic expertise and skills? Many notable civil society actors in this study are closely allied with digital hacktivists who leak internal memos and logs about the ways and instances when technology providers have knowingly assisted in the violation of human rights. This means that some sympathetic civil society actors are well-connected and have established ties in state-based and private sector agencies. Private sector and state-based actors are relatively straightforward in their motivations and norms, but the most interesting new ideas seem to emerge from these new civil society-based infrastructure activists. How did this happen? What are their particular norms and vested interests?

During the Arab Spring, for instance, several mobile technology providers, including the UK's Vodafone and Finland's Nokia were identified as providing authoritarian rulers assistance in identifying political dissidents with their equipment and expertise. Access, the activist civil society organization started in response to the 2009 Green Revolution in Iran, was behind several publicity and petition campaigns to rile up public pressure on the violating corporations. Although in studies of international politics civil society stakeholders are seen as traditionally weaker in comparison, in the internet freedom arenas, they are highly active, well-coordinated, and seem to be producing the most coherent articulations and evaluations about why internet

freedom matters. In other words, this stakeholder community is worth our attention because they are driving the normative agenda to meaningfully establish internet freedom frameworks to best serve the democratic interest of digital media users—not just the pragmatic interest of technology providers seeking to get out of their public relations failures. So if we want to see where the emerging norms and values that will matter for citizens are coming from, examining these activists and tech-savvy civil society stakeholders is a key space worth unpacking.

Network Ethnography of a Transnational Tech-Policy Community

This opening chapter (Chapter 1) has offered a starting point for investigating the complex issues and new categories of stakeholders surrounding internet freedom promotion. It has done so by outlining the recent history of transformative political change that has swept across the Arab world and also been observed in similar protests around the globe that have relied on digital technologies. I expanded on that point by bringing attention to the undergirding digital infrastructural conditions that have allowed these ICTs to be politically opportune, or risky, for democracy promoters in repressive political systems. As a consequence, several stakeholders have already recognized this scaffolding and its connected political economy and have increasingly agitated on the international level to debate the politics of digital infrastructure.

Since the Arab Spring, there have been at least ten prominent internet freedom conventions, as well as the launch of the Freedom Online Coalition—a pack of twenty-one mostly advanced democracies that want to support the advancement of internet freedom. However, this policy issue, while novel and important, has stagnated and become heavily gridlocked because different stakeholders have very different goals and interests. Therefore a coherent internet freedom regime has not yet been established. But these policy goals are worth pursuing because of the important ramifications digital infrastructure and ICTs are having on the welfare of users' human and political rights. To accomplish this, we must better understand who these stakeholders are, which norms they are promoting, and what avenues may best lead to a pragmatically and normatively viable internet freedom regime that can secure the needs of citizens.

To do so, the empirical framework for the rest of this study will be an adaptation of Howard's (2002) "network ethnography" research design for investigating hypermedia organizations and their collaborative practices used in the study of the US Presidential "e-

politics" network during the early 2000s. In this comparable study of digital infrastructures stakeholders and their efforts to govern similar internet technologies and consumer ICTs after the Arab Spring of the early 2010s, I update and extend the *network ethnography* framework by adding three analytical frames to guide this investigation. These core elements of this network ethnography include: a *network analysis* of the involved stakeholders' online social ties; an *participant observation* of a core email community of civil society activists generating the new norms focused on serving citizens; and an *event analysis* of a global communications treaty negotiation to test and observe these diverse stakeholders during a major policy negotiation.

These three combined analytical strategies, elaborated on in Chapter 2, allow us to identify and triangulate the core elements of the norms system that has emerged since the Arab Spring revolutions and the different communities of practice that now compete to shape internet freedom policy frameworks as they are being debated. Collectively, this implementation of this network ethnography research design allows for evaluating the capabilities of the infrastructure stakeholders promoting different and competing infrastructure policy norms. More importantly, these analytical frames allow me to substantively evaluate and address the guiding research questions defined previously (in section 1.3):

- Who are the new stakeholders and communities of practice involved in and being engaged to define the issues and contours of internet freedom policies? (Chapter 3)
- Of these various stakeholders and their constitutive communities or practice, from where are the most democratically-viable norms and frameworks originating? (Chapter 4)
- How coherent and coordinated are these democratically-oriented values being pursued when the stakeholders compete to establish concrete policies and treaties? Who are the most fickle, and most promising proponents of internet freedom, and why? (Chapter 5)
- Finally, what are the best prospects and new challenges that continue to face these stakeholders in better scoping this proto-regime to be more effective in promoting a democratically-oriented internet freedom policy agenda? (Chapter 6)

The benefit of adapting the network ethnography research design in this way is that it strikes a balance by beginning this empirical investigation with an ecological understanding of stakeholders through a network analysis and their trans-organizational relationships between different communities of practice (Chapter 3). It then more deeply investigates their practices through grounded observation (Chapter 4). Finally, the historical event analysis frame allows me

to complete the picture by testing my understanding of these stakeholders by observing and analyzing their activities and relationships in a temporally closed and self-reflexive system of practices that have already taken place in the "real world" of a major policy negotiation where the stakeholders and their behaviors have been made observable, documented, and discussed (Chapter 5).

Chapter 3 maps the global *stakeholder network* of actors, their social ties, and their institutional backgrounds, using data curated from actual stakeholder meetings from the proto-regime formation period. The data combines participant observation and interviews with participants' self-generated user-generated content and social ties reflected in their online social networking patterns. Existing literature in communication studies overwhelmingly focuses on the role of journalists in playing a watchdog role for publicizing the intricacies of complex bureaucratic and regulatory issues of public import on behalf of the public interest. But this chapter argues that these watchdogs are not the most important or even capable actors for addressing the esoteric issues related to global digital infrastructures. So Chapter 3 confronts this important anomaly and provides evidence to demonstrate that an entirely new cluster of actors coming from governmental agencies, technology companies, and human rights organizations are struggling to do this work, not journalists. Through this network analysis, Chapter 3 offers grounded categories and definitions to understand three key stakeholder communities currently pushing for different norms: 1) primarily advanced industrialized Western democratic state agencies, 2) multinational technology corporations that provide the hardware and software constituting digital infrastructure, and 3) technology-savvy human rights and civil society organizations being aided by sympathetic political hacktivists.

Chapter 4 extends the stakeholder analysis begun in Chapter 3 to directly observe the most novel and important category of stakeholders: political technology designers and hacktivists working on self-described "liberation technologies." These actors primarily represent the interests of civil society, but are importantly networked with all three stakeholder communities. They are important because they are generating the important new norms about digital infrastructures that are most relevant to citizens and users. Because these technology-savvy civil society experts exist as a transnational community of authoritative-knowledge producers, they share normative and principled beliefs about the political importance of digital technologies and are committed to promoting the democratic importance of their tools. They do

not yet have a fully coherent normative framework for what internet freedom promotion should be, but they are the key community most likely to generate the most interesting and impactful norms. Furthermore, because they are networked with state-agencies (through think tanks and policy experts) and technology providers (through their technical expertise and scientific backgrounds), they are also able to meaningfully consolidate different stakeholders' concerns related to internet freedom. In Chapter 4, I trace how since 2008 this community of experts has crowdsourced the social ties, curated the expert and experiential knowledge of technology designers and technology users, and monitored every major international event and scandal involving ICTs between 2008 and 2012. Chapter 4 also importantly points out that: 1) news media organizations and journalists critically depend on regular alerts from these experts to make sense of the complex violations of digital infrastructure by state powers (both democratic and authoritarian) and 2) state-based policy makers who have initiated the internet freedom stakeholder arenas also depend on these experts to help curate the esoteric and specialized knowledge necessary to design a more pragmatically viable set of definitions and norms for regulating digital infrastructure in the name of internet freedom.

Chapter 5 combines the lessons from Chapters 3 and 4 to test the capacities of various infrastructure stakeholders and their norms systems in a real-world scenario by unpacking the WCIT-12 treaty negotiations in Dubai, especially the least observable and understood: private sector stakeholders. The December 2012 gathering of the United Nations-sponsored ITU gathering, titled The World Conference on International Telecommunications is the most important field site for this investigation because it represents the first time in the past twenty-five years that nation states from around the world gathered to negotiate and update a major global communication treaty regime: the International Telecommunication Union (ITU). In this *event analysis* of the WCIT-12 proceedings, I evaluate the consistent ability (or lack thereof) of the different infrastructure stakeholders to effectively promote internet freedom norms at the international stage. More importantly, the controversies surrounding this event are necessary for understanding the underlying political economic tensions that guide our stakeholders' political ambitions and commitments. Doing so allows us to understand under what conditions, and why, certain stakeholders failed to promote internet freedom. This analysis also provides a valuable opportunity to test the influence of rogue nations that are not part of the internet freedom proto-

regime (i.e., authoritarian regimes), and possible members who might join if the internet freedom regime is constructed in a way that is relevant to their needs (i.e., developing countries).

Finally, Chapter 6 concludes the study by synthesizing the policy norms and frameworks that have been defined by these disparate infrastructure stakeholders and the current status of the internet freedom proto-regime. I argue in the conclusion that the stasis of the current proto-regime can be resolved by drawing in civil society actors through more formal inclusion, in contrast to existing attempts like Internet Governance Forum (IGF). This can be accomplished by redefining the stakeholder category of "civil society" to formally include the technology experts who have been evolving important new standards upon which this future regime may rest. Their normative standards, because they consistently maintain a normative focus on the democratic needs of users, can be promoted by narrowing the focus by anchoring the regime on these stakeholders. Mainly, the current proto-regime must excise certain norms areas that are less important to internet freedom as understood from a user's perspective, for example net neutrality standpoints that prioritize the private sector exclusively, or cyber terrorism concerns that speak exclusively to states' concerns. I provide examples of important prototypes of what these new nurturing spaces resemble in the aftermath of the 2013 NSA global surveillance scandals and the response from civil society stakeholders and organizations.

Chapter 2 – International Fieldwork and Data Collection

"The adaptation of institutions to rapid and unpredictable changes in their operational environments is perhaps the greatest challenge to communications policy today."

William Drake, Internet Governance Forum (September, 1988)

In the previous chapter (Chapter 1), I have outlined the investigative arc for this study, and justified doing so by reflecting on the recent activities in the international arena where several new categories of stakeholders have involved themselves with digital infrastructure policy issues. I also argued that we must understand how state powers, technology providers, and transnational civil society actors are all interacting with each other in the process of policy entrepreneurship surrounding but not limited to global telecommunications policy. The standard regimes of focus in existing approaches include the International Telecommunications Union (ITU) or the Internet Governance Forum (IGF). In contrast, the issues bringing together the stakeholders observed in this study relate to efforts attempting to establish an internet freedom regime best reflected, but not necessarily constituting, the emergence of the US-backed Freedom Online Coalition (FOC) after the Arab Spring.

Collectively, these predominantly Western states have pursued independent but coordinated activities to promote internet freedom by establishing new norms and policies for doing so, and more importantly drawn together stakeholders of different communities of practice. These new politics surrounding digital infrastructures do not resonate with the existing corpus of internet governance studies, and in fact there is evidence suggesting that these stakeholders' new challenges are importantly separate from the foci of existing telecommunications policy regimes. I have referred to these activities as constituting the emergence of a new *proto-regime* that has not effectively emerged, but is in the process of being defined and constructed by the involved stakeholders. So the challenge of this study is to find methodological avenues that can effectively access and observe the new intersections and phenomena connecting these actors.

There is a long precedent for studying multiple categories of stakeholders who are involved in the construction of communications policy regimes (Drake 1988). The established tradition from telecommunications policy studies does this by adopting the global "information" economy frame—i.e., the new transnational marketplace that has connected states and societies

through the joint processes of globalization, integration, and commercialization since as long ago as the 1970s. While this tradition focuses a great deal on the definitions of new policies and regulations that shape global communication systems (and the services which are operated upon them), there are also competing analytical models for studying telecommunications policy making that have been brought into discussion.

One important counter-perspective relevant to this study is the critical telecommunications policy tradition, which argues that the orthodox approach to studying globalization processes does not have much utility to explain the experiences of states and societies on the periphery of global communication systems—from where many of our effected political activists in the Arab Spring originate (Saleh 2010). In fact, these users embedded in peripheral developing economies and states constitute the majority of digitally mediated social experiences but tend to be the least examined and understood by standard scholarship concerning global telecommunications policy. The critical approach to telecommunications policy addresses this by focusing on the global economic dependence that less industrialized states and societies face in their experiences with globalization, but also tends to remain focused on the macroeconomic-level elite interactions and activities of governmental agencies and private corporations.

However, we must also include in this study the users and citizens as part of the stakeholders, in addition to the state and private sector stakeholders. Civil society organizations and actors have observably been organizing from the bottom up to affect global communications policy decisions, as seen during the Arab Spring. Furthermore, recent work focusing on the activities surrounding the IGF and the World Summits on the Information Society in Geneva and Tunis (WSIS 2003, 2005) all point to the increasing influence that civil society activists are having on internet governance politics (see: Servaes and Carpenter 2006). So in fact there is already an established scholarly tradition for studying lesser actors because these civil society and activist networks have been effective in organizing in peripheral but impactful ways to shape global telecommunications policymaking.

Still, neither the orthodox nor the critical approach has yet enlarged the domain of observable actors and stakeholders worthy of examination to include the kinds of digital activists and digital politics observed in Chapter 1. So the important focus of the kinds of politics and actors discussed in this study must push further towards the periphery of most internet

governance investigations, and certainly outside the standard focus on state powers and private companies exclusively. How might we approach this arena of policy making that is taking place across knowledge communities and stakeholder categories?

This investigative demand poses some important empirical contexts and methodological challenges that need to be reconciled. First, standard methodological approaches to studying telecommunications policy often take one of three analytical orientations: 1) those narrowly focused on defining legal perspectives about regulations and policies that only legal experts can contribute to; 2) those too focused on elite sectors like governmental agencies, but tends to reflect only the experiences of a miniscule set of privileged elite stakeholders; or 3) those broadly focused on measuring the levels of public interest and understanding of regulatory issues. For this study we need a purpose-built analytical approach that is neither *organizationally deterministic* in constraining the range of stakeholders and actors to be observed to the established elite stakeholders (states or corporations) that are traditionally examined, nor too *technologically deterministic* in limiting the types of data required to more fully understand a complex multi-stakeholder ecology. The kinds of social interactions featured in this study could also be described as an "ecology of games" (Dutton 1995)—intersecting arenas where different actors, publics, and organizations from sometimes altogether different industries meet in purposeful arenas (e.g., internet freedom summits) but pursue their self-interests whilst using different tactics to convince other stakeholders to fall in line. Additionally, the kinds of organizational flows observed in this study are more fluid, and defined as "hypermedia organizations" where actors and stakeholders are not only connected loosely but often move around from one organization to another, switching stakeholder categories and cross-pollinate in different communities of practice.

For all these reasons, the *network ethnography* approach is well-suited analytically towards the environmental conditions and requirements for aggregating and synthesizing evidence from different levels of activities and kinds of stakeholders (Howard 2002). Network ethnography, as I will discuss in the following section, strikes a balance between the organizational determinism of the ecology of games approach, and the technological determinism of standard data collection strategies. Network ethnography can also be effectively applied to investigate the transnational network of infrastructure stakeholders and norm makers engaged in internet freedom related policy entrepreneurship both peripherally and centrally.

2.1 Ethnography of Stakeholders

Network ethnography is an analytical strategy that combines an ethnographic understanding of complex social phenomena with an ecological (i.e., social network) understanding of different stakeholders' positioning and relationships amongst each other (Howard 2002). This particular approach is especially well-suited for this study because the social actors being observed are connected to each other due to the shared issues and challenges that force them to intersect, and particularly because their interactions are being facilitated by the arenas that have been set-up to bring them together by Western states responding to the Arab Spring crises. So although the observed stakeholders are positioned in different countries and industries, they are being drawn into a common space by a shared problem: deciding on strategies and policies to defend digital infrastructures in the democratic interest (although different stakeholders will decide what these mean based on whose interests and demands they have in mind).

The network ethnography approach also works to describe human behavior systematically within the context of different organizational cultures. Thus, the "data" required for doing so is collected through first-hand observation, and because of the different ways that these communities are structured, I adapt the approach contextually to the environments I am immersed in—which includes, in particular, web-based communications and online organizing activities. So how did I decide on what data to collect and where to collect it from? One strategy for deciding this is being open about where the interesting phenomena are observable to begin with. For example, a broad and multi-stakeholder phenomenon like internet freedom policy entrepreneurship seems to increasingly resonate with communities of practice that are decentralized—a direct effect of the type of communicative spaces where internet freedom issues are often voiced and deliberated on (i.e., in specialized email lists, activist networks, etc.). The consequence of this is that the social phenomena of interest exists "offline" when social actors meet and interact in person, but also "virtually" when they stay connected through mediated technologies and digital environments, identify joint challenges, and decide to organize offline to more substantively engage with their concerns.

So, for this investigation, I began the research design by appreciating that the modern organizational structure relevant to internet freedom discussions was both hybrid in nature (i.e., hyper-mediated) and consequently decentralized. In other words, these communities and their efforts are socio-technically determined. And because of this important characteristic, I was

careful not to make methodological choices at the outset that were organizationally deterministic, or technologically deterministic in nature. What do these unique forms of determinism mean, and how might they manifest in research practices?

Firstly, *organizational determinism* refers to the risk that a researcher faces when trying to impute a community or actor's culture or norms from the formal hierarchies present in its encasing organization. In the context of this study, organizational determinism could take place if I, the researcher, were to categorize a stakeholder with a label based solely on the legal definition of that actor's professional or public identity—and remained agnostic to the reality that employment, like identities, change over the life-course of the study. For example, a computer engineer working for a private technology security firm could be categorized as a private sector stakeholder because she was employed by a for-profit technology company. However, as is often the case in this internet freedom policy entrepreneurship, several such engineers also shared underlying ideological (i.e., political) allegiances for open-source technologies and worked as hacktivists in their off hours. So in fact, individuals like this should not be categorized only according to their public occupational labels. Therefore, triangulating in-person interviews, observing them during conferences (as well as what they were saying on social media and email discussion networks), and observing their social ties was a necessary process throughout the ethnographic fieldwork. Doing so allowed for gradations and more granular determinations of how embedded some actors were to different communities of practice or formal organizations.

Second, this investigation also faced the risk of *technological determinism* when I tried to impute a stakeholder community's culture based only on its online activities (a technologically determined limitation of what I could observe), especially in cases where most of the important activities took place online. For example, when studying an important online discussion community which was behind the political tools being created and tested by activists, in addition to conducting interviews, I was required to attend their actual design meetings. Sometimes, because some projects were entirely "cloud-based" (i.e., all of the collaboration took place digitally without direct offline interaction) I reflected on the public transcripts of communication exchanged between actors throughout the development and deployment of their toolkits. This was sometimes easier than expected, because email discussion communities had automatic archives (which were also indexed by popular search engines, like Google—helping to

improving data completion and depth of observational data), and provided intimate details such as the time of the discussion, the identity of the discussant, and their contact information, useful for asking follow-up questions or setting up interviews.

In other cases, when I would find certain actors' social media pages or personal web pages, I incorporated those details as well. For instance, some members of the online discussion community, such as a Scandinavian hacktivist I met through fieldwork who also worked in a European research lab would appear as an organizer for state-sponsored internet freedom summits, whilst holding cyber-libertarian views against state involvement in the management of digital infrastructure. In this case, I was able to identify this apparent anomaly through participant observation and triangulation of that individual's online discussion content, and confirm her activities with face-to-face interviews. Through combined online and offline participant observation, and follow-up interviews, I was able to ascertain that in this case, the hacktivist's intention to facilitate state-backed internet freedom stakeholder gatherings was to help subversively populate the discussion with cyber libertarian-friendly experts espousing those norms and values—a tactic to introduce anti-statist culture into a state-initiated project.

Framework and Sampling

In the previous section, I discussed and provided some examples of how network ethnography is a useful approach for helping curb both *organizational* and *technological* determinism. Network ethnography also provided me with useful strategies for purposefully sampling actors and arenas when the organizational environment seemingly lacked a concrete organizational structure. Here, I used the organizational content and technical structure of a core network of actors as an initial sampling framework, and then branched out by snowballing and digging more deeply into certain networks or spaces. By "digging more deeply" I mean enriching some seemingly banal information about aggregated social media ties by adding more in-depth interviews, and tracing connected discussion environments in virtual spaces that helped give meaning and facilitate deeper understanding.

For example, in practice, I aggregated all of the social media ties available on Twitter's API[8] of the ten internet freedom stakeholder meetings that I had already identified. This social

[8] API stands for "application programming interface" which refers to a common platform created by web developers to access their servers automatically to access certain information. In the case of Twitter's

network database provided social tie information which I was able to use to run community detection algorithms to identify clusters of actors based on network centrality computations via NodeXL[9]. Based on their purely computational structure determined by the relationships between nodes and edges, I was able impute with a several network clusters too improbable to be random (Tyler, Wilkinson, and Huberman 2003). But understanding and explaining *why* required that I look at both the content of the sub-clusters and the personal histories and practices of those constituting the nodes (i.e., stakeholder actors) (Stommel and Koole 2010). I did so by establishing formal codes to categories stakeholders and then applied those codes to the network maps to see which clusters different stakeholders tended to congregate more or less in. Once certain sub-clusters were identified as being dominated by one or a few sets of stakeholders, I pursued interviews with key gatekeepers to different network clusters to determine the purpose, identities, and cultures of the different network clusters[10] that had appeared.

So network ethnography provided me with a guided and (re-)traceable framework for strategically sampling and digging deeply into important communities of practice that lacked formal organizational structures. For example, by following a snowball sample of technologists I had built relationships with at the MIT Civic Media Lab in a Boston "hackathon" gathering, I was able to make use of that social capital and gain entry into a connected hackathon that took place four months later in Bizerte (Tunisia). Because several participants in the Tunisian hackathon were connected to and collaborating with the Boston-based hacktivists, this social capital served as a lubricant to enter a new community of practice that was important for my investigation but would have been impossible to do so without the help of field informants originating from this peripherally connected community.

In fact, these examples abound and also further illustrate another key feature of network ethnography: the ability to directionally impute the transfer of knowledge and practices as

---

API, the module allows common marketing research toolkits the possibility to access its servers to collect web analytics about users, their activity frequencies, profile information, and social ties.

[9] NodeXL is an open-source network analysis and visualization package for Microsofr Excel created by the Social Media Research Foundation. All information regarding computation algorithms and community detection algorithms can be found directly on the NodeXL CodePlex, here: nodexl.codeplex.com.

[10] Broadly, this was the analytical strategy used to identify the state-based cluster of norms being cultivated in the London Agenda and the civil society-sponsored cluster of norms being promulgated by the Silicon Valley Standard that I will discuss in Chapter 3.

originating from one community of practice and being transferred to and modified by another. In the same example, the individuals and their norms from Boston were being exported to Tunisia, and I determined this by following the transfer of practices myself and observed the exchange of field lessons regarding specific technology-in-use case studies that participants were deliberating on. For example, all the attendees from Boston were treated as elite organizational leaders in Tunisia, whereas the Tunisian participants did not enjoy equal status in Boston. Furthermore, specific vocabularies used in this community of practice, like "civic hacking" and the strategies being taught, like visualizing city-level budget data to identify local and national-level bribery, were being exported by past experiments conducted in San Francisco—something I observed directly by observing and interviewing the social actors transferring knowledge uni-directionally. In other words, the network ethnography approach told me not only what was happening, but also what had happened and how this community had come to be.

Separately, the sampling and community-tracing approach in network ethnography is especially powerful for outlining fields of activities in complex communities with different spaces that have incubated distinct practices, as was the case in this study. For example, I began the study by identifying all the events fitting my topical interest that took place between two important historical moments to establish broad "historical" boundary conditions for the overarching investigation about internet freedom policy entrepreneurship after the Arab Spring. Those boundary conditions were *the end of the Arab Spring* (June 2011) and *the WCIT-12 meeting in Dubai* (December 2012) as an endpoint for the network ethnography. But this was not clear when I began fieldwork (February 2012) that December 2012 in Dubai would be the conclusion of the study. More importantly, it was *through* fieldwork and tracing different actors that I began to learn of the importance of the WCIT meeting in Dubai for most of the involved stakeholders. Particularly, WCIT reflected the first time in a quarter century that the UN was meeting to redefine global telecommunications policy. So it was the field informants themselves that helped identify a major event that produced a logical conclusion of the study because of its analytical utility in testing and observing ideas about how internet freedom promotion was being defined, and practiced.

To restate the boundary conditions of this study, the first step for this study was to identify all of the major meetings that took place and were sponsored by, or took place in, Western democratic regimes since June 2011 (the end of the Arab Spring protests), and during

the fieldwork I determined to conclude the investigation in December 2012 because it provided a conceptually appropriate endpoint to reflect on the effectiveness of internet freedom work since the Arab Spring. Specifically, these boundary conditions were set through a three-step determination. *First*, I mimicked the process that a civil society stakeholder would have followed—by searching for information online and asking individuals in the network for guidance. This required that I actively sought out information on Google, Bing, and Yahoo! (collectively the most popular search engines) with the query "[internet freedom] AND [meeting OR summit OR conference OR convention]." When required, after identifying the FOC and its list of member states, I would add "[country name]" to the Boolean search, to find country-specific meetings, if there were any taking place in FOC member states. Throughout the fieldwork period, I updated[11] my database of events once every month between January 2012 and December 2012, while also staying tuned to my network of activists, the blogs I was following that they authored, and the Twitter handles they were maintaining, for any breaking news or updates concerning new meetings that might have been announced.

The *second* step, to triangulate and identify all internet freedom stakeholder meetings, was to archive and digest the information available on the identified events' Web pages. I did this because each meeting seemed importantly connected to the other gatherings I had discovered, and the web content seemed to indicate a very important fact: many events routinely referenced each other's activities and ongoing progress (though they were organized independently). For example, the Stockholm Internet Forum made explicit mention to the London Cyber Conference and the FOC in The Hague from previous months, and the organizing committee stated explicitly their intentions to "continue the work" started in these separate meetings to promote internet freedom. This further corroborated my understanding that although the internet freedom proto-regime does not have a formal organization, the activities surrounding it by involved stakeholders proves proto-regime in formation because of coordinated and self-aware progress that disparate states and stakeholders were promoting through coordinated meetings and joint and shared norm-setting goals. As yet another method to triangulate and identify all the public meetings that may have been part of the proto-regime, I also inquired directly with meeting organizers for similar examples by writing to them directly, having field

[11] This is the monitoring system that allowed me to identify WCIT in Dubai as a key moment for this proto-regime.

informants help by introducing me through their trusted relationships, or by posing questions to their community email lists whenever possible. These strategies helped to identify the full range of meetings and "field sites" that were at least publicly known, both by search engine archives, and organizing and attending participants. These direct inquiries also helped me to establish trust and rapport so that I could exchange this social currency later on to gain access to key stakeholder meetings. For instance, as I reference in Chapter 5, I was able to gain invitation and travel support to stakeholder meetings in Stockholm, Berlin, Toronto, Doha, and other stakeholder meeting grounds. I did this by establishing rapport and trust with members' state-based agencies (e.g., US Department of State) and civil society organizations (e.g., Access) by serving as a an active participant-observer in their meetings and activities, providing reports and offering intellectual labor in exchange for access and participation.

Third, after identifying and exhausting the field sites of internet freedom-related stakeholder meetings, I needed to identify as many of the actors and participants who were part of the proto-regime formation effort. To do so, I used a snowball method to extend the range and access to involved stakeholders and actors by curating the attendee lists on all event pages and portals. This was done in two steps. I began by archiving the web content of internet freedom stakeholder meetings. In each of these stakeholder meetings, organizing members and attending members were listed by name and organizational home. For example, an attendee representing Facebook's policy team would be listed by name, as well as the organization she represented at the meeting (e.g., Jane Smith, Facebook). For each meeting, whenever available, I collected and tabulated the attendees by name and affiliation. This gave me important details, such as how many broad stakeholders by category were in attendance. This helped to define and categorize *private*, *governmental*, and *civil society* actors as three important grounded stakeholder communities.

After archiving the attendee lists and processing their categories, I needed to trace the identified participants' social media ties (whenever available). I did this by identifying their email addresses, Twitter accounts, and Web page information. This step helped to provide access to the virtual spaces where their activities and interactions extended. For example, each internet freedom stakeholder meeting had an official Twitter hashtag that was generated by the conference organizers to facilitate online discussions live during stakeholder meetings. In my field observations, civil society stakeholders made the most energetic use of this to engage with

and sometimes prod other unwilling stakeholders into conversation. An example of this was when the Swedish Foreign Minister was shamed by attending Syrian activists at the Stockholm Internet Forum on Twitter during his live televised welcoming speech because TeliaSonera (a Nordic telecommunications agency) was caught providing hardware tools to repressive rulers the morning of the launch of the Stockholm Internet Forum. These interactions taking place online were valuable to me as a researcher because on Twitter their follower/following relationships were made transparent and their biographical information made publically accessible. By combining and aggregating that information through Twitter's API-based social network data, I collected and categorized different connected actors based on national, stakeholder, and organizational categories. Similarly, this technique of tracing proto-regime actor's digital media presence also allowed me to identify the LiberationTech email discussion community as an important sub-community that was home to many of the digital activists attending several internet freedom meetings. The LiberationTech email community served as an important peripheral community of practice in this study, discussed in more detail in Chapter 4.

Research Sites and Actors

Network ethnography is more than a framework and sampling technique that allows me to avoid organizational and technological determinism when studying loosely connected and hyper-mediated communities of practice (Howard 2002). It is also an empirical approach that allows deeper access to elite and perhaps insular institutions often examined in international relations and studies of regime formation. Recent work in political science has incorporated communities of practice (COP) as an effective method to examine formal treaty organizations, like the North Atlantic Treaty Organization's reformation period during the 1990s following the dissolution of the Soviet Union (Adler 2008). The analytical utility of COPs is demonstrated here in their ability to bring together groups of policy practitioners of various security communities during the Helsinki Process and the Post-Cold War transformation of Western European and North American alliances. Furthermore, Adler makes use of the COP framework to identify how: 1) actors with symbolic power and cognitive authority endowed material objects with newly legitimated social meanings; 2) how these new meanings were translated into practices by dominant institutions; and 3) how these COPs were effective in reaching a "tipping point" and expanding their new definitions and practices into an effective international regime.

Moreover, in discourse studies, the COP concept is also being applied to new sites of social interactions, like digitally-mediated environments. Stommel and Koole (2010) study an online support group as a community of practice and conduct a qualitative conversation analysis of email interactions between group members to describe how that community engages, incorporates, and eventually molds new members. Advances in organizational communication have also produced computational network analysis strategies for identifying communities of practice using the digital meta-data traces left by users and participants' profile information and communication habits (Tyler, Wilkinson, and Huberman 2003). I combine these strategies of micro-interaction analysis and computational network analysis to study the peripheral participation of internet freedom stakeholders as they have engaged in constructing a proto-international regime. In the following discussion I expand on the three phases of data collection over the twelve-month period of international fieldwork for this study, and the underlying logic that guided those decisions, particularly in identifying research sites and working with actors in the field.

In the *first phase*, I began data collection in January 2012. This phase took place over three months, between January and March, and focused on identifying the meeting places where activists and stakeholders were gathering physically to discuss internet freedom. This was done through a three-step method to triangulate the search for meeting places (systematic online search, archival web content, and engaging field informants), many of which at that time had not been announced so had to be routinely conducted alongside fieldwork. Through the registries of attendants listed in previous events, I became aware that this was not the standard circuit of internet governance stakeholders that tend to attend ITU, IGF, or WSIS gatherings. Notably, many of the interesting civil society activists belonged to political movements and anti-censorship projects active during the Arab Spring. So this was not a gathering to bring together internet governance stakeholders (e.g., states and corporations); it was a meeting of users and activists who had come to care politically about internet governance!

Therefore, it was important for me to learn more about these tech-savvy political activists who were different from the elite actors often examined in internet governance literature. Because I had budgeted 12 months for field immersion with the understanding that this was a transnational case study of ongoing events, my ethnographic and data collection required that I travel to locations and meeting points where tech-savvy activists were meeting or originating

from. For this reason, after identifying some major internet freedom stakeholder gatherings, I began by relocating to the effected political zones where some of the indigenous Arab Spring tech-savvy activists present at elite meetings were arriving from. The burning question that served to start my ethnographic work was: "Who are these new activist stakeholders at elite meetings about internet freedom, and where are they coming from?" This question encouraged me to begin the second phase of the fieldwork, which required moving to the Middle East and North Africa.

In this *second phase*, after first identifying and tracking the meetings and actors who were revolving around several internet freedom gatherings, I relocated from Seattle to the Beirut and Tunis between the months of March and June. During this period, I split my time traveling and interviewing between Beirut, Lebanon, and Tunis, Tunisia, for two different reasons. Both were locations that I used as base camps from which to travel to neighboring countries to meet with journalists, fixers, and activists who were still active in post-revolution organizing after the Arab Spring. But I selected Beirut as a starting point, because it is home to a critical mass of political activists and political analysts interested in Arab politics. At the time, given the civil war that Syria was engaged in (which is still ongoing as of this writing), Beirut positioned me strategically within thirty to fifty kilometers of the border where the fixers and activists from Syria's protests were actively smuggling digital content to Western journalists and media outlets. If I wanted to observe tech-savvy activism in contentious conditions, Beirut was a live site for these activities.

During my time in Beirut, the American University of Beirut (AUB), the Lebanese American University (LAU), and the United Nations Economic and Social Commission of Western Asia (ESCWA) provided research spaces and assistance in networking with experts and activists for my fieldwork and interviews. The interviews and observations made in the Beirut (the Levant region) of the Arab Spring were notably more pessimistic and the experiences of the activists I interviewed were more dangerous given the severity of the local events. This exposed me to the understandings and concerns of activists who were using digital media technologies under considerably risky circumstances.

After concluding interviews in Beirut, I relocated to Tunis for access to a separate set of experiences in contrast to Beirut. In Tunisia (the Maghreb region), where the Arab Spring was sparked, my field work and interviews suggested a clear contrast to the experiences I collected in

the Levantian region. Simply put, the Maghrebi experiences of digital activists were far more optimistic, perhaps because the regime repression there was far less violent and therefore less risky. Exactly why is not the central focus of this study, but Tunisia provided an important case to extend the coverage of experiences related to tech-savvy political activism in a recently "successful" and optimistic Arab Spring case. During my time in Tunisia, the National Democratic Institute (NDI), the National School of Communications in Tunis (SUPCOM), and I-Watch provided valuable field contacts and access to local projects where digital activists were employed. Furthermore, I decided to reside in Ariana, a neighborhood bordering SUPCOM where I was able to obtain residence with a commune of political hacktivists active during and since the Tunisian revolution. These young activists allowed me access to their direct experiences, ongoing strategizing, and even their gigabytes of hard drive content, all of which exposed me very intimately to a different narrative and notably more efficacious attitude towards digital activism than what I had observed in the Levant. Rather than pontificating between cyber utopian and cyber pessimistic opinion editorials, these activists and their real experiences grounded my fieldwork data rich evidence indicating causal complexity with regards to internet freedom and digital mobilizing.

During my time with immersed in fieldwork with Arab digital activists, I systematically maintained contacts with a different set of elite transnational activist I had met while at Harvard's Berkman Center for Internet and Society and MIT's Civic Media Lab in February just before relocating to the Arab world. These elite transnational activists were helping me broker contacts and interviews with the local activist sites in the Arab world. Sometimes, I would meet both elite and indigenous activists in person, for example during meetings called "civic hackathons" held locally both in Beirut and Tunis. Here the indigenous activists would take charge of sponsoring and organizing the meetings, and the transnational activists would fly in from Western Europe and North America as consultants, sponsors, and speakers to share tactics and tricks of their trade. The directional flow of practices and norms between these actors seemed to be "abroad" towards the meetings revolving around internet freedom promotion that I had begun tracking before leaving Seattle. In other words, the local activists were constantly looking outwards at the meetings sponsored by Western democracies taking place outside the Arab world, and were struggling to gain access to such meetings. The transnational activists who tended to have easier access to these meetings were also looking in this direction, towards the

stakeholder meetings happening in Western Europe and North America about internet freedom, and working to get there themselves. However, the local activists in Tunis and Beirut often did not have the funds to afford flights, hotels, and the political capital to easily obtain visas and travel permits to leave their countries. So there was ample reason for me to begin moving in the direction that both elite transnational activists and local indigenous activists where vying to go: towards the internet freedom stakeholder meetings sponsored by Western democracies.

This began my *third phase* of data collection after field immersion in the Arab world. It seemed that all of the important meetings, discussions, and decisions about how to promote internet freedom were happening "abroad" over there (see Table 1). So between the months of July and December, I spent three months in Sweden and three months in Switzerland focusing concertedly on gaining access to and conducting interviews with state-based policy makers and technology sector advisers based in Zurich, Stockholm, Amsterdam, and London.

In Sweden, the Jonkoping International Business School and the Media Management and Transformation Centre served as host sites while I collected my data and conducted interviews with these elite stakeholders. I was also able to attend several of the internet freedom meetings personally because they were far more accessible geographically. It was also during my stay in Sweden that I began collecting Twitter API data and aggregated all of the internet freedom meetings that had taken place since the Arab Spring. This data provided social network information, personal identities, and autobiographical details about who the attending and interested individuals and organizations were that had followed or tuned in to the discussions about those meetings on Twitter.

When I relocated to Zurich in October, the Swiss Federal Institute of Technology (ETH) and the University of Zurich (UZH) and their associated Centre for Comparative and International Studies, and the Media Change and Innovation Division provided valuable research space and computational infrastructure to continue the social media data collection I began in Sweden (while continuing to attend meetings and conduct interviews with participants). Namely, I used the NodeXL toolkit developed by computational sociologists at Microsoft Research. This toolkit and a National Science Foundation training fellowship in the summer of 2012 in Washington DC equipped me with the methodological tools to run community detection algorithms on my Twitter database of internet freedom stakeholder meetings.

During this third phase of international fieldwork, in addition to the face-to-face interviews and meetings conducted with individuals identified in stakeholder gatherings, I also assembled lists of attendee's names, ranks, and affiliations by collecting the event attendee registries made available by the organizer's either online with the public, shared in print during stakeholder gatherings, or both. Using this aggregate information, I prioritized my networking activities to seek out interviews not only with the keynote speakers, but also the discussion moderators and side-event organizers. This ensured that I was expanding my range of observations to include the important architects of these negotiations, not simply the talking-head figures and official spokespeople.

It was also during my time extending fieldwork into Western Europe that my interviewees and connected activists from the Arab World began agitating about an upcoming telecommunications conference in Dubai (UAE) in the final two weeks of December 2012. While I was scheduled to return to the US, the amount of tension and the long period (almost six months) of organizing for the ITU meeting in Dubai provided sufficient reason to extend my stay by one extra week. During this week, I attended the WCIT gathering in Dubai, although I did not have official sponsorship or permission. This in fact served surprisingly well for providing interview material, because as it turned out, none of the civil society contacts I was intent on meeting were provided access either[12]. During this fortuitous week of fieldwork in Dubai, I served as participant-observer and worked hands-on with members of Access, the Center for Democracy and Technology, and other civil society organizations. During this fieldwork, because I was relatively free of major responsibilities, I was asked to provide communications help by networking other activists who were not there physically. This active role as a participant-observer gave me privileged access to the chat information and organizational discussions that civil society members were having about state-based and private sector stakeholders who did have exclusive access to and attended the delegations.

So in summary, the network ethnography and field immersion for this study took place over twelve months of data collection, of which four months were spent in the Arab World and six in Western Europe. Throughout this, I interviewed sixty-eight key informants who held positions as executives, directors, managers, and cofounders of activism organizations, technology companies, and governmental agencies (see Figure 1 and Table 2). These three

[12] I explain how, and why this is crucial in Chapter 5

phases of international fieldwork (in North America, the Arab World, and Western Europe) allowed me to amass a rich and purposive collection of evidence reflective of the different sites where stakeholder activities were being conducted as internet freedom issues evolved.

Throughout each meeting that took place, I also collected evidence and archives of information 1) during the live discussions and debates of the stakeholder gatherings, 2) from their extending virtual activities that were taking place online in email discussion lists and on social media platforms, and 3) from the official policy documents and frameworks that were frequently produced by meeting organizers in the aftermath of the meetings to share with the participants and interested public summarizing the norms established during these gatherings. In the following chapters of this study (Chapters 3, 4, 5, and 6) I make use of different portions of these data sources to empirically assess each chapter's core research questions and themes. In the remaining discussion of this this chapter, I provide chapter-specific details about how each chapter and its corroborating analytical frame approached and utilized different pieces of the data amassed through twelve months of international fieldwork constituting this network ethnography.

Figure 1: Tag Cloud of Interviewee Positions

Note: Tag cloud created with Wordle.net based on sixty-eight informants interviewed between March 2011 and December 2012.

Table 2: Examples of US and Non-US-based Organizations of Interviewees

US-based Organizations:	**Non-US Organizations:**
Access	Association for Freedom of Thought and Expression (Egypt)
Brookings Institution	Center for Enlightenment and Human Development (Sudan)
Center for Democracy and Technology	Center for Technology and Society (Brazil)
Facebook	Federal Ministry for Economic Cooperation and Development (Germany)
Ford Foundation	Supreme Council of Information and Communication Technology (Qatar)
Freedom House	Institute for Contemporary Observation (China)
Global Network Initiative	International Federation for Human Rights (France)
Google	Software Freedom Law Centre (India)
National Democratic Institute	Swedish International Development Association (Sweden)
New America Foundation	Syrian Center for Political and Strategic Studies (Syria)
RAND Corporation	Tunisian Internet Agency (Tunisia)
US Department of State	Foreign and Commonwealth Office (UK)

Note: List of examples is non-exhaustive, and inter-organizational units and individual names and positions are not included to mask identities of informants and interviewees.

2.2 Analysis of Data

The preceding discussion has provided the methodological approach for collecting data, and the system I used to identify field sites for immersion (offline and online) and tracing the diffusion of norms across different stakeholder communities. In the remaining discussion I will now provide specific information about how the twelve months of data were aggregated and analyzed to address the core research questions and thematic concerns of the following chapters. In Chapter 3 I present a *network analysis* to establish stakeholder definitions and examine their norms being propagated at internet freedom stakeholder meetings. In Chapter 4 I trace a peripheral but important online *community of practice* that is rooted in transnational civil society and is connected to a group of core political technologists. In Chapter 5, I conduct an *event history analysis* to understand how an important policy regime was organized and its surrounding conflicts and contentions between stakeholder groups, particularly the private sector providing technologies and components of digital infrastructures. These three analytical chapters required different types of data and analysis to furnish supporting evidence; therefore in the next discussion sections I explain how this was accomplished for each chapter through data collected from international fieldwork.

Social Network Analysis: Stakeholder Social Media Ties (2011 to 2012)

Data for Chapter 3 covered nine[13] out of the ten major internet freedom summits that have been organized between 2011-2012 (see Table 1). The main concern of Chapter 3 was establishing stakeholder categories and definitions and observing how these stakeholders are connected in relation to each other. This required four steps to produce the appropriate evidence.

First, I devised a method by which to identify the broad transnational network of stakeholders located intra-organizationally across stakeholder categories. To do so, I turned to the social graphs that were created during each stakeholder summit by the participants and organizers themselves through their social media networking practices. Twitter is an important industry platform where professionals from all sectors meet to extend their professional strong and weak ties (by following each other based on mutual interest or personal meetings). My

[13] The Council of Europe's "Our Internet – Our Rights – Our Freedoms" summit in November 2011, that took place in Vienna, was the only gathering that was not curated officially on Twitter. All remaining nine out of ten gatherings were also curated during and after the summits to help attendees and the interested public by the event organizers.

strategy here was to identify and combine their Twitter social graphs into a "meta-social graph" (see Figure 2) combining the nine[14] event-based Twitter social networks that had been curated by the organizers of each stakeholder summit. I collected these data in late October 2012, after the conclusion of the final stakeholder meeting covered in the fieldwork period (in September 2012). I also collected all nine graphs in the same, final week of October 2012 because it provided enough time (one month) for the final event in the series of summits to fully conclude and stakeholder networking activities to subside.

The software package used was NodeXL, which has a built-in automated import mechanism to collect between one and three degrees of social network data directly from Twitter's API. This process works by starting with one seed account (in this case, the meeting's official Twitter handle), and then crawls the followers of the seed account, and then extending the crawl to follow the follower's followers. Doing so allowed me to identify and isolate only the bidirectional social ties seeded from the main Twitter account. Thus, the population was snowball-sampled outward to identify those that had officially followed that meeting's account and those connected to them. Isolating only bidirectional ties further refined the validity of the data by examining dyads of actors who, out of their own agency and self-interest, found it meaningful to follow each other, independently.

To illustrate, if John Smith (a digital activist) was following the State Department's internet freedom meeting account, it is likely that John Smith had an interest in internet freedom or the State Department, or both. But sometimes, as is common on social media platforms, John Smith could be a "spam-bot"[15] or an inquisitive internet user who happened to follow the meeting account less purposefully. This is why I followed Jane Doe, who was also following John Smith, and whom John Smith was following in return (i.e., they were bi-directional ties, and reduces the likelihood that a purposeful user would return-follow a spam-bot). The probability that John and Jane were following each other mutually and unintentionally, and were connected within one degree of separation to a major internet freedom stakeholder gathering,

[14] Access and the FOC each organized two conferences, one in 2011, and one in 2012, so the Twitter handles representing their events are the same (presumably done by the organizers to maintain the social network they had curated from the previous gatherings). Therefore, although there are nine events that were covered on Twitter, they are contained in seven social graphs.

[15] It is estimated that Bot traffic has grown 30 percent in 2013, and may account for 40-60 percent of all web traffic: http://techcrunch.com/2014/03/05/mobile-bot-traffic-reportedly-grew-30-in-2013/

was quite unlikely, and therefore provided a validity check and increased the threshold for being included in the social network analysis. In other words, the social network ties examined in Chapter 3 refer only to the bidirectional ties identified surrounding the nine out of ten internet freedom stakeholder meetings—an exhausting and demanding data quality criteria.

Then, I aggregated all nine social graphs together to construct one large meta-graph (see Figure 2). After constructing the meta-graph, I double-checked the Twitter IDs I had collected during the fieldwork from the meeting's official attendee lists to see if they were included in my graph, and for all nine meetings the percent of Twitter IDs was greater than 70 percent. In other words, seven out of ten participants in the "live" meeting with Twitter IDs were present in my meta-graph—this indicates that I had good coverage of "real" stakeholders in my social media network meta-graph. The stakeholder network's meta-social graph therefore represents the combined network of stakeholders that had tuned in to and voluntarily formed ties with other stakeholders over the past twelve months of internet freedom stakeholder networking.

An additional characteristic of this meta-social graph is that if particular stakeholders were present in more than one event, collapsing these layers together preserved their multiple ties created in more than one event. In other words, if actor "Bob" attended the meeting in Layer 1 and Layer 3, and Bob's friend "Jen" did the same, then the ties between Bob and Jen were duplicated, indicating Bob and Jen's doubly present importance reflected in their having attended two discrete stakeholder events and having maintained bidirectional ties at both events. By stitching these layers of different meeting together, what results is the composite sketch of all sub-networks cultivated during each stakeholder gathering with respect to how central and engaged different actors were in the internet freedom summits and online discussions.

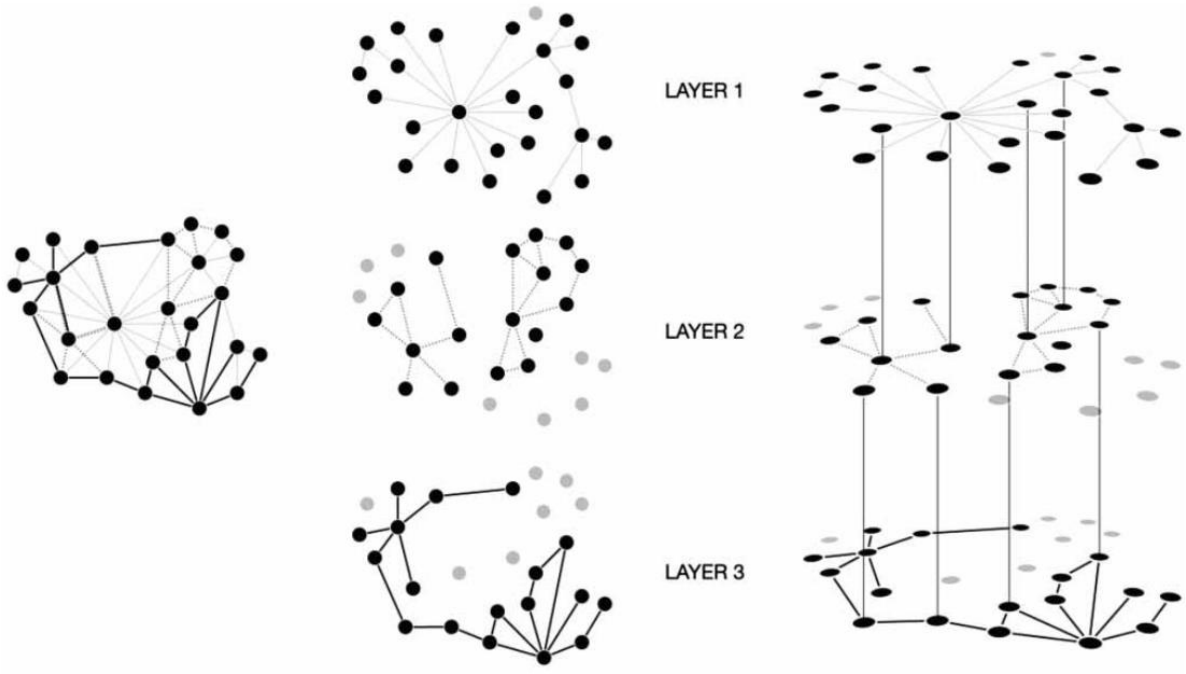
After producing the meta-social graph, the second step for Chapter 3's data processing required hand coding each node (or actor) according to a stakeholder category. To develop indicators for stakeholder categories, I designed grounded definitions for each stakeholder category from a random subsample of 10 percent of the nodes present in the meta-graph. Furthermore, to reduce the chance of my ethnographic subjectivity, I trained two research assistants to code the remaining nodes according to the indicators I had generated from grounded ethnographic observations, and they categorized each node as belonging to: 1) state-based actors, 2) private sector actors, 3) civil society actors, and 4) technology designer actors (percent agreement ranged between 72 percent and 83 percent between the two independent coders on all

items). To further improve the agreement scores, their coding assignments were randomly sorted, and neither knew that the other had the same set of coding tasks. This allowed me to resolve their disagreements by addressing the differences myself and double-checking each of their coding disagreements.

After coding the network nodes according to the grounded indicators developed for each stakeholder category, the third step involved identifying naturally occurring network community clusters and the most central nodes within each cluster. To do so, NodeXL's community detection algorithms were employed to identify statistically improbable network clusters. To identify nodes by centrality, Eigenvector centrality scores were used because they represent a more robust and sophisticated measure than Degree, Betweenness, or Closeness centrality algorithms. The strategic value of selecting Eigenvector centrality rankings over these is that "a person with few connections could have a very high […] centrality if those few connections were themselves very well connected" (Hansen, Shneiderman, and Smith 2011:41). Because the meta-graph reflected the combination of several disparate events, Eigenvector centrality was the best measure to identify nodal centrality across the large and distributed dataset of stakeholders.

In Chapter 3 I provide a visualization of the 125 potential communities identified by the community detection algorithms, and the fact that only two of the 125 communities account for over 80 percent of all stakeholder nodes. After identifying the community clusters, especially the two dominating groups accounting for over 4 out of 5 nodes, I examined the diversity or homogeneity of the naturally occurring clusters to see which categories of stakeholders were present within each. It was obvious based on frequencies of distributions that one group accounted mostly for state-based stakeholders, while the other major group contained most of the civil society activists. Private sector stakeholders did not have much of a community structure, suggesting that while they were present, they were not actively networking or building ties with any particular community, even their own. After identifying that there was a community of state-based actors and another composed of civil society stakeholders, I revisited the associated labels of events, my filed notes, and interview content with each stakeholder community to make sense of and give meaning to these clusters. This is where I identified the *London Agenda* and the *Silicon Valley Standard* as the most influential policy articulations synthesizing the different norms that state-based and civil society stakeholders were promoting.

Figure 2: Conceptual Illustration for Constructing the Stakeholder Meta-Social Graph



Source: Martin Krzywinski, Genome Sciences Center, Vancouver, BC

E-Mail Interaction Analysis: LiberationTech Online Community (2008 to 2012)

Data for Chapter 4 came from an online participant observation of an email discussion community based in Silicon Valley. The reasoning and selection of the LiberationTech community was made from the analysis completed in Chapter 3: mainly that an important peripheral community of technology users and designers seemed to be producing similar norms and approaches in thinking about digital infrastructures. As I discuss in Chapter 4, they are also producing the most interesting ways to think about internet freedom. Therefore, in Chapter 4 I investigate them in the habitat that has couched most of their discussions, labor, and practices: the LiberationTech email list originating at Stanford.

To collect these observations from this web environment, I became an active member of the discussion community three months before departing for fieldwork (though I had been a familiar, but less active member since mid-2009). During those three months, I paid daily attention to the discussion topics and the types of actors participating in the forum. It was apparent from the beginning that although the email list was mostly Stanford and San Francisco Bay Area technologists, they often discussed and collaborated with a globally distributed community of enthusiasts from around the world, and because of the recent backdrop of the Arab Spring, in particular with Lebanese and Tunisian hacktivists. These were among the important reasons why the LiberationTech email community was important to study.

Another key reason was because ongoing field immersion in Beirut and Tunis further bolstered the importance of LiberationTech: in Chapter 3's analysis, I identified that the opinion leaders and gatekeepers connecting state-based and civil society stakeholders to Arab Spring activists were part of this email community, and often engaged in "backburner" conversations before and after major meetings. In other words, the LiberationTech community was the environment where a distinct community of practice was generating important norms that were drawing together civil society and state-based stakeholders (even though in Chapter 3 I identified that they have competing norms). It was important to study this dispersed community in its most natural and centralized habitat, which was the online email list itself (born from an experimental course offering at Stanford in 2008).

Operationally, to synthesize, collect and process this vast email database, first, I archived all the emails from the LiberationTech list and uploaded them by date and subject into a tab-delimited spreadsheet with several columns of metadata. For example, Column 1 contained the

subject title of each email sent by community members since 2008 till the end of 2012, Column 2 contained the name of each email sender, Column 3 contained the date of each email, and Column 4 included the stakeholder label of the sender if identified previously in Chapter 3. In this way, Chapter 4 was a logical and synthetic extension of the phenomena and actors identified in Chapter 3's stakeholder network analysis. But the important task in Chapter 4 was to answer the questions: Who were these interesting pseudo third party actors bridging the civil society and state-based stakeholder clusters and their norms identified in Chapter 3? What new norms of ways of promoting internet freedom were these tech-savvy political activists and technologists introducing to the policy arena? To answer these questions, I conducted a grounded conversation analysis of their communications, which revealed their activities, identities, and meaning-making and cultural production practices over the course of years.

The email meta-database I constructed accounted for over 5,000 emails sent by more than 1,000 distinct individuals since 2008. By frequency of discussion participation, approximately 100 core discussants contributed over 66 percent of all email discussions. So although the email list had a long tail of well over 900 passive listeners, it was a surprisingly small group of 100 core contributors that kept the community of practice alive since its inception. To examine these 100 core members more deeply, the second step in the construction of this database required identifying the Twitter IDs of these prominent discussants to help trace their online activism and organizational linkages. By cross-referencing these Twitter IDs with those of the meta-social graphs constructed in Chapter 3, I was able to determine that more than a majority of the top online discussants overwhelmingly overlapped (71 percent) with the nodes in the civil society stakeholder community, but were ranked very highly in their Eigenvector centrality scores. In other words, they were coded as civil society stakeholders, and they were present in the social networking clusters containing mostly civil society stakeholders. Most importantly, they were also positioned in the macro-social graph of all internet freedom stakeholder meetings as very central to the "known universe" of policy-making stakeholders. These 100 actors, then, were grounded in civil society networks but were also highly influential to the global community of internet freedom stakeholders more generally.

Based on this important observation, the final step in Chapter 4's data analysis required that I delve into the actual discussions and collaboration activities and projects since 2008 to observe their current activities, as well as their past involvements, ideological positions and

evolutions in approaches to internet freedom. This required deep and grounded participant observation, or in other words, reading, understanding, and tracing both their discussion, collaborations, but also the outcomes and current statuses of several projects and debates that had started on or had been shared with the LiberationTech community and its participants. For example, cryptographic tools that were peer-reviewed by LiberationTech designers had, during the time of this chapter's analysis, been deployed in places like the Middle East. So in addition to reading more of the emails, understanding the debates, and contextualizing their norms, I also investigated the outcomes of the most popularly discussed tools and debates outside of the email list by asking actors during the fieldwork about their status and opinions about these tools. Chapter 4's substantive discussion centers on identifying who these core 100 members are, tracing their training and background, and also their current offline activities and involvements between January 2013 and June 2013 (when this chapter's analysis was completed).

Event History Analysis: WCIT Negotiations in Dubai (June to December 2012)

Data for Chapter 5 came from an event history analysis of the WCIT treaty negotiations in Dubai (UAE) which took place during the final two weeks of December 2012. However, as is common with case studies of events, it is usually the case that the activities constituting an event extend far beyond the period of official proceedings. For example, those studying a US Presidential campaign must not limit their case study and observations to Election Day or even the last few days of campaign activities. This is because a case study of a presidential campaign must at the very least cover the full two years before Election Day since that is when various search committees to identify candidates and campaigns begin their organizing. In much the same way, the two weeks of participant observation that I conducted during the ITU's World Conference on International Telecommunications in Dubai in December 2012 were not at all wholly encompassing of the entire event's relevant history, activities, and politics. Thus, three categories of data were analyzed to complete this chapter's historical event analysis.

First, six months prior to the meeting in Dubai, I had begun to observe that field informants routinely discussing the December gathering as a major moment for their work. In the beginning, this seemed to be an anomaly because the WCIT preparations were not focused on promoting internet freedom as with the other summits I had been tracking. So why were my

actors so concerned about a non-internet-freedom event? But as the event drew closer, so did the controversy surrounding it in the stakeholder network I had been tracking.

During the summer of 2012, two George Mason University faculty established a website titled "WCIT Leaks" to assist in leaking the policy documents and frameworks being prepared for the treaty negotiations, and it became apparent that the *exclusion* of internet freedom issues was the reason why this event was relevant, and critical to include in this analysis. I quickly began a separate archive of content, news articles, and interview data that related to these discussions about the meeting, and also monitored the LiberationTech list to see mentions of the WCIT meeting. In June, I noted that both my civil society actors in the field and discussants on the LiberationTech list had also quickly established initiatives to prep for the Dubai meeting.

As a consequence, second, in addition to the six months of online discussions and articles preceding WCIT, I archived the hundreds pages of policy documents that were being leaked and shared as they happened by WCIT Leaks and associated ITU-opposition activists on LiberationTech and in my broader stakeholder networks. Several leaked documents contained detailed attendee lists of all country delegations, along with their members' names and contact information several months ahead of the gathering in Dubai. I collected these counts of delegates being sent to Dubai by world governments, the agencies and corporate entities they were anchored in, and pinpointed the civil society groups I had been networking with that were likely to attend. From these tabulations, it became apparent that almost all of the 2,000 delegates officially allowed to the UN meeting in Dubai were either members of governmental agencies (like the US Department of Commerce) or policy advisers to major multinational technology companies (like Google and Facebook). In contrast, none of the leaked delegate attendee lists had prominent civil society actors. So as early as October 2012, three months in advance of the meeting in Dubai, with the help of observing field informants and the peripheral online community of practice, I was aware that this meeting was one of the rare moments where state-based and private sector stakeholders were gathering with the near-full exclusion of agitated civil society stakeholders.

Finally, third, in preparing to attend the event in December as a participant-member, I needed to observe how civil society groups would strategize to influence this exclusionary policy making body where internet freedom issues were on the table. During my attendance at WCIT-12, I rendezvoused with and worked alongside excluded civil society members in their efforts in

exchange for access to observing, interviewing, and collecting their discussion transcripts and monitoring their successes and failures to gain entry to the elite and exclusive treaty making delegations. This analysis in Chapter 5 is a historical event analysis informed by the six months of hundreds of leaked policy documents, detailed delegate information and interviews, intimate field observations of excluded civil society members, and in particular forty-five pages of minute-by-minute Skype transcripts and original documents collected over the two-week period of the Dubai negotiations.

Human Subjects and Ethical Considerations

The subjects and informants identified in this study range between the ages of twenty-five and fifty years old and are relatively gender balanced, although their races and ethnicities vary considerably because the participants are internationals from both Western democratic nations and emerging countries. The broad inclusion criterion for interviewing individuals, referring to their policy documents, or observing their interactions and social ties was whether they were explicitly working on internet regulation policies or internet freedom promotion. Interview questions focused only on their reflections on the experiences, opinions, and interests in being part of public technology regulation discussions and activities. The ethical issues of confidentiality and the protection of human subjects are important ones in this study. In order for my analysis to take into account the real political debates and policies being designed to promote internet freedom, it is necessary for some members of the stakeholder network and the affiliated institutions to be named. However, I have taken several steps to anonymize and protect the identities of rest of the subjects and informants employed in this investigation.

Because this study examines the public negotiations between several transnational stakeholders and organizations attempting to regulate the uses of computer and digital networks (i.e., digital infrastructure), it includes examination of prominent transnational activists, multinational corporations, and policy makers. Therefore, the limited range of subjects I do refer to and the policy documents I make use of are original primary documents already readily populated and shared by their organizations both during stakeholder gatherings and online, before and after their meetings. I try as much as possible to identify individuals and give voice to their opinions and views from their public documents and utterances they themselves have made available publicly. However, the limited range of informants I quote from personal interviews

and online discussions are primarily policy makers, technology lobbyists, political activists, or academic researchers who are already public with many of their views and concerns. Finally, for those informants who are not prominent public officials or international experts, or those who have asked explicitly to not be identified, I have assigned pseudonyms and randomized references to their genders, ethnicities, and countries of origin, in order to mask their identities.

Furthermore, beyond the expressions of opinions and ideologies surrounding internet freedom promotion, this study also makes use of social graph data collected and aggregated from virtual environments that these human subjects maintain an active online presence in. These digital data-shadows exist primarily in the form of social tie information on Twitter's API and email discussion lists where these stakeholders conduct most of their communication and networking. Although these seemingly unprecedented data are readily and legally traceable and indexed through popular search engines' servers, like Google's, it is unethical to reveal particular individuals' intimate socio-technical ties and positions. Whenever referring to social tie data, I present it in aggregated form to help anonymize and mask individual actors' identities and positions. These composite descriptive sketches refer to the broad trends, whenever possible. However, sometimes it is impossible to make some actors' identities untraceable because their statements are archived and publicly available on digital servers readily searchable online (and made more challenging because "right to be forgotten" policies have not taken root yet in the US-based internet policy regimes). In this case, I have little choice but to defer to the terms of user agreements that these users acknowledge and accept when conducting their activities in public email lists and web spaces like social media sites. Beyond my efforts to protect the human subjects involved in these studies, it is also my measured hope that the benefits of this study outweigh any unintended risks posed to my participants.

Chapter 3 – Communities of practice and Stakeholder Norms

"There is a material reality to the internet. Most people look at the internet as magic: 'I click a button. Something happens. I get the information.' They don't care to acknowledge the actual physical infrastructure that's moving that data. It's pipes in the ground. […] So, how does a free network figure into the movement? Well, it's not the movement, but it is a necessary and foundational piece of infrastructure that has to be in place before the movement can fully blossom."

Isaac Wilder, Free Network Foundation (March, 2012)

There have been at least ten conventions and conferences arranged by the foreign policy offices of key Western democratic nations since the Arab Spring. In the two years following the Arab Spring, information activism has grown more sophisticated (and more complicated). Access, the main organization that lobbied corporations to keep communications networks running and pressured ICT companies to stop selling software tools to dictators, organized the Silicon Valley Human Rights Conference in November 2011. The event was sponsored by Google, Facebook, Yahoo!, AT&T, Mozilla, Skype, and other key multinational ICT corporations and brought together corporate leaders and foreign policy officials from major Western democratic nations to design policies for corporate social responsibility in the interest of human rights. Similarly, the governments of the United States, the Netherlands, Sweden, and the European Union have all publicly followed suit and created formal funding programs providing upwards of $100 million to support digital activists working from within repressive regimes. These meetings have brought together information activists and ICT corporations. US Secretary of State Hillary Clinton has referred to this interesting mix of brokered meetings as "21st-century statecraft."

The new types of digital activists and technology policy makers increasingly find themselves working diplomatically with Western foreign policy makers while targeting and lobbying multinational ICT providers to stop enabling repressive regimes with technical surveillance and censorship capacities. In sum, these stakeholder conventions organized by Western democratic governments in the aftermath of the Arab Spring were the first in recent history, and have facilitated an important and formal process for drawing together these different types of actors and stakeholders that sometimes defy easy categorization. The task of this chapter is to help define, categorize, and understand their complementary and competing norms towards promoting "internet freedom." Mainly, who are the new stakeholders that have become engaged

in policy discussions surrounding digital infrastructures? What are their backgrounds and committed interests, and what types of norms are they drawing into the policy entrepreneurship surrounding internet freedom?

3.1 The Global Network of Internet Freedom Promoters

The recent political transformations in the Arab world have helped to bring the politics of digital infrastructure to the forefront of public discussions and global policy making. In turn, these developments have also pushed the designers and regulators of digital technologies to better understand the potential benefits and risks of the digital tools that have been used by political activists in recent waves of protest around the globe. What is particularly challenging for studying these kinds of infrastructure politics is the lack of formal membership requirements to enter the policy discussions, mainly because stakeholders have many originating backgrounds and the proto-regime in question has not been effectively defined nor been formally encased with organizational capacities. In the previous chapters, I described the recent advancements in communication studies that have provided empirical approaches and analytical frames by which to study these types of transnational actors by conducting a "network ethnography" (Howard 2002) of these various communities of practice. This chapter begins that effort by mapping the global network of actors comprising the diverse stakeholders currently working to promote internet freedom since after the Arab Spring.

The actors identified in this analysis are located transnationally, encompassing both democratic and repressive political systems. They also include experts and key knowledge producers who have, for significant periods of time, been raised in non-democratic environments, but then immigrated to advanced industrialized democracies. Since doing so, they have drawn on their experiential knowledge to urge other stakeholders to rethink their approaches and norms towards managing digital infrastructure. This leads them to bring new and distinct understandings about what constitutes digital infrastructure, and consequently how that infrastructure should be secured to promote internet freedom in ways that the standard approaches towards internet governance or media policy may be agnostic towards. So we need to understand both who the actors are (and how they are connected to each other), and how this positioning might shape their norms and approaches towards digital infrastructure management.

Because of the distinct institutional backgrounds that proponents of internet freedom are grounded in, this examination of the network's ecology focuses narrowly on the promoters of internet freedom. In other words, the sampling approach begins by identifying the key experts who attended the ten internet freedom stakeholder meetings identified in chapter one. This also means that this analysis does not tell us very much about the actors resisting internet freedom, like authoritarian regimes and repressive rulers. That is because the goal of this chapter is to examine the norms guiding the promoters and norms surrounding internet freedom policy, and who is behind specific norms, and why. Furthermore, as discussed in Chapter 2, the data for this chapter comes from the aggregation of individual activists and policy makers and their social ties. This information was made public through the discussions and debates fostered through the ten internet freedom summits organized since the Arab Spring. In addition to making use of primary field observations at the gatherings and interviews with key experts, this chapter also broadens the network to include their social media ties cultivated during and after the meetings.

3.2 Defining the Stakeholder Communities

This chapter is a network analysis of the stakeholder meetings sponsored primarily by Western democratic governments since the Arab Spring. These conventions were organized to bring competing stakeholders together to deliberate, design, and implement new policy approaches for realizing the democratizing potential of digital tools and internet infrastructure in non-democratic states (i.e., digital infrastructures). So, what has been the outcome of these meetings? Who are the new actors that have now been connected because of these efforts by Western regimes, and in particular the United States, to identify and unite them for internet freedom promotion? This discussion helps to typologies and describes these stakeholders, who come from governmental, civil society, and the private sector.

In addition to those categories, there are new actors who are difficult to categorize. This includes the new and interesting breed of technology-savvy political activists that have taken root after various recent protests, like the Green Revolution in Iran in 2009. These new activists and their supporting NGOs, like the US-based Access (which also grew out of the Green Revolution in Iran, in 2009) and the Electronic Frontier Foundation, have expanded the scope of their activities to pursue internet governance issues in nondemocratic states. They seek the support and backing of Western democracies to promote internet freedom abroad, but sometimes

also struggle with them when those principles are violated domestically by their supporting regimes. For example, Access was quick to launch lobbying campaigns to pressure technologies companies like Vodafone to turn connectivity back on in the Egyptian revolution, but was also forced to fight Western software companies over their accountability for selling censorship technologies to the repressive governments of Syria and Bahrain. We will need to think closely about these types of actors and examine what, if any, structure or coherence these actors may have in relation to the major categories that have been defined so far.

So I begin by identifying and defining three categories of stakeholders, providing several examples of each: a) *state-based* stakeholders; b) *private sector* stakeholders; and c) *civil society* stakeholders. Together, the actors who fit within these categories encompass more than 80 percent of the social ties shared within this stakeholder network. Broadly, civil society stakeholders have the most representation and connectivity, while state-based and private sector actors have the least connectivity (below the average level of social ties for the entire network). Who are these stakeholders, and what more can we say about their ideological interests and commitments to the promotion of internet freedom?

State Actors and Western Democracies

State-based actors are people, groups, or agencies acting on behalf of a governmental body and therefore ultimately subject to the interests and policies of the governments under which their position and affiliated agency may reside. Although this definitional category of stakeholders is relatively straightforward, it can and does become problematic when pertaining to individuals and professionals who have previously held positions in other sectors. Beyond the more commonly recognized complications of jurisdictional overlap (e.g., private companies that are subsidized by states, like TeliaSonera, a telecommunications provider majority owned by the Swedish and Finnish governments), the state actors involved in this network also deal with extensive cross-sector socialization that they experience when consulting for or holding multiple positions in advisory roles to the private telecommunications industry and civil society organizations.

Actors who fit this profile of state-based actors typically have a clear self-narrative in which they primarily express their concerns in relation to their responsibilities and duties towards federal governments or state agencies as a binding legal and financial employer. Overall,

less than 7 percent of actors in the global network of infrastructure stakeholders with respect to internet freedom issues belong to the state-based category. Furthermore, these state-based actors accounted for less than 4 percent of the total online audience following internet freedom stakeholder summits, discussions, or attending participants. In other words, although state-based actors are relatively well represented in the stakeholder community that was initiated and cultivated by Western democratic regimes, they are not the most "listened-to" nodes in the global network of internet freedom stakeholders. So, while these governmentally affiliated actors were present in the meetings (as expected, because these meetings were primarily organized by states), they are not the primary figures that are being listened to or present in the broader stakeholder network.

Furthermore, almost all of the most popular and central figures in the state-based actor category wholly reside in advanced Western European democracies and their foreign policy interests, as expected. Examples include governmental employees working for *development agencies* (e.g., the UK's Department of International Development and the Swedish International Development Cooperation Agency), *defense ministries and cybersecurity agencies* (e.g., the UK's Ministry of Defense and its International Cyber Policy Unit), and *human rights agencies* (e.g., the UK's Human Rights and Communications Team). The rare exceptions to these sub-categories are self-described "internet evangelists" working for some government's state-backed governmental bodies. These include governmental personalities like Marietje Schaake (the Netherlands' prominent Board of Governors for the European Internet Foundation) and Moez Chakchouk (the chairman and CEO of the Tunisian Internet Agency). But these kinds of personalities are far less visible in the stakeholder's connected to state agencies. Overall, state actors are involved in the global stakeholder network promoting internet freedom, but they are not very central, nor are they the most active networkers (despite belonging to the category of actors that has formally initiated these internet freedom summits).

Technology Providers and the Private Sector

Private sector actors are those that have sole proprietorship (often representing boutique companies and new start-ups), partnerships between a small number of directors, or were working for influential multinational corporations are also involved in internet freedom discussions. Often, these stakeholders are the providers of both the basic internet infrastructure

and the associated ICTs (e.g., mobile phones and laptop computers) that individual users make use of to access digital media. A **private sector** stakeholder is a person, group, or agency held primarily by non-governmental organizations working at for-profit technology companies. Both publicly traded agencies as well as unquoted and unlisted companies are present in this broad category representing the technology sector. Defining a private sector actor does become complicated in some cases, for example when telecommunication companies (such as those based in Northern European and the Arab Gulf countries) that are either partly (less than 50 percent) or in the majority (more than 50 percent) owned by the states where they are registered. So, despite some instances where mixed-ownership formats do exist, most private sector actors in this network belong to commercial enterprises with an overt profit-maximizing incentive.

Approximately one out of four individuals (24 percent) present in the global community of internet freedom actors belong to the this private sector category, most of whom we can describe as being part of the boutique industry of single-person start-ups providing for-profit consulting services. An important characteristic is also that the vast majority of the most central actors in this stakeholder community are geographically and economically rooted in Silicon Valley, while other substantive locations include Washington, DC and Boston, followed by various European global cities including London, Stockholm and Amsterdam. In other words, the private sector technology providers are almost entirely based in Global North countries described as advanced industrialized Western democracies.

These private sectors actors are similar to their state-based counterparts in that they are also the least "followed" nodes in the internet freedom community. Private sector stakeholders account for nearly one fourth of all actors, but have only 12 percent of the global audience following them (for state-based actors, this similar ratio was less than a fifth of actors receiving less than 4 percent of the global audience). So, on average, both private sector and state-based stakeholders rank below average in the amount of followers they share, despite being the important providers of technologies that are at the center of internet freedom debates.

So if both private sector and state-based actors are not very centrally located or popularly followed, what might be some important differences between them? These private sector actors involved in internet freedom activism seem to consistently provide two broad and differentiated services: a) analytics and social media engagement tactics for their market clients, and b) internet safety and security services, including tools for cybercrime and cyberwar issues to governments

and corporations. So while the category of technology providers can be broadened to include any form of digital services and technologies, there seems to be a large market demand for tools to fight cybercrime and cyberwar that states seem to be messaging or signaling them about.

Several of the Silicon Valley based actors, for example, define their services with statements like the following: "Our online software helps businesses turn analytics into insights that guide decision-making and growth," accompanied by promises to help increase customers' revenue or avoid loses by $25,000. These estimates are often followed by advertisements for their technical consulting services, which begin with subscription plans starting at $150 per month. These chairmen and chairwomen describe themselves as veterans of "fighting malware" with applied experience ranging from ten to thirty years in the industry. In industry slang, these individuals sometimes refer to themselves as "white hat hackers," computer hackers and security experts specializing in penetration testing of information systems to improve network security. A typical biography reads: "I am a whitehat who enjoys writing software, tinkering with computers and everything security related." Their stated intentions for involvement in the internet freedom discussions range from wanting to stay up-to-date with the latest discussions regarding network security issues to drawing on and providing experiences from around the world to their community of hackers and tinkerers:

> [M]y main intention here is to engage in a broader conversation with you and discuss other things that sometimes fall beyond boring security issues. I travel a lot, meet many people from different countries, and give many public speeches. I believe such a broader and more relaxed interaction will be much more interesting and provide better insights.
>
> *~ Biographical statement expressed on corporate blog.*

Some individuals also seem to be motivated in applying their regional expertise and personal backgrounds into their consulting service offerings. These individuals typically originate from repressive political systems, like Yemen, but have since migrated to Western democracies where they continue to engage in their political work from abroad but do freelance work on the side:

> In self-exile in _REDACTED_ since May 2011, I'm a freelance writer and blogger since 2010 focusing on women's rights, democracy, and politics of Yemen. In April 2011, my blog has been featured as one of the 10 must-read blogs from the Middle East by CNN. […] I have worked as a reporter for Yemen Observer newspaper 2008-2011, and the _REDACTED_ International Radio 2012 and currently work at _REDACTED_. […] I am a public speaker on Yemen's affairs and regularly write columns about Yemen for publications in Yemen, Sweden, UK, Kuwait, US and UAE.
>
> *~ Biographical statement expressed on consulting site.*

Individuals like this Yemeni activist possess journalistic ideals, yet contribute actively to discussions of network security and internet freedom as freelance advisers and consultants. This tendency to combine political work with private consulting reflects the negotiable identities of actors embedded in the private sector and their own boutique consulting services. This is due to the opportunities they are observing and the demand for the experiential knowledge which states are signaling about when convening summits and conferences to discuss internet freedom promotion. Many are also motivated beyond profit by the possibility of entering "prestige industries" including the realm of policy consulting and advising that internet freedom policy entrepreneurship seems to open doors to.

This raises another theme that is characteristic of the private sector presence at these conferences, particularly of boutique companies and freelance consultants. While civic-mindedness is a shared theme across private sector and civil society actors, individuals that are more centrally grounded in the private sector companies profess a broad yet social entrepreneurial-based identity as their motivation. Examples of this civic-minded entrepreneurship are statements and self-descriptions of their services such as: "Digital engagement for people with more sense than money" which seems to prioritize the socio-political importance of their technologies and strategies over the financial payoffs.

Some examples make this quite obvious, like Metahaven, based in Amsterdam, which is in the business of designing communications and public relations strategies to negatively affect dictators and non-democratic regimes:

> Bridging between design, geopolitics, architecture, and branding, *Metahaven's Uncorporate Identity* [a book created by Metahaven] defies easy categorization as a monograph. The book is organized as a sequence of five chapters, dealing with data havens and statehood, post-communist architecture, visual legacies of the war on terror, tourist brands and border control, and social networks restructuring soft power, branding and governance internationally. With each chapter comprised of case studies, notes and essays, it explores visual identity in a networked and multi-polar world.
>
> *~ Book jacket content on company's publication.*

Amsterdam's Metahaven has also published a similar book easily downloadable on Kindle targeted towards digital activists titled *Can Jokes Bring Down Governments? Memes, Design and Politics*:

> These are serious times, or so our governments keep telling us. Strangling economies with their austerity policies, they assure us that they have no choice. In a world where "there is no alternative", how do you dissent? Once upon a time, graphic designers would have made political posters and typeset manifestos. Today, protest has new strategies. Enter the internet meme. With its Darwinian survival skills and its viral potential, the meme is a way of scaling up protest. Hackers and activists have learned to unleash the destructive force of a Rick Astley video. They have let slip the Lolcats of war. Pranks have become a resistance strategy. As the rise of Beppe Grillo in Italy testifies, this may be the hour to fight nonsense with nonsense. Jokes are an open-source weapon of politics, and it is time to tap their power.
>
> *~ Biographical statement expressed on company's publication.*

It is notable that these private sector actors seamlessly integrate for-profit consulting and technology services with civically minded applications, tools, and strategies for their audiences and consumers. This indicates that some individuals not only see digital technologies and digital media spaces as politically impactful; they are also seeing these as possibly profitable arenas to provide their services to states and activists.

Finally, and this comes as a rather significant surprise, is that *most major technology corporations are not present in the stakeholder network*. Most individuals belonging to the private sector actually belong to the long tail of boutique companies and single-person start-up security outfits run from blogs and garage workshops. Some major multinational technology corporations are present, but far less visibly than the boutique organizations and single-person start-ups. Examples of these important, but rare, corporations include the heads of policy or open-source initiatives in major corporations including Twitter and Facebook.

Civil Society and Political Technologists

As I have described so far, state-based and private sector stakeholders are present in several meaningful ways in this network, but they are not the largest or the most central set of stakeholders shaping this network. The single most influential and well-represented stakeholder category is actually the civil society actors. Civil society actors encompass the single largest category of actors present in the internet freedom stakeholder ecology and have roots mainly in transnational civil society organizations: one out of every two actors overall (50 percent) belong to this civil society category of stakeholders. Furthermore, in contrast to state-based and private sector stakeholders, civil society actors on average are also the most followed actors, measured by the overall size of the public following of these actors (over 81 percent). Put another way, the total number of online actors belonging to transnational civil society account for 4 out of 5 audience members following stakeholders belonging to internet freedom discussions.

In this study, a **civil society** actor refers to a person, group, or agency based primarily in the "third sector" of society, distinct from state-based actors and the private business sector. The undergirding experiences, interests, and demands voiced by global citizens often find their roots and expressions in organizations and spaces manicured in this civil society sector independent of, and often in contrast to, the interests of governmental and corporate interests described previously. In contrast to the motives of profit and sometimes social entrepreneurship present in the private sector stakeholders, and the power to create and enforce policies and regulations by state-based stakeholders, civil society stakeholders do most of their work on a voluntary basis from a sense of a normative obligation to serve the public's interest. The fact that they have engaged themselves in the esoteric concerns of global internet freedom promotion indicates that

they feel there is importance in concerns about regulating ICTs and digital infrastructures that can (or have been observed to) impact their civic lives.

What are the key features that differentiate civil society actors from the social entrepreneurs described in the discussion of private sector actors? First, civil society is the only sector that visibly features individuals we can refer to as *"indigenous" political activists* working behind the borders of dictatorships and authoritarian regimes. These are citizens who actually reside within repressive political systems and are engaged in political activism and democracy promotion work from dangerous positions that put their livelihoods at risk. Examples of individuals that fit this category include a Syrian-born Yemeni activist who describes himself as a"[d]octor by day, blogger by night!" Other examples include netizens who contribute to transnational civil society organizations like Global Voices, where they actively contribute to global discussions about technology and politics from "bottom-up" locations in the Global South including Bangkok, Bogota, Cairo, Manila, Nairobi, Santiago, Tunis, and others. These technology-savvy political activists also interact fluidly with one another despite speaking and writing in a slew of native languages including Arabic, Thai, Korean, Spanish, Portuguese, and others. So they are both substantively political in resistance activism and democracy promotion, yet they are also reaching out transnationally to find new tools, strategies and opportunities that have made them realize or become curious about the politics surrounding digital infrastructures.

Political hacktivists are another set of civil society actors present in the civil society category, but do not describe themselves in the same way as the "white hats" in the private sector. Instead, these "hacktivists" openly identify themselves as political-motivated hackers who were active during several recent transnational protest campaigns like the 15M movement in Spain, and offer self-descriptions like "Hacktivista por la libertad de expresión en internet. Activista del #15M" ("Hacktivist for freedom of expression on the internet. #15M activist"). Intimately connected to these political hacktivists are technologists and software engineers that frequently discuss the applications of "liberation technologies." This language consistently refers to and originates from an online discussion community that started at Stanford University in 2008, which has since become a thriving place of deliberation and design for a nascent network of hackers and technology policy makers who have more recently found prominent positions in global research universities, foreign policy think tanks, and multinational technology corporations.

This community is worth further discussion. LiberationTech not only refers to members of an online discussion community; it is also a formal program at Stanford that actively curates discussions on Twitter with its own account. The @LiberationTech node is *the single most central and influential Twitter account in the entire database of internet freedom Twitter handles*. Other important members who share linkages to the LiberationTech community and have central positions in this civil society category include Evgeny Morozov (of Belarusian origin), Rebecca MacKinnon (with extensive field experience in China), and activists Nadim Kobeissi (originally of Beirut), Rafik Dammak (of Tunisian origin), Marcin de Kaminski (a member of Europe's Telecomix hacktivist network), and Anonymous (a political hacking network covered widely by mainstream media). All of these civil society stakeholders and digital activists have been cross-fertilizing their collaborations and policy ideas with state-based actors and private sector stakeholders since before the Arab Spring, and have prominent public proponents that frequently write opinion editorials in news media bringing light to the politics surrounding digital infrastructures.

Finally, in addition to their technical expertise, many civil society actors also exhibit advanced legal training and expertise about internet governance issues. Those with professional legal training, like law degrees, are currently based in advanced Western democratic states, where they work to advocate at some highly visible institutions on behalf of internet freedom issues, drawing increasingly on internet regulation issues as a critical set of items to be both devised and promoted from the perspective of global civil society in discussions and debates about global internet freedom. Most of the top legal experts from this category share geographic proximity to Washington, DC–based think tanks specializing in internet policy, foreign policy, and human rights abuses. These organizational and institutional actors' current relationships include: the Council on Foreign Relations, Freedom House, the Internet Society, the Henry Jackson Society, the Committee to Protect Journalists, and the Center for Democracy and Technology. Other nodes outside the DC policy corridors include London's Index on Censorship, Bangalore's Centre for Internet and Society, Moscow's AGORA, and Santiago's ONG Derechos Digital.

Table 3: Estimated Distribution of Global Stakeholders by Actor Categories

Stakeholder Category	Total Nodes	Percent Nodes	Total Edges	Average Edges
Civil society	3,000	50%	4,794,000	2,961
Private sector	1,439	24%	711,000	494
State-based	421	7%	228,000	542
(Unknown)	1,140	19%	187,000	164
TOTAL	*6,000*	*100%*	*5,920,000*	*987*

Note: Categorizations computed by two trained expert coders, see Chapter 2 for details on coding procedures and category indicators.

3.3 Identifying Competing Norm-Making Communities

In the preceding analysis, I developed a grounded categorization scheme for identifying the different types of actors that have come together over the two years following the Arab Spring to address digital media and information infrastructure politics of global internet freedom regulation. I also described the relative presence of each category, notably that civil society activists surrounding digital infrastructures politics and internet freedom promotion are the most represented and vocal, while state-based and private sector actors are less present and less engaged (with the private sector also excluding many of the important multinational technology providers in question). Having typologized the three categories of actors as state-based, private sector, and civil society stakeholders, then, I now examine the overall relationships between these communities of practice from a social network perspective.

To do so, I extend the network ethnography by examining the clusters of actors that have emerged since the ten internet freedom summits sponsored by Western democratic governments. I consider how heterogeneous or homogeneous these clusters are, and if any discernible norms or collective goals seem to be emerging from them, and why. Once emergent clusters of stakeholders are observable, I explore each cluster through an ethnographic investigation of the individuals and organizations belonging to that cluster and the types of norms they seem to be propagating. To do so, I review the statements they have made about the importance of the internet freedom activities and discussions they have paid attention to and participated in. When policy statements and frameworks have been formulated, I also take note of which norms and issues different clusters seem to have supported.

Investigating whether these theoretical typologies actually stick to the contours of the emergent clusters shaping the internet freedom network can help tell us which ideological forces and norms are likely to play influential roles in the eventual regime that may or may not emerge. To do so, the analysis proceeds by first using an inductive network analysis and network clustering approach—this allows us to begin by documenting what the naturally occurring network clusters are—and after identifying those, by assessing the interactive stakeholder presence in each naturally occurring network cluster. After identifying the emerging clusters in the global network of infrastructure stakeholders, I observe whether the interactions and social ties reach across different clusters or if their network relationships primarily point inwards within clusters. In other words, for example, if a hypothetical cluster of private sector actors is present

in the network, do these private sector actors connect with state-based or civil society actors more, and if so how might their norms and understandings be effected by these new socialization patterns? Broadly, what are some of the overall structural characteristics of the emerging global internet freedom communities of practice?

To begin with, Figure 3 illustrates the global network relationships among all actors and identifies the emergent network clusters. The structural formation of the global stakeholder network as it has formed over the two years since the Arab Spring is currently distributed across a potential 125 disparate group clusters. But of these 125 computationally distinct clusters, the two largest network clusters account for well over 66 percent of stakeholders. The remaining 33 percent are distributed in a difficult-to-decipher distribution of more than 120 clusters, each averaging less than an average of 2 percent of nodes and social ties. Because the two largest clusters contain almost all of the actors under investigation, I limit my ethnographic analysis to these two influential segments and extract the most contrasting norms that each cluster of stakeholders and their interactions seem to be generating (see Figure 3). *What activities and norms are being cultivated in these two encompassing and distinct communities of practice?*

First, state-based stakeholders are primarily located in cluster G1, while most civil society stakeholders are located in cluster G2. Furthermore, over 75 percent of all state-based actors identified in the network are exclusively located in cluster G1, and their social ties reach mostly within the cluster, not outside of it. Second, while civil society stakeholders are located primarily in cluster G2, prominent nodes fitting the civil society category are well distributed across clusters G1, G2, G3, and the rest of the minor clusters between G4 and G125. In other words: most state-based actors are exclusively located in cluster G1, while civil society actors are congregated heavily in G2 and across other clusters globally. This means that, in contrast to the insular structural network characteristic of state-based stakeholders, civil society stakeholders enjoy the structural positioning of an influential network core and a heterogeneous distribution across the greater ecology of the internet freedom network's clusters. *Finally, and importantly, the private sector actors are distributed across all clusters and also lack a cohesive congregation in the internet freedom network. In other words, the private sector likely does not have an observable and meaningful presence in the social ties and practices.*

These network and cluster distributions call into question some of our existing assumptions about the importance of the internet freedom stakeholder communities and how they

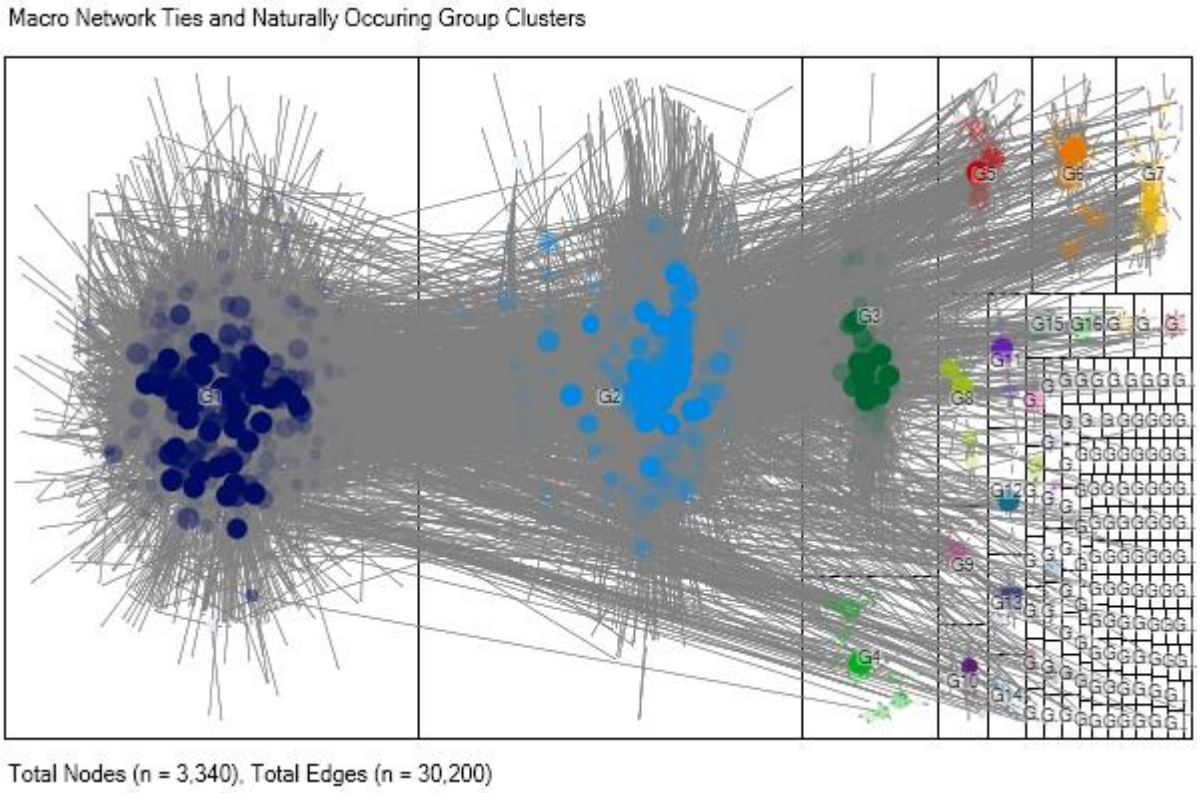
may be organizing. First, if state-based stakeholders, who have initiated these summits and stakeholder negotiations to begin with, really want to meaningfully engage other stakeholders, why are they the most insular and well-isolated set of actors? Second, civil society stakeholders seem to be positioned interestingly between state-based stakeholders and have organized a safe space for themselves where they seem to be generating their own ideas simultaneously. If this is the case, how distinct and novel are the norms and approaches they are cultivating in comparison to existing ones? Third, while technology providers are critical to draw into the conversation about internet freedom norms and commitments, why are they disorganized and loosely distributed in the global network? If these private sector actors have eluded the internet freedom discussions and interactions online, where, if at all, are they being meaningfully brought into internet freedom promotion work?

To examine these puzzles, in the following discussion I argue that while there have been at least ten key stakeholder conventions organized by Western democratic states since the Arab Spring, two core normative issues seem to be balkanizing the two largest communities of stakeholders (state-based vs. civil society interests). Additionally, due to this normative split on how to focus the regime, technology providers have effectively slipped out of the discussion and efforts to promote internet freedom—yet they are important to reign in, and this remains an enduring challenge facing the proto-regime. They are doing so by publicly sponsoring and attending the discussions, but have not substantively contributed their own normative ideas about how to enact internet freedom norms and policies. In other words, they are passive audiences, not active participants in the proto-regime construction efforts. I support these claims by identifying the notably divergent norms characteristic to the agendas and objectives expressed by these different stakeholders, primarily states and civil society, which were also subsequently reflected in the emerging structures of the global internet freedom network clusters. Understanding these divergent foci of norms is relevant for understanding the competing directions constraining, and threatening to split, the proto-regime into halves.

In the following sections, I demonstrate this balkanization of norms by discussing two specific examples and agendas that elegantly express the divergent norms: the *London Agenda* curated after the London Conference on Cyberspace, an event initiated and sponsored by state-based actors. The norms of this community of stakeholders focus primarily on issues of network security from the perspectives of state powers. Second, I contrast this norms agenda with the first

gathering of the Silicon Valley Human Rights Conference and the comparable *Silicon Valley Standard* – a competing norms framework that differs importantly from the concerns expressed by states, but is more directly related to the needs of users and citizens. This alternative set of norms focuses on the responsibility of technology designers and the risks faced by technology users—in contrast to London's focus on the cyber threats facing governments. Third, what is also important in this discussion is the missing role of technology providers and the private sector. While technology companies have been present in both kinds of events, they have not produced much of the substantive new thinking or norms about promoting internet freedom. Instead, they seem to be present solely for the purpose of public relations concerns.

Figure 3: Combined Social Graph of Stakeholder Ties and Emergent Clusters



Note: Graph prepared by author based on social network analysis of Twitter's data collected from stakeholder meetings involving internet freedom promotion that maintained an active Twitter "handle." NodeXL was used to access these data directly from Twitter's API based on the seeding of ten specific event-based hashtags and handles. All ties refer to bi-directional relationships and centrality scores were determined by re-occurring presence of nodes across events, in addition to their centrality based on edges.

State Norms: Securing and Safeguarding Critical Infrastructure

One of the earliest stakeholder conventions in the series of state-backed gatherings in the aftermath of the Arab Spring took place in London in November 2011. This gathering was sponsored by the United Kingdom's Foreign and Commonwealth Office and was called the *London Conference on Cyberspace*. The explicit aim of this high-level yet public gathering was to develop and design the "London Agenda"—a set of norms, principles, and guidelines for stakeholders to follow with regard to digital infrastructures. The London Agenda, and the proceedings of the London Conference on Cyberspace reflect the major category of state-based actors and ties present in the stakeholder network. Critically unpacking the London Agenda will help to illustrate the norms favored by state-based actors and their concerns for doing so when promoting internet freedom promotion. For example, the London gathering explicitly and deliberately framed internet freedom issues from an exclusively states' rights and industry-engagement perspective:

> [T]he London Conference on Cyberspace on 1–2 November will be hosted by the Secretary of State for Foreign & Commonwealth Affairs, the Rt Hon William Hague MP. It will launch a more focused and inclusive dialogue between key cyberspace actors from across the world including from government, industry and civil society. This will aim to develop a better collective understanding of *how to protect and preserve the tremendous opportunities that the development of cyberspace offers us all*. The ideas and proposals which emerge from the conference will develop into the "London Agenda", a plan to help us realise the full potential of cyberspace—one of the great challenges of our time.
>
> *~ Official statement and announcement from the UK Foreign Office*

So not only was the opening strategy for the summit framed from the perspective of governments and corporations; the reasoning behind its initiation was also significant. For example, the opening statement for the event first and foremost focused on the protection and "preservation of cyberspace." This cultivated the idea that it was the fundamental infrastructure (i.e., the "internet backbone") that was at stake and needed protection, as opposed to the users (the perspective of human rights and civil society observers) or the technology designers and regulators (the perspective of corporations and providers). Like the other conventions, though,

the London gathering promoted both public and online discussion about the gathering, actively and publicly shared policy documents with stakeholders, and invested heavily in drawing a global audience of participants and discussants during the event's proceedings both at the event and online.

The organizers for the Foreign Office also outlined five critical themes to be developed, discussed, and debated during and after the gathering. These were: 1) economic growth and development; 2) social benefits; 3) cybercrime; 4) safe and reliable access; and 5) international security. Despite the seemingly open and broad range of issues listed at the onset that could have engaged a variety of stakeholders and concerns, the main outcome of the historical moment inspired by the "London Agenda" has in fact been a focused, but limited, range of issues concerned with state sovereignty in cyberspace. Civil society issues, in the rare occasion that they were raised, were discussed in a highly constrained fashion that lacked the level of nuance afforded to cybercrime issues dominated by state and industry stakeholders. Because the London Agenda was defined from the perspective of state-backed actors, civil society interests, like user safety and citizen welfare, did not receive substantive discussion or critical evaluation. To support this claim, in the following sections I refer to fieldwork data and interviews with members who attended the London convention, and also analyze some of the important policy documents that they discussed.

First, with regard to the London conference's understanding of civil society's concerns, state-backed stakeholders often defined internet freedom in an overly generalized fashion based in a broad, technologically deterministic, and overly optimist understanding of digital technologies:

> Cyberspace is blurring geographical boundaries and breaking cultural divides. It brings families and friends closer together and builds knowledge and understanding between communities and nations. The internet is educating whole generations, giving many a better future by granting rapid access to information and ideas. It is enabling ordinary citizens to hold their governments to account, supporting democratic change and improving the lives of millions. New technology offers the opportunity to improve the provision of public services as well as the response to emergencies and natural disasters.

> It's clear that the social and economic benefits of a networked world can be enormous, particularly for developing countries."
>
> *~ UK Foreign Office's framing of the "social benefits" of cyber space*

Similarly, in the "safe and reliable access" scheme, the organizers did ask some key questions with regard to users' safety and human rights, like "[h]ow best to promote public risk-awareness and education in safe and secure online behaviour (particularly for vulnerable groups)." However, the overarching approach here focused primarily on regulatory stakeholders, such as governance organizations like the ITU and infrastructure providers like telecommunications corporations, but provided little access to civil society actors and affected users themselves. State-backed actors also took a top-down approach of asking themselves how best to *teach* users and civil society actors about risk awareness, not considering the possibility that the users and their experiences might actually teach them something important about their problem definitions and proposed solutions. This top-down pedagogical approach essentially isolates users and citizens, when instead it is they who are the most effected from the threats to internet freedom to begin with.

Second, the London Agenda devoted a greater amount of focus, discussion, and deliberation to cybercrime and cyberpolicing issues, privileging the concerns of private sector interests:

> Criminals are also exploiting the growth of cyberspace. They are using it to extort money, steal identities, ideas and designs, defraud government departments and businesses, as well as exploit the most vulnerable in our societies, particularly children. The annual cost of cyber crime to the global economy could be as much as $1 trillion.
>
> *~the UK Foreign Office's framing of the "cyber crime" scheme*

So while users and citizens were tasked with "teaching themselves" to use technologies in safer ways, the needs of the private sector were elevated to receiving far more serious attention. Additionally, closely allied with the cybercrime focus of the convention was the overlapping focus on cyberwar, which concerns states and governments:

> Governments could theoretically launch hostile attacks on another State's critical infrastructure, such as its telecommunications system or key public services, or attempt to acquire sensitive information. Actors who are not governments may attempt to do the same thing. The complex nature of cyberspace makes such incidents liable to produce misunderstandings, unforeseen crises or even conflicts in the future. Meanwhile, terrorists have and will continue to use it to plan attacks and flood chat rooms with their ideology to recruit their next generation.
>
> *~the UK Foreign Office's framing of the "international security" scheme*

Overall, then, though the London Agenda helped to cultivate public awareness about internet freedom issues, it is both surprising and telling that cybercrime and cyberwar norms came to dominate the agenda – after all, it was a meeting organized by a state for states to address the risks facing "critical infrastructure." Civil society's user-level perspectives did not receive any serious attention nor were norms and frameworks developed to address users' needs. This second point helps to support my claim that state-based stakeholders have an insular approach to designing technology policy that doesn't speak to the important normative nuances of designing technology policy in the interest of human rights or democracy promotion.

To further support this claim, we can also examine the wide range of policy documents that were distributed by states at the gathering to shape the discourse around and after the convention, with telling examples like: "Cyber Security Strategy" (Estonia's Ministry of Defense), "National Cyber Security Policy" (India's Ministry of Information and Communications Technologies), "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (the US Office of the White House), "The National Cyber Security Strategy" (Holland's Ministry of Security and Justice), "Cyber Security Strategy for Germany" (Germany's Federal Ministry of the Interior), "Canada's Cyber Security Strategy" (Canada's Office of Public Safety), and "Defending the Networks" (NATO's Policy on Cyber Defense).

Across these policy documents, only three normative concerns areas are consistently presented and only concern the welfare of states and providers (but not citizens): a) cyber espionage; b) cyber terrorism; and c) cyber crime threats. Furthermore, as part of the coordination strategy to deal with these three threats to "critical infrastructure," I find that state-

based cooperation, industry cooperation, and sometimes academic cooperation are often explicitly highlighted in these documents, but very few instances of meaningfully coordinating with civil society organizations and issues of communication rights are suggested or expounded on in these policy discussions.

In order to illustrate these consensus themes for non-specialists, these governmental policy analysis documents also provided "recent examples" to illustrate and support their state-centric norms. The choices of these examples also reflect the London Agenda's focus on state security issues. Despite the wealth of existing studies and calls from civil society in the aftermath of the Arab Spring, the London Agenda consistently drew on limited examples of criminal incidents (e.g., malware programs like Stuxnet, botnets like BredoLab, which originated from Armenia, and hacktivist organizations like Wikileaks), but somehow missed the countless and obvious examples of private sector collusion and governmental abuses of digital networks for political and non-democratic purposes in the Arab Spring. General approaches towards responding to these cybercrime threats primarily focused on public-private partnerships (i.e., between states and the private industry sector), but suggested few to no strategies for allying with digital activists and civil society. Again, references to or acknowledgements of civil society's utility and importance are not found. In the rare event that users and civil society were referred to, the language of these official policy documents encouraged individual responsibility on the part of users, not substantive cross-sector cooperation with civil society groups: "All users (individuals, businesses, institutions, and public bodies) should take appropriate measures to secure their own ICT systems and networks and to avoid security risks to others. They should take care when storing and sharing sensitive information and respect the information and systems of other users." (London Agenda, 2011)

There are, however, at least two notable exceptions to the general lack of civil society and human rights issues in the London Agenda. The official policy language of both the United States White House as well as the Council of Europe contains overt recognition of users' rights and human rights responsibilities. The United States' language is directly built into its framing of the "Internet Freedom" discussion and refers to the importance of supporting "fundamental freedoms." To further the goal of supporting fundamental freedoms, the United States' policy priorities during the London Agenda were to:

1) directly support civil society actors with safe and reliable platforms for freedom of expression and association; and
2) collaborate with civil society actors to establish norms and standards to protect activists, advocates, and journalists in particular.

The Council of Europe was even more explicit, with aims to maximize rights and freedoms for internet users by developing:

1) a charter of rights for internet users; and
2) human rights–based guidelines and best practices for governments and internet intermediaries.

Despite these rare inclusions of users' and civil societies' needs, the responsibilities of the private sector and states' responsibilities in developing a language of rights and democratization with regard to internet freedom issues were notably missing during the formation of the London Agenda. Serious policy references for inserting human rights into the agenda remained limited, but some public comments during the event nonetheless reflected, however briefly, on the intersection of internet freedom and human rights:

- "The Arab spring used Facebook to mobilize, twitter to live stream and YouTube to report."—Helen Clark, UNDP
- "Twitter and Facebook did not cause revolutions, but were catalysts."—Atiaf Alwazir, Yemeni activist
- "60 governments are blocking access to the internet for their citizens."—Uri Rosenthal, Dutch Foreign Minister
- "Social mobilization is more effective and more volatile because of the internet."—Helen Margetts, Oxford Internet Institute
- "The virtual world is the real world."—Ahmed Ashour, Al Jazeera

To summarize, the norms that have emerged from the London Conference on Cyberspace privileged the interests of state-based actors above others, and categorized technology providers and the private sector as the victims of internet freedom-related threats and risks. Consequently, the normative outlook and stakeholder commitments of the London gathering were overwhelmingly constrained by the organizers and focused on addressing *cybercrime*, *cyberterrorism*, and *cyberwar*. They did not substantively entail involving civil society or

considering the human rights violations by the abuse of internet freedom, or technology providers' aid in doing so during the Arab Spring. Consequently, very few normative standards and stakeholder relationships between civil society actors were cultivated, and an important opportunity was missed to broaden the range of ways in which state-based actors could have thought about incorporating affordances for human rights and democracy promotion into the policy discussions of internet infrastructure and internet freedom.

In short, the London gathering and affiliated state-based actors have had a structural and normative impact on the formation of the global internet freedom proto-regime and the state-centric and private-sector friendly norms that it has cultivated. These norms and ideological commitments frame internet freedom as a matter of economic securities and threats, but exclude human rights and civic responsibilities as important domains for states to act on and encourage stakeholder commitments to be cultivated in preserving. The London Agenda reflects this tendency by state-based actors to focus on "internet securitization" discourses that promote states' rights above the rights of others, to the exclusion of civil society and users' experiences in the shaping of the global internet freedom regime.

Activist Norms: Building a Digital Scaffolding for Civil Society

As we saw in the network distribution of internet freedom stakeholders, civil society actors are the most influential overall cluster in the global network of stakeholders. Most importantly, it is the LiberationTech-affiliated cluster of policy experts and digital activists described earlier that predominantly hold the most influential positions in various think tanks and global NGOs interested in internet freedom promotion. While state-based stakeholders from Western democratic regimes were busy discussing and shaping the London Agenda, at the same time on the other side of the globe in California's Silicon Valley, a very different segment of stakeholders from these think tanks and NGOs were organizing a very different approach to promoting internet freedom.

In October 2011, a lesser known organization called Access (previously called AccessNow when it was formed after Iran's Green Revolution) had quickly organized the largest human rights convention and internet freedom conference to date: the Silicon Valley Human Rights Conference. With the backing of the US State Department and generous funding from prominent technology corporations, Access kicked off the event with opening talks by Michael

Posner, Secretary of the US Department of State's Democracy, Human Rights, and Labor department, and one of the LiberationTech's community's most influential opinion shapers and policy experts, Rebecca MacKinnon. Funding and sponsorship for this digital activist-friendly gathering came from no less than Google, the Ford Foundation, Facebook, Yahoo!, Mozilla, Skype, AT&T, and the Electronic Frontier Foundation. In counterpoint to the London Agenda, this cluster of stakeholders was formulating its own set of norms and standards, called the "Silicon Valley Standard." I argue here that this set of norms, developed by technology providers and designers on one hand, and civil society and digital activists on the other, is competing directly with the state-centric norms reflected in the London Agenda. To examine how these different norms might profitably collaborate or compete with other norms in the internet freedom proto-regime, we must not only observe the network of stakeholders competing for them, but also pay close attention to the differences in focus on contrasting problem definitions propagated by this civil society approach.

First, from the perspective of convention organizers and key figures, the Silicon Valley Human Rights Conference seamlessly integrated established and influential technology policy advisers (e.g., Electronic Frontier Foundation, Citizen Lab, Global Network Initiative, etc.), major governmental representatives in key agencies engaged with foreign policy issues (e.g., the US State Department), indigenous activists experienced in digitally enabled political organizing within repressive political systems (e.g., the Guardian Project, SMEX, Diaspora, etc.), and public policy heads of private sector companies (e.g., Facebook, Google, Twitter, etc.). This allowed for a far more heterogeneous set of experts representing technology designers, users, and regulators to confront and reconcile competing norms about internet freedom promotion.

The overt framing of the gathering itself was digital politics and its impact on human rights. This framing was important because it legitimized a broad and open agenda regarding the need for discussion of issues of internet freedom to recognize users' interests alongside state-centric concerns. Additionally, registered attendees numbered in the hundreds and attendance was encouraged from all sectors, including journalism, academia, and the technology sector. So in addition to members of think tanks, governmental agencies, and high-tech businesses, the Silicon Valley gathering featured a critical mass of high-tech civil society organizations from across the spectrum, especially those political activists from repressive political systems most effected by internet freedom policy promotion:

> A conference examining and exploring how the human rights and high tech sectors can better plan for and manage the human rights implications of new technologies. It is an outcome-oriented event, centered on private roundtables and public sessions, that will bring information and communications technology (ICT) *entrepreneurs, executives, and engineers* together with *policy analysts, human rights specialists and charitable organizations* in the field. The conference is sponsored by Google, Facebook, Yahoo, Skype and Mozilla, amongst others, and held *with partners from the civil society sector*.
>
> *~ official conference announcement by Access; emphasis mine*

In contrast to the London Agenda, the Silicon Valley gathering was convened as an explicit response to events, problems, and failings of various stakeholders during key democratization movements like the Arab Spring. This allowed for a grounded historical context in which to directly identify the complex problems and the diverse stakeholders facing them:

> Companies and civil society are constantly dealing with privacy issues at home, security issues abroad (particularly during moments of political instability), and ethical issues. We've seen the exciting role communication technologies companies and social media platforms played in enabling people to challenge and topple authoritarian regimes in the Middle East and North Africa. […] Yet while the communication technologies have undoubtedly had a net positive impact on our global community, it has also, for example, enabled certain governments in their efforts to quash personal freedoms and disrupt social movements striving for reform. It is not the first time that technology has been used effectively and simultaneously for participation and exclusion, for revolution and repression, but the dramatic events unfolding in the Middle East and beyond have raised many questions about the rights and responsibilities of the technology sector globally and the relationship between corporations, governments and end-users—both here and abroad.
>
> *~ summary statements from the Silicon Valley Standard*

This framing of the stakeholder summit differentiated itself importantly from the state-centric norms of the London Agenda. However, this gathering was still able to design some compelling technology policy objectives included in its comprehensive Silicon Valley Standard. Unlike the push-model approach of the London Agenda (i.e., applying regime-determined policy language to the internet freedom agenda), which focused primarily on the three issues defined earlier (cybercrime, cyberterrorism, and cyberwar), the Silicon Valley Standard developed from a more grounded and grassroots pull-model. Instead of pushing state-determined concerns about technologies onto stakeholders, the Silicon Valley Standard emerged as an outcome of the meetings and discussions itself, and summarized fifteen major norms and issues adopted at the conclusion of the stakeholder gathering from fifteen working groups.

These norms were crowdsourced directly from a range of stakeholders and experts by directly consulting members of the private sector and civil society actors who attended the deliberations. These fifteen points can similarly be summarized as fitting three broad sets of norms, understandings, and expectations, but are characteristically and fundamentally distinct from the issues identified by state-centric actors who formulated the London Agenda. First, there was a clear recognition that technology companies do in fact enable, support, or threaten the end user's (i.e., internet users) freedom of speech, access to information, and freedom to associate, and thereby share a burden of responsibility towards their users (something the London Agenda did not do). Therefore, privacy of users (but not necessarily anonymity) should be the point of focus from the outset when discussing internet freedom, and total transparency of how social data is collected, processed, and protected should be encouraged.

In addition to existing human rights and business sector frameworks, the Silicon Valley Standard championed the idea that the best knowledge in dealing with new challenges comes directly from the frontlines, i.e., the users themselves. In other words, technology companies should regularly monitor the human rights impacts of their tool deployment and update their policies and procedures regularly. Second, there was a push to integrate human rights as a framework at the policy and practice level of the private tech industry, and civil society activists championed for Ruggie's "Protect, Respect, Remedy" approach to be adopted by the UN as Guiding Principles on Business and Human Rights, and, further, that internet regulation should only be approached if the fundamental openness, quality, and integrity of the internet backbone is at stake—i.e., the multi-stakeholder dialogue model preferred by the private sector should

prevail. Any regulations covering "internet intermediaries" like ISPs (Vodafone, AT&T) and content hosts (Google, Facebook) should not require them to determine the legality of the content they host. However, this second set of norms also enlisted technology companies to generally resist any efforts by governments and law enforcement to limit or interfere with their services during moments of crisis. In later chapters, particularly in Chapter 5, I will unpack this tension between infrastructure providers and content providers, but for now it is enough to recognize that the Silicon Valley Standard privileged securing autonomy for content providers from any form of data traffic manipulation, either for costs or political reasons.

Third, the Silicon Valley Standard acknowledged that human rights concerns should also be built directly into the technology innovation and research and development phases from the outset. And to do so, technology companies should be responsible for innovating basic levels of security tools and protocols through better encryption software. Furthermore, by recognizing that both technologists (engineers, developers, programmers, etc.) and their products (tools, code, software, etc.) have an impact on human rights, it was acknowledged that civil society actors should be enlisted directly to help shape both the process of innovation and production of new technologies, not only in designing policies and regulations for these tools. And finally, the Silicon Valley Standard held that mobile telephony, social networking apps, and visual media technologies are of paramount focus given their wide usage and "revolutionary capacity."

Overall, then, it seems that when states define the norms behind promoting internet freedom, they focus on securing the internet backbone from terrorists and criminals by pushing their norms onto other stakeholders (or ignoring them). But when civil society and digital activists define the norms, they take a much more nuanced and even-handed approach that works to enlist stakeholders with distributed responsibilities that embrace the multi-layered nature of digital infrastructures. Nonetheless, it is notable that the private sector has thus far seemed to be a passive participant in constructing the norms—neither introducing, nor resisting any. Instead, technologies providers again simply seem to be passively ignoring the internet freedom norms construction process overall.

Conclusion: What of Technology Providers and the Private Sector?

So how do the two norm making environments described previously compare with each other? Because the London Agenda placed state autonomy as the perspective from which to shape the

internet freedom norms, it focused primarily and most explicitly on *cyberwar*, *cybercrime*, and *cyberterrorism* issues that states see as the primary problems and threats facing internet freedom. These concerns also constrain the work of promoting internet freedom to securing the internet backbone, which is an important but limited piece of the broader digital infrastructures at stake. This has incubated a top-down norm-generating stance where states' interests and visions were handed down primarily to private sector stakeholders. This also meant that civil society was substantively excluded from contributing to the norms-construction process. The analysis of the making of the London Agenda is a good illustration of why states are currently not good generators of a coherent internet freedom regime. This is because a viable regime cannot be consolidated by simply ignoring core members of the effected community. Furthermore, little substantive input from civil society was garnered at all, even though civil society actors seem to be generating most of the original thinking and new norms as was illustrated in the counter example from the Silicon Valley Human Rights Conference.

In contrast, because the Silicon Valley Standard was led by a focus on the end user, the ideological underpinnings of this norm-generating system focused on integrating human rights concerns from the bottom up. In contrast to cyberwar, crime, and terrorism concerns, what is exhibited in civil society–led norms is a far more nuanced understanding that meaningfully addresses the democratic potential of digital technologies and necessarily goes beyond simply securing the fundamental internet backbone. The civil society approach introduces system users, technology designers, and infrastructure providers as influential actors who share responsibilities in securing their distinct pieces from the multi-layered digital infrastructure. This means that the private sector and civil society actors are regarded as potential sources of influence both on the design of the technologists as wells as on the policies regulating those tools. In comparison to the state-sponsored London Agenda, the civil society-led Silicon Valley Standard was sponsored by states (e.g., the US Department of State), led by the activist community (e.g., Access), and provided the private sector actionable goals to produce both technical innovations and new self-regulation standards (e.g., Google).

To summarize, there seems to exist a fundamental paradigmatic difference between the state-sponsored security–oriented approach to internet freedom promotion and the private sector and civil society partnership focused on innovation cultivated in Silicon Valley. State-backed approaches to internet freedom seem to take an overtly technologically reductionist (and

fatalistic) perspectives on the importance of "critical" internet infrastructure. In this approach, infrastructure is seen as a pre-determined structure that can only be secured by states and regulated by providers. On the other hand, the norms designed by civil society actors in collaboration with the technology community seem to envision a constructivist ideology for promoting internet freedom where both the technologies and social practices can be re-engineered more cohesively alongside coherent legal norms respectful of human rights.

In this civil society-defined approach, private actors seem to more openly acknowledge their role in and responsibility for redesigning their systems and tools by better understanding the lack of security and anonymity in information infrastructure. Furthermore, civil society actors, drawing on the experiences of users in the Arab Spring and related events, seem to be backing the perspective that users also rethink and reimagine ways of using existing systems. From the field of technology development studies, this parallels the approaches explored in studies of "human-centered design" and "human-computer interaction." These norm making approaches go beyond the construction of simple legal regulations towards ways also building better and safer tools that must respect citizen's privacy whilst balancing security concerns. So while state-based actors tend to imagine digital tools as static objects that can have a general social or political impact, civil society actors, in contrast, recognize that tools have potentialities, which are built into digital tools during the design phase, but that can also be nurtured through better policies and regulations that apply lessons from their users' experiences.

This contrasting of two very different ways of generating new norms also helps to explain why civil society actors consistently champion the idea that human rights concerns should be integrated at the most basic level of creating a digital tool itself, not simply regulating the tools after they have been fully constructed. In this way, technology innovators and access providers share a burden of responsibility, unlike the London Agenda's relegation of this burden to users' "individual responsibility" in learning safer practices in using existing tools. In order to explore this interesting social constructivist and interventionist approach towards promoting internet freedom, in the next chapter (Chapter 4), I investigate the core community of LiberationTech technologists identified earlier in this chapter. LiberationTech refers to a Stanford-based community of technologists and online discussants that have been debating and designing digital tools to support political activists in repressive political systems since 2008. If we want to

understand the activist community's norms for defining how to pursue internet freedom, studying the LiberationTech community is an appropriate site to start such an investigation.

Chapter 4 – Political Technologists and Civil Society

"People think beyond the normal capabilities of an object, and try to surpass the limitations it imposes on itself. [...] This kind of object imposes a limit on the user, because it comes with an established technological code, which hardly ever satisfies all of the user's needs, and sometimes he exceeds these needs. He manages to go beyond the object's capabilities. [...] And it represented many ideas. Especially the audacity to confront very complex technology and to risk one's life by using a potentially lethal object. [...] At that same time, I discovered the idea of technological disobedience [...] which allowed me to summarize how Cubans acted in relation to technology. How they disrespected the 'authority' held by these contemporary objects. How Cubans surpassed this authority. […] And in this way, they break all limitations: aesthetic, legal, economic. And this liberation is a moral liberation."

Ernesto Oroza, on Technological Disobedience in Cuba (June, 2013)

In Chapter 1 I argued that ICTs have altered the causal matrix available to political activists by offering new organizational capacities produced by meshing personal social networks of citizens and activists and connecting them to international human rights and news media observers, even in the most repressive political systems (Howard and Hussain 2013). Dissidents and activists around the world have exploited this digital infrastructure for political gain, while struggling with repressive rulers who are working hard to turn that very opportunity structure against them by implementing new surveillance and censorship strategies. Because of the important utility these new technologies seems to have given them, many activists have actively joined the international conversations being promoted by Western democratic regimes to promote internet freedom since the Arab Spring.

In the last chapter (Chapter 3), I also examined how the internet freedom proto-regime lacks cohesion in promoting coherent policies to implement internet freedom, and is currently balkanized between two opposing communities of practice generating and incorporating distinct and competing norms. Therefore, stakeholders have thus far failed to meaningfully consolidate a viable set of norms that policies can be enacted around that work effectively with the multiple layers constituting digital infrastructures. On the one hand, states are overly concerned with the internet's backbone and approach it as a "critical" infrastructure and ignore citizen's needs. On the other hand, civil society actors are producing some innovative norms and practices but lack the power to enforce them. In both cases, technology providers and the private sector have evaded meaningful participation and their responsibility for doing so. Given these precarious

issues at play, where might we find the best spaces or communities of practice working to consolidate these seemingly diametrically opposing normative frameworks? Where, if at all, is the substantive intellectual and experiential knowledge surrounding digital infrastructure politics and the social shaping of political technologies being formulated and aggregated? What new and innovative norms might emerge from here of use for internet freedom norms consolidation?

So far it seems that civil society-led initiatives have produced the most interesting sets of ideas and norms to draw other diverse stakeholders together. Unlike the state-led gatherings, when internet freedom promotion is led by tech-savvy civil society organizations and leaders (as exhibited in the Silicon Valley Standard), the involvement of technology providers and the private sectors is also importantly different. Here, the private sector stakeholders were invited explicitly by political activists to help design new security approaches and technologies in order protect users' rights. So there already seems to exist a fundamental paradigmatic difference between the state-sponsored security-oriented approach to internet freedom promotion and the civil society-led approach which explicitly partners with private sector stakeholders to produce both tools and policies as a broader way to promote internet freedom. We can say more than just that the *norms these communities of practice produce are different* – more importantly, *the ways in which these norms are negotiated and clarified* are also different! In contrast to state-based stakeholders, civil society actors seem to view digital infrastructure as much more malleable environment and therefore able to be redesigned with new affordances that promote internet freedom both through its architecture, and through its regulations and policies.

So in this chapter (Chapter 4) I extend the stakeholder analysis from Chapter 3 to ethnographically investigate the most novel and important category of civil society stakeholders that seem to be contributing the "first fix it, then regulate it" approach to promoting internet freedom. To do so, I focus on the community of technology designers and political hacktivists working on self-described "liberation technologies"—discussions, tools, and practices aimed explicitly at helping dissidents and human rights activists use digital infrastructures and ICTs for their political goals. I refer to these actors who are helping civil society stakeholders as *political technologists*. They are important because they are generating the important new norms about digital infrastructures that are most relevant to citizens and users. How they are doing this is also important: they are working hand in hand with users and activists to learn about the utility and pitfalls of their tools. Because these technology-savvy civil society experts exist as a

transnational community of authoritative-knowledge producers, they share normative and principled beliefs about the political importance of digital technologies, and are committed to promoting the democratic importance of their tools. Since 2008 this community of experts has crowdsourced the social ties, curated the expert and experiential knowledge of technology designers and technology users, and monitored every major international event and scandal involving ICTs between 2008 and 2012.

In short, this group is not a formal community of stakeholders, but it is a core sub-community of tech-savvy helpers working primarily with civil society networks more broadly. If we want to understand who civil society stakeholders turn to in order to learn about new tools and strategies they can test out in their political work, and why civil society-engineered norms and norms consolidation procedures are different, novel, and innovative in comparison to state-based approaches, we should start by looking here. Moreover, if we want to see who state-based actors also sometimes turn to for policy consultations on how to rethink their understanding of digital infrastructures, we should again look here. So who are these individuals, and what is the substance of their technical work? What are the motivations behind the new political technologies being built and deployed to support democratization initiatives by these actors? Who are their designers and what tensions must they face in producing such innovations? How have they come about, and where might we expect their efforts to proceed within the changing regulatory conditions under which states have traditionally enjoyed greater leverage?

4.1 Digital Activists' Very Own Geek Squad

It is March 2010, and Google London's pristine facility near Buckingham Palace is buzzing with recently arrived young tech-savvy and business-card-wielding professionals. This is the third meeting of the Alliance of Youth Movements Summit (AYM). I have arrived two hours earlier via London Heathrow from Seattle. I am in my second year of graduate study at the University of Washington. Having few ties to this particular tech-venture community, I am waiting somewhat anxiously in the lobby, contemplating how to make good use of my time at this interesting gathering of venture capitalists, IT professionals, and youth civic leaders. These seem to be an exceptional bunch, coming from venture capitals like San Francisco, Dubai, and Singapore, and rapidly climbing to the ranks of policy advisers in major social media companies and foreign ministries, or running their own start-ups. Soon, after a few hellos and brief introductions, I

begin to feel a little more at home. It seems that several of these people in their early to late 20s know or are friends with people who are also engaged in their areas of work in Seattle's University of Washington, Google's Kirkland facility, or Microsoft Research's Redmond spaces—while I don't personally know them, at least I can get a conversation started around the interesting projects I know that are happening in Seattle and the UW that seems to have piqued their interest.

Although at that time I did not know very many people at the London gathering, or their friends back home in Seattle, I was originally invited to attend at the behest of Jonathan, a friend who was working in a Seattle philanthropic organization at the time. Like his colleagues, and unlike me, Jonathan had moved to Seattle just a few months earlier from a PR and advertising job in New York. Prior to the job in New York he worked as a journalist in Egypt, Palestine, and the greater Levantine region. But in his new post in Seattle, Jonathan's day-to-day responsibilities revolved around networking with other new social enterprise startups backed with angel funding from the local technology sector. Most of his technology sector friends were based in the Bay Area's Silicon Valley, New York's Silicon Alley, or civic entrepreneurship and community engagement projects in Boston, Chicago, or Seattle. His other network of friends was based abroad, extending across major political capitals in Europe and the Middle East—people he met while working as a journalist, but whose company he came to enjoy because of their shared fascination with social media and internet politics.

When thinking about Jonathan's profile and the intersections of his work, it became more obvious to me why he was invited to this gathering—most of the people I was meeting were much like him: young, entrepreneurial, and boldly joining or starting up their own technology-based political activism projects. Some of them had migrated into this network after their tenure in the 2008 digital campaign to elect Barack Obama president; others had found their way in after being identified and invited to the gathering by the United States Department of State because of the success of their seed projects on digital media and civic engagement. But at this particular gathering in London, the overwhelming majority of young technologists and experts actually represented a broad cross-section of youth leaders from emerging democracies and authoritarian regimes. The training and sharing of digital media tactics for political participation and social change hasn't necessarily been a new phenomenon, but the active propagation of these strategies to repressive and downright dangerous political systems seemed radically new.

The March 2010 summit in London was the third and (thus far) final meeting of the AYM—previous meetings were held in New York City (2008) and Mexico City (2009), and backed by powerful individuals and supported by major digital corporations and governmental agencies. Among the 50 to 100 organizations that have attended the three AYM summits, there have been participants from Bahrain, Brazil, Colombia, Ecuador, Egypt, Guatemala, India, Lebanon, Malaysia, Mexico, Moldova, Nigeria, Pakistan, Peru, Saudi Arabia, South Africa, Sri Lanka, Turkey, and Venezuela. Organizers and attendees included the talents behind the Obama campaign's New Media Team (many of whom had moved to Blue State Digital, the consulting agency behind Howard Dean's 2004 and Barack Obama's 2008 and 2012 campaigns), and the US Department of State. Official sponsors of the AYM events included Meetup, Howcast, Google, Facebook, Twitter, YouTube, Gen-Next, Causecast, TechPresident, the World Bank, the RAND Corporation, the US Institutes of Peace, and the Center for Strategic and International Studies, to name the most visible. Collectively, these sponsorships indicated a mutual intersection of stakeholders positioned within international think tanks, international non-governmental organizations, telecommunications providers, and software and social media corporations.

For stakeholders attending meetings like AYM in London, this backdrop of political technologies and social entrepreneurs inspired collaborations and partnerships between technology designers and political activists. They seem to enjoy tinkering with or building their own social networking tools, platforms, and campaigns, both "at home" in advanced democracies and "abroad" in repressive nondemocratic societies. Who are these enthusiastic and ambitious proponents of political technologies and digital-enabled democratization initiatives? What might we learn by understanding the history of their ambitious, sometimes even unrealistic, campaigns? Not every activist network or cause in repressive political systems has the benefits or access to squads of political technology consultants and political communications strategists, but there seems to be a lot more that we can say and understand about the cultivation of new digital strategies and toolkits. Where is most of this work taking place, and how is it often accessed by the broader transnational activist community?

Online Discussion Forums for Curating Technical Expertise and Best Practices

One of the ways in which political technologists and digital activists have built their collaborative relationships, designed platforms, and experimented with new strategies has been through sometimes official and open, but often closed and by-invitation-only online discussion groups of likeminded enthusiasts. The AYM community has its own closed email list—but you have to be invited, and invitations are extended only to individuals who have been invited to and attended an AYM summit. On the other hand, the Progressphiles list is a far more exclusive network. It includes the technology designers behind the 2008 Obama campaign's digital media platforms. Many of them are members of the New Organizing Institute (known as the "West Point for organizers"), but far more were introduced to each other while working on the Obama campaign. Progressphiles is the main discussion community of data and technology experts working in American progressive politics. To be invited to this email list, one needs to be vetted and have the support of two existing list members. By cultivating safe spaces for like-minded politically oriented technologists or political activists seeking technology services, over the past several years, they have allowed their discussions and experiments to become more public. While the email lists for these discussion groups do not originate in authoritarian states, they are also being read by those in the cosmopolitan neighborhoods and activist cafés of Beirut, Tunis, Cairo, etc.

One specific online group came up in conversations consistently throughout my interactions with various young civic actors in the neighborhoods of Amman, Beirut, Cairo, London, San Francisco, and Washington DC: the *LiberationTech* email list from Stanford University started in 2008. Throughout my fieldwork and interviews, I have also noted the presence of this email community in the most surprising places. Here are three examples.

First, in July 2012, while living in a neighborhood in Tunis near Tunisia's most important telecommunications and computer engineering college (SUP'COM), I interviewed several political hacktivists who were active during the revolt to depose Ben Ali during the Arab Spring. The LiberationTech email list made a surprise appearance during this fieldwork, when a cache of hard-drive content and files was shared with me by Ahmed, an active Tunisian hacker who regularly competes in hacker competitions in Paris and Moscow. His data files included PDFs of technical manuals, political books, computer games, and four months of emails archived directly from the LiberationTech email list.

Second, in May 2012, while interviewing political activists in Beirut's Hamra neighborhood (historically known as the best place to meet dissidents and activists since the civil war) several of the fixers who were actively smuggling hard drives of footage documenting the Assad regime's human rights violations had ties to the LiberationTech community. These fixers do their work by assisting international journalists in finding local contacts and sources for their stories. They also do the dangerous work of transporting sensitive footage across the Syrian border into Beirut, where these images and footage of human rights violations are uploaded onto YouTube and shared with their news contacts to get the stories covered by global media networks. Frequently, these fixers discuss their network security concerns with technologists directly or closely connected with members of the LiberationTech email community. Indeed, many of the most important members of the LiberationTech community also come from Lebanon, Iran, and other places with non-democratic regimes. This anecdote from fieldwork indicates that the LiberationTech community not only exports strategies and best practices, it also provides a space where affected parties can share their experiences and expertise with mindful and concerned technology designers.

Third, near the completion of my fieldwork in Sweden, in August 2012, LiberationTech members again made appearances as the organizers behind "hackathons" and sponsors of conferences discussing the politics of information infrastructure. These actors are members of the LiberationTech email community, and they are also affiliated with the hacktivism communities of Anonymous, Telecomix, and other Western-based activism networks. Across these three examples, then, drawn directly from primary fieldwork, we see consistently that the LiberationTech email discussion network helps connect disparate actors from technology companies and security agencies based in Global North countries with political hackers and journalist fixers from the Global South. These relationships happen either directly (i.e., they know each other or consider each other to be collaborators) or indirectly (i.e., they can be connected to each other with very few degrees of social separation). This anecdote reflects the characteristic that LiberationTech's online discussion community is actually a transnational community composed of political activists seeking help with technology problems and technology experts motivated to help with civic issues. They mostly do their substantive work and collaborations online, but sometimes they also organize offline events and meet face to face.

In other words, they imagine themselves as a community and build and trade on social capital with each other to pursue collaborative projects.

Overall, the LiberationTech discussion network gives us a rare opportunity to listen in on and track the evolving perspectives of political technology designers and promulgators of these tools in repressive political systems. These factors, along with several unique advantages, collectively position this discussion email list above several others. Their purpose-driven ambitions focusing on the political application of ICTs and digital media inform the context and help explain the political ideology behind tech-savvy activism. These characteristics of the LiberationTech community are precisely what make it a useful context in which to examine more closely the ambitions and self-understandings of political technology designers, and their project collaborations and tool deployments. Doing so helps us to more deeply understanding why civil society stakeholders want to promote internet freedom and how certain norms and frameworks have been generated from their discussions and collaborations with allied technical experts.

4.2 Silicon Valley Roots: Origins of the LiberationTech Community, 2008-2012

The LiberationTech email discussion network started as a course-related project of Stanford University's Center for Democracy, Development and the Rule of Law (CDDRL) in 2008. One of the earliest topics of discussion to arise in this list began with a call in seeking to invest several hundred thousands of dollars with social entrepreneurs. The call cited interest specifically in social entrepreneurs possessing the belief "in the power of innovative and passionate individuals to change the world." The handful of awardees would receive $50,000 multi-year fellowships via angel funding to enable their visions under a venture capital model.

The language of calls for funding like these was not without cause, because sponsoring organizations and individual benefactors often had their early success in Silicon Valley's economic boom period of the 1970s and 1980s. These angel funders made their fortune by investing in companies like Activision, Apollo Computer, and Dionex. Technology and innovation was the culture shaping these early participants' worldviews. Furthermore, early calls like the one in 2008 also came from family foundations that also have a history of leadership in international social development platforms and organizations like the United Nations Development Programme. So from its inception, the LiberationTech community was up to something interesting: they were drawing in the funders and venture risk takers of the IT industry

and extending their domain to include social entrepreneurship and international development initiatives. The formation of the LiberationTech community was bringing together technology designers and civic entrepreneurs. As a result, for the majority of its first two years of activity, this discussion community developed quickly, but also remained primarily a forum for news and calls for sponsorship that helped build its ties with Silicon Valley–area funders, technologists, and activists.

In those early years between 2008 and 2010, it was also not uncommon to see just under thirty to forty updates a month, mostly revolving around helping local nonprofits find web designers and programmers for their needs (see Figure 4). Some calls for proposals joined together e-business ideas with social causes, and others simply shared news and articles about ICTs being applied broadly in the international development field to solve social problems, like providing mobile banking to fishermen in villages, setting up internet kiosks in slums, etc. Between 2008 and 2010, this community was mostly a network bridging the geeky and the cool with examples of prototypes and experiments from around the world. During this time the total membership of the community was also quite small, and included less than 100 total members irregularly contributing a few messages over the entire twenty-four-month period.

But all of this began to change rapidly in the summer of 2009 because of what was taking place a world away in Tehran, Iran. Sparked by the fervent discussions surrounding the importance of Twitter and social media tools during Iran's 2009 contested elections and the ensuing Green Revolution of student-led protests against the theocratic regime, the LiberationTech discussion network was jolted to life with activity and debate. The events following the Green Revolution helped to solidify an identity based on an impossible purpose: designing and testing the utility of ICTs to overthrow despotic regimes.

The community developed a concerted focus on examining the political uses of social media tools by dissidents during the mobilization period. These new kinds of discussion topics went beyond ICTs for development, and the membership and active discussants exploded on the list. During the first half of 2010, this community rapidly propelled itself from a general focus on technology and social entrepreneurship to having an overt and defining interest in the digital politics surrounding repressive states.

This ascent took place for two specific reasons that went beyond just the discussion of current events and dealt with the actual substantive work being done by its members and the

tools they were developing. First, a cryptographic software designed to help Iranian dissidents maintain online connections in the face of government efforts to locate them came to the forefront of debate and discussion on the list. LiberationTech members vocally expressed their concerns about the closed technical details of the technology. This tool and its production process violated the community's basic norms, namely that all collaborations should have an open-source approach. This culture was aimed at opening up any strategies or tools to be vetted by members in the list who saw themselves as "hackers who know their stuff." The underlying idea here was that if you said that your tool could afford certain practices or protect from certain risks, community members should first test it out before users deployed it for real (and dangerous) political acts in repressive countries.

Second, Facebook's content regulation norms became the center of debate when the site shut down portions of a community campaign page focused on boycotting Target. This conflict was picked up by the news media, who framed the issue as "Grass-roots activists organizing boycotts against large corporations like Target stores and BP now find themselves directing some of their ire at another corporate monolith: Facebook" (Email communication: September 18, 2010). Additionally, the United Arab Emirates, Saudi Arabia, and India began pressuring RIM, the company behind the popular Blackberry smartphones, to change its basic infrastructure security protocols. Because the Canadian company refused to give these regimes the technical capacity to monitor data transmissions over its networks, members from LiberationTech were quick to begin assessing the corporation's decisions and investigating the normative claims being championed by these regimes and corporations. One member, foreshadowing the NSA breaches we were to see years later, astutely commented:

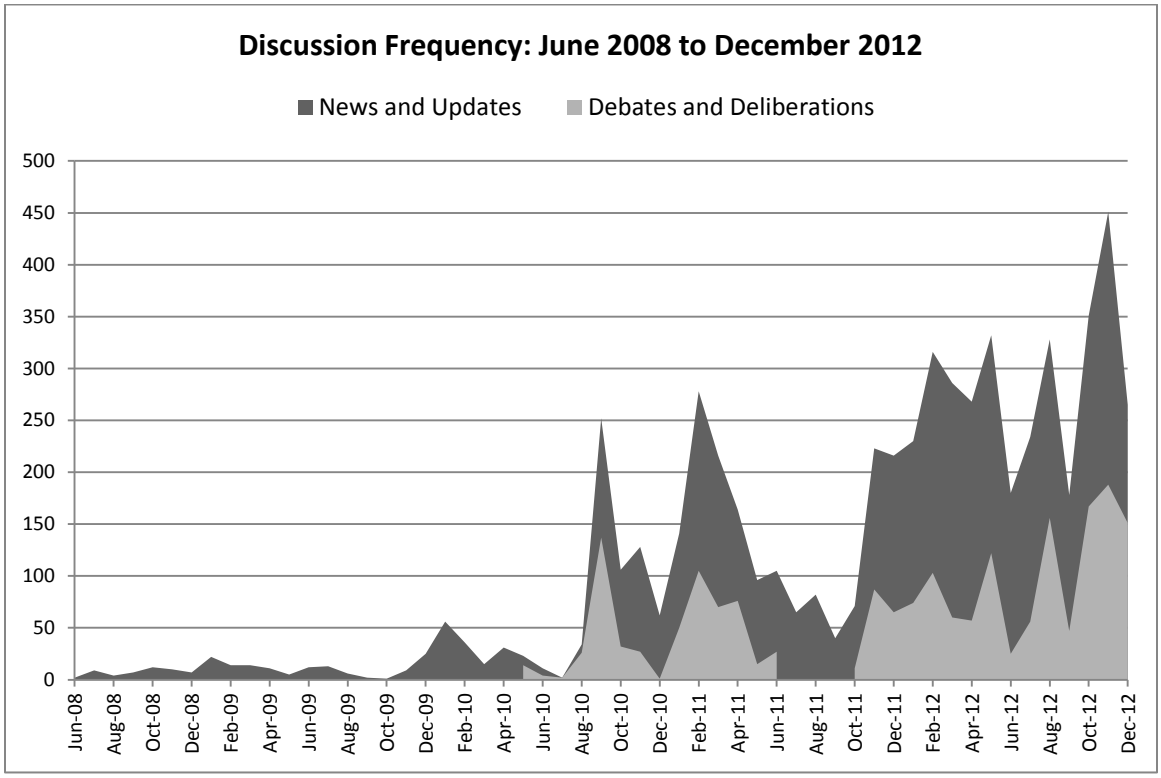
> "The tyrannical mentality of the UAE, Saudi and Bush DHS authorities are far from aberrational. They are perfectly representative of how the current U.S. administration thinks as well: every communication and all other human transactions must be subject to government surveillance. Nothing may be beyond the reach of official spying agencies. There must be no such thing as true privacy from government authorities."
>
> *~ Email communication: September 27, 2010*

So in addition to the tools they were designing, these political technologists were also facing challenges in the regulations impacting the basic layer of the internet backbone that enabled their tools and strategies to begin with. Collectively, incidents like these also helped to solidify the foci of this community around some core new challenges and outcomes: a) tool development and testing to aid democracy promoters and digital activists, b) monitoring the norms and behaviors of technology powers and their collusion with state powers, and c) assessing the regulatory policy frameworks of regimes themselves who were increasingly restraining the digital infrastructure that activists were making use of for political purposes.

The LiberationTech community's identity-formation period following the Green Revolution in Iran also corresponded with a critical mass of incidents around the world. Digital activism expanded to encompass more than just the use of existing tools for political participation. This rise in activity and discussion topics correlated with the increasing number of observations from around the world where technologies were being seen as impacting politics and democratization. Digital activism also meant promoting activism to protect the utility of ICTs and digital infrastructures. Through this important phase of community growth and increasing cohesion, LiberationTech membership increased exponentially from generating less than fifty messages per month by a small community of under thirty active members to a phenomenal 200+ messages and debates by a rapidly expanding collective of 150 active contributors by the end of 2010.

Who are these new individuals that began to make up this active collective of political technology experts? What expertise did they offer and in which institutions or contexts were they imbedded? Having a deeper understanding of their experiences and backgrounds is particularly important because while the popular discourse about technology-savvy activism often frames them reductively as naïve enthusiasts suffering from bouts of technological determinism, this does not tell us very much about the substantive issues underlying the politics of digital infrastructures and how these new risks were being identified. In the next section, I describe the types of activities that have been cultivated by political technologists, as well as their institutional linkages enabling their sophisticated skills and policy perspectives.

Figure 4: Discussion Frequency of the LiberationTech Online Community



Note: Figure prepared by author based on data collected from the LiberationTech email list. Each distinct email was organized and aggregated based on email-subject and treated as a unique case exhibiting detailed case information within the email body. Email subjects were aggregated and those that generated fewer than eight responses were categorized as "news and updates." Those topics which generated more than eight responses were categorized as "debates and deliberations." The cutoff of eight was established through grounded case readings of 20 percent of all individual emails paying attention to the diversity of discussants and longevity and depth of the topical discussion.

Individual Expertise

The collective of political technologists that formed around the LiberationTech email list can be conceptually described as a "community of practice" (Wasko and Faraj 2000). The term refers to groups of people who organize around a shared craft and set of problems, and are gelled together with the social capital and group identity that they often form as an outcome of their collaborative efforts. Communities of practice have been examined particularly in virtual communities, like email discussion networks, and the concept is apt for framing how and why the individuals in question have come to interact with each other.

First, these members shared normative beliefs about the political significance of communications technologies and digital informational tools they wanted to examine and design. Second, they shared a complex causal understanding that these political technologies can have important impacts on the users employing them. Third, they shared strong notions of community standards regarding open software and peer-reviewed processes for the development, deployment, and uses of said tools. Finally, they shared concerns about the policy developments surrounding political technologies at the hands of both private sector technology corporations and state-based governmental agencies, with a presumption that the welfare of users also depends on the regulatory norms surrounding digital infrastructures within which ICT tools and web-enabled practices are embedded.

In order to understand these themes in greater detail, it is important to examine the actors themselves and their products. But doing so is not so simple, given that communities of practice are not necessarily organized formally by organizational hierarchies nor constrained by overt and binding relationships, like institutions and organizations. To further complicate matters, many of the members in this network are self-described hackers, who tend to remain private or anonymous to protect their identities and reputations. While not everyone on this email list is a hacker, many self-described hackers work for security companies and governmental agencies and are bound by nondisclosure agreements and obligations. On the one hand, these conditions limit their ability to publicly discuss or speak openly about their activities and concerns. But on the other hand, they seem to enthusiastically discuss these potentially risky subjects openly and frequently on the LiberationTech email list.

Despite the lack of a binding hierarchy in the discussion community, there are also vast differences between the most central and active contributors and the long tail of interested

observers and listeners who contribute far more infrequently. For example, Ahmed, the Tunisian hacker described earlier in this chapter, reads and archives the discussions on this email list, but has never posted or contributed to the discussions himself. This variation in contribution is sometimes due to the unequal distribution of skills and interest, as a large number of less active contributors are there simply because they are interested in staying up to date on the latest technical discussions or getting help from more knowledgeable programmers or strategists. Some are also journalists who are present on the list because they want to report on a new topic they don't fully understand. Others are foreign policy makers who want to do the same, and use the list to invite these experts to advise them on policy frameworks by helping to draft policies or participate in events where these policies are being debated.

Despite the varying distribution of engagement and contribution among the total community of participants on the email list, to date the total contribution of discussions, debates, and deliberations have totaled more than 6,000 discrete email messages (see Figure 5). These messages have been shared by a visible set of 850+ contributors, while the total community membership size is well over 1,500. It is difficult to say more about the list because although it is technically[16] public, the membership lists are not. List moderators have announced several times how best to treat the site, and have consistently shared concerns about list members residing in places like Tunisia, Lebanon, and elsewhere, where their public involvement in political technologies and hacktivism would endanger their welfare. However, as Figure 5 also reveals, there is also a visible and heavy skew in the activity levels and centrality of actors. Although nearly 1,000 individuals have contributed to the discussions over the past four years, less than 100 members have been responsible for contributing well over 66 percent of the discussions and deliberations. In other words, 100 top contributors have shared over 4,000 messages (66 percent) over the past four years about internet politics.

This is important because the knowledge being produced, curated, and evaluated surrounding the development of political technologies is actually generated by a core group of knowledge experts. These experts do most of the hard work in designing and deploying

[16] Visible because the full registry of email addresses and names is not publicly available, to protect the identities at-risk activists and dissidents. However, when individuals participate by sending a message to their list, their identities are compromised because their email addresses and registered names are made visible to the community members (and the internet public—the email list and message are crawled by Google).

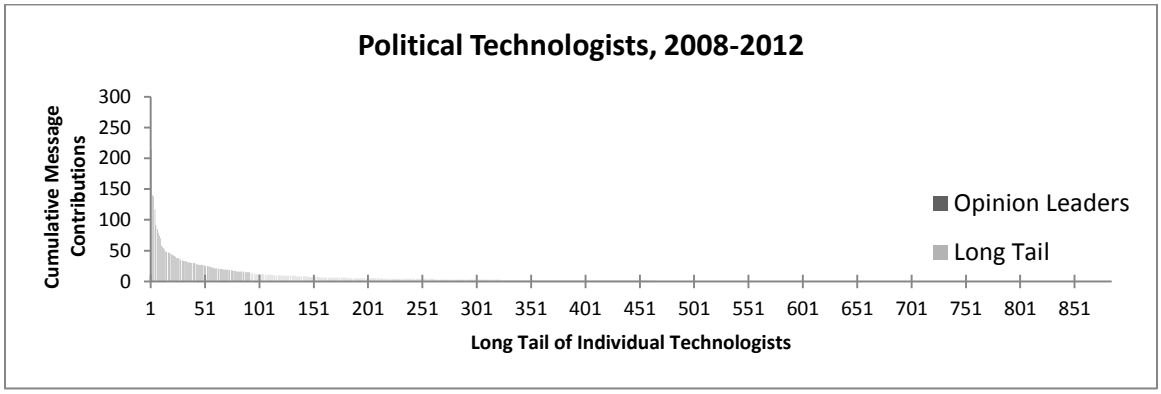
technology toolkits in repressive political contexts, although the long tail of community members also helps crowdsource expertise and experiences from far corners of the globe. Many of them are well connected, have advanced graduate training in a small number of the world's top research programs, and though not all are expert technologists, the vast majority are. They are located in governmental agencies, work as international journalists in dangerous conflict zones, belong to prestigious academic institutions and technology labs where their research profiles focused on digital politics. They also include political hackers who were active during the Arab Spring protests, internet policy experts who share high-level positions in internet regulatory agencies, as well as individuals positioned within top policy think tanks. The fact that these top 100 contributors inhabit such an important leadership role in the LiberationTech community and share roots in disparate and diverse institutions helps to further justify profiling this community and its expertise is crucial.

So who are these core 100 technically-skilled contributors? First, approximately 85 percent, or the overwhelming majority of them, can be described as male technologists, many of whom have sophisticated technical engineering backgrounds, and several of whom describe themselves as hackers working in the security industry. Of the less than fifteen women in the community, three or four can be categorized as technologists working on designing, programming, and testing hardware and software applications. The remaining minority of nontechnical actors includes a diverse group of academics, lawyers, social entrepreneurs, self-described "policy wonks," bloggers, and journalists. Therefore, the overarching archetype of the top knowledge workers in this community reflects the stereotypically young, male hacker, writing code and debating appropriate application of security protocols. They often work for security consultancies and corporations to make a living, but in their off hours have a passion for open-source development.

Second, these members have all attended an overlapping small number of research institutions and conferences. These labs and discussions have allowed this collective to train and acquire its technical skills and specialized knowledge base. They work and share information on the email list, but they also extend these collaborations offline. The core network of supporting institutions where they meet or learn their trade includes American universities: Harvard and Stanford, as well as MIT and Berkeley. Most of the tech-savvy programmers seem to have trained in one of these top institutions. To a lesser degree, Georgetown and Yale frequently

appear as institutions where the lawyers and self-described policy wonks acquired their graduate and law degrees. Some German and British universities also make the cut, with Oxford being the most common node. Canadian and Scandinavian universities are more peripheral but still important spaces for technology labs. As an important exception, the University of Toronto, home to the Citizen Lab, has been an important space outside the American network of universities, although it has strong ties within the network of American institutions.

Figure 5: LiberationTech Email List Participants by Frequency of Contributions



Note: Figure prepared by author based on data collected from the LiberationTech email list. Each email address contributing a minimum of one email between 2008 and 2012 was tabulated by total contribution of emails. Missing data includes those who belong to the email list but have not contributed any content (i.e., they are invisible to the community).

Supporting Organizations

Beyond universities, the San Francisco–based Electronic Frontier Foundation (EFF) and the Washington, DC–based New America Foundation (NAF) represent some of the most important policy development spaces to which LiberationTech members have graduated. They have "graduated" in the sense that, at some point before taking these policy positions, they spent time in programs like Harvard's Berkman Center for Internet and Society; Stanford's Center for Democracy, Development, and the Rule of Law; MIT's Media Lab; and Yale's Internet and Society Project where they developed their thinking and relationships to digital politics work. Outside the United States, Oxford's Internet Institute and Toronto's Citizen Lab seem to be two prominent institutions connected to this intuitional network. San Francisco's EFF and Washington's NAF are particularly worthy of further discussion.

The EFF was founded in 1990 as a nonprofit organization focusing on the intersections of law, freedom, and privacy and provides legal support, produces legal briefs, and protects both individuals and technologies from governmental intrusions regarding the privacy and protection of users and data. Some LiberationTech members have referred to the EFF as the "ACLU of Internet Freedom." The NAF, on the other hand, came about much more recently, in 1999, under the leadership of Google's chairman, Eric Schmidt, and deals with private industry-based concerns on technology policy. The EFF grew out of the challenges that came about with the arrival of the Information Age during the 1980s and 1990s in the San Francisco Bay area, and now shares its workload with a growing number of similar supporting outfits like the Center for Democracy and Technology (Washington, DC), Computer Professionals for Social Responsibility (Seattle), Privacy International (London), and, most recently, the Global Network Initiative (GNI) The GNI was established in 2008 to represent a coalition of corporations, nonprofits, and universities and places digital rights in the framework of the International Covenant on Civil and Political Rights. The EFF and related organizations illustrate a steady advancement in the treatment of technology policy focusing on data privacy and its consequences for human rights and political freedoms.

In contrast, Washington's NAF has focused on similar initiatives to the EFF, though it is less focused on legal counseling and more on lobbying and shaping public policy. The NAF has a noticeably new focus on technology policy. Established about a decade after the EFF, the NAF has cultivated policy making at the intersection of security studies, technology policy, and the

"new economy" being powered by digital media and internet infrastructure. Of particular note is its leadership history, which includes Google's executive chairman Eric Schmidt as chairman of the board of directors. Schmidt initially helped shape the mission of the organization to "emphasize work that is responsive to the changing conditions and problems of our 21st Century information-age economy." Furthermore, influential funders of the NAF include the family foundations of Eric Schmidt and Bill Gates (Microsoft), followed by the Silicon Valley Community Foundation, Google, the Open Society Institute, and the US Department of State. The NAF's fellowship program has actively supported several experts on internet politics and policy, of whom several have been members of the LiberationTech community.

Collectively, these new policy institutions seem to connect, and increasingly house, the most active members of the discussion community designing political technologies. Castells's (2011) concept of the "space of flows" helps describes the nature of work pursued by these political technologists and their institutional anchoring in North American and Western European research institutes and think tanks (see Figure 6). The concept of *space of flows* moves beyond traditional approaches of describing work spaces as passive and separate locations towards "the material organization of time-sharing social practices that work through flows." So, although the most important members of this online community of practice are based in several different organizations and industries, they are engaging in a connected body of work involving designing and deploying political technologies. These organizational nodes support and make possible continuous time-sensitive communications and information flows around a complex and rapidly changing issue area, and connect these individuals to a cybernetic community that also meets face-to-face in conferences, project meetings, and policy discussions. Applying this logic to the community of political technologists in question, we can observe that they are transnationally and globally located, yet communicate in real time to coordinate actions and develop norms of work-sharing habits. Due to the institutions including universities, research centers, think tanks, and technology industries that have provided them with the material resources for their work, it is possible to also identify the hierarchy of locations where most of this work is taking place.

First, all of the top locations are based within the political borders and economic systems of Western democracies. Second, all of these locations are strictly bound to the most industrially advanced Western democracies, and include the United States, the United Kingdom, Canada,

Germany, the Netherlands, and Sweden. Although the top ten cities around which the labor of political technologists are concentrated include the examples stated previously, the technology industries of the United States remain the home of the vast majority of this work. Third, Silicon Valley, which continues to have the largest presence of both venture capital and social entrepreneurship projects, is the single most important location of cultural incubation in influencing the ideologies and objectives of these actors. These political technologists in the aftermath of the Arab Spring are becoming central to the designing and shaping of the policies and regulatory frameworks surrounding internet politics. Therefore, the next section examines the actual technologies that have been developed and tested, and the technical work that these actors have conducted over the past 4-plus years. The following discussion covers both the successes and failures of their new experimental work. Doing so helps to illuminate important aspects of the norms underpinning their approach towards digital infrastructure and further tells us how they relate with different sets of actors and stakeholders influencing internet freedom promotion.

Figure 6: Global Distribution of Top Political Technologists

Note: Figure prepared by author based on data collected from the LiberationTech email list. Each of the top community members contributing well over 66 percent of all content were identified (n = 100). Biographical details about each community member were culled from their social media profiles, biographical details listed on personal blogs and websites, and curriculum vitae found on research laboratories and think tank agencies' websites. Furthermore, personal interviews with 20 top community members at participant observation sites provided additional personal background information.

4.3 Crowdsourcing and Synthesizing User-Experiences: Practices and Pitfalls

Over the past four years this community of approximately a thousand members and especially the core group of 100 political technologists has been actively designing, testing, and observing the uses of their political tools. But what are these tools? How are they used? What is the utility of these tools for the intended users? First, the political technologies created thus far underpin a normative framework most similar to crypto anarchism (Ludlow 2001). By crypto anarchism I refer to the subculture within political anarchism that has developed since the 1970s but became more widely recognizable after John Perry Barlow's "Declaration of the Independence of Cyberspace" in 1996. Barlow, also a former lyricist for the counterculture rock band the Grateful Dead, has since the early 1970s become an early internet enthusiast, partaking in the WELL online community in the mid-1980s, and eventually helping found the Electronic Frontier Foundation in 1990. The Declaration of the Independence of Cyberspace came about shortly after the foundation of the EFF (which was mentioned in previous discussion) in response to the United States Congress's Communications Decency Act of 1996.

The act attempted to regulate online pornography and was eventually overturned by *Reno v. ACLU*, but nonetheless was a critical moment in the shaping of contemporary digital politics and internet regulations within the US. The conflict was eventually settled in the courts, but individuals like Barlow and organizations like the EFF, who were part of the techno-utopian ideology supporting an unregulated internet, came to fruition from these incidents. The opening paragraph of Barlow's declaration, reads: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." As idealistic as such statements may seem to non-enthusiasts, since the early days of the internet these thoughts have helped to influence current norms and expectations about how digital content and the underlying digital infrastructures should be regulated. For instance, Barlow's declaration is now permanently memorialized on the EFF's webservers, and Barlow was recently inducted into the Internet Society's "Internet Hall of Fame"—an award recognizing lifetime achievement in significantly developing and advancing the internet shared with the likes of Vint Cerf and Tim Berners-Lee.

Barlow's libertarian and anti-statist frameworks are not uncommon in Silicon Valley culture. This ideological perspective also traces its roots to the culture and political economy of

information technology development in the Bay Area of the 1970s and 1980s. Another statement that foreshadowed Barlow's standpoints was penned by Timothy May just a few years earlier. May was then a senior scientist and engineer at Intel, and argued (1992):

> A specter is haunting the modern world, the specter of crypto anarchy. […] Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. […] These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation. The technology for this revolution—and it surely will be both a social and economic revolution—has existed in theory for the past decade. […] The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. […] The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration.
>
> ~*The Crypto Anarchist Manifesto*

Since the early expression of these concerns about state-based intrusions in an unregulated internet (which, oddly enough, was made possible by of the backing of the United States to begin with), anti-statist discourse and skepticism of any form of regulation has come to be a defining ideological feature of the LiberationTech community. Crypto anarchism is an appropriate ideological frame for describing the motives and underlying norms shared by the programmers and hackers in this community. Their core motive has been to defend "the infrastructure" against the surveillance of digital communication, to monitor against any type of censorship, and to promote the unregulated freedom of expression of all content, agnostic to cultural, social, or political stances. These technologists try to do this primarily through the development of tools created for the purpose of evading tracking and promoting anonymity by users—that is, *cryptographic technologies*.

Their efforts have also appealed to international journalists and political activists working in repressive regimes as whistle blowers, because in nondemocratic regimes there is rarely a regulatory or legal framework available to protect users. Thus, these new allies of crypto

technology makers are forced to rely on their tools, and consultation with designers is beneficial to both parties for pragmatic and political reasons. Because of this overt bias towards addressing problems technologically (as opposed to legally or in a regulatory fashion), the LiberationTech community has appealed mostly to the interests and involvement of programmers and cryptographers, but recently (as of 2010) exploded in its popularity because of actors like journalists and dissidents turning to them from repressive political systems for aid. These "power users" have enthusiastically joined the community and have collaborated globally on some spectacularly large-scale and complex projects and toolkits. To illustrate this, let us now examine cases drawn from their work that allow us to gauge this particular technologically laden identity and techno-utopian ideology in action.

Building Crowd-Sourced Toolkits

In the summer of 2012, nearly four years after the LiberationTech community had outgrown its early practices of sharing news and updates, the organizers behind it were forced to update some community guidelines to manage the growing diversity of members, interests, and activities. The announcement read:

> You're an amazing bunch of researchers, practitioners, and journalists. You all have a passion for and an interest in how research and design of information and communication technologies (ICTs) can be used to promote democracy, human rights, development, governance, and other social goods. [We are] focused on fostering discussion and exchanging information about how we can best achieve these ends.
>
> *~ List Moderator Update (August 3, 2012)*

In saying so, not only did the moderators explicitly acknowledge the technologically driven pursuit of promoting democracy, rights, and social goods, the objectives were further extended to include: seeking advice on strategic and technical issues and sharing resources on news, jobs, and grant-funding CFPs/RFPs.

In other words, seeking experts' technical feedback on tools and software was openly sanctioned and encouraged as an important community norm. Furthermore, the safety of members of this community and potential threats facing them are also understood as being

technological in nature. Here, the concern centered on the welfare of activist members who are "likely targets of internet attacks, such as viruses and spyware" along with more serious possibilities including automated theft of documents and information from users' systems or activation of cameras and microphones on users' devices to track and document users' activities. The point here is that it was technologies that were imagined to be the basis of democracy's promotion, as well as the source of risks and threats towards individuals and activists. The substantive technical knowledge of expert designers and programmers seemed to support these ambitious ideas, and the growing number of users who brought their experiential knowledge from facing these risks and opportunities seemed to further support these ideas.

Beyond moments of growth and change, we can also look at some of the actual products this community has created through its day-to-day activities, which also exhibit the hallmarks of a techno-utopian ideology. One of the most consistent subjects of heated debate as well as remarkable collaboration and technical problem solving that this community regularly engages in involves its own development of cryptographic software designed to provide safe and anonymous platforms for exchanging messages online. The following are several specific examples of the most important tools (defined as the tools that the community has spent the most amount of time discussing, debating, and testing)—including the best successes and notable failures, and the surrounding challenges and processes that led to their development.

The first example, initially released in May 2011, *Cryptocat*, was an open-source web application which allowed secure encrypted online chatting. Technically, the application worked by encrypting data on the client side using trusted servers with data that was already encrypted, but was made accessible to users as a browser extension and plugin for Google Chrome, Mozilla Firefox, and Apple's Safari. The community's top technologists ranked it as more secure than Google Talk (a popular industry alternative that had a large user base). In 2013, Cryptocat's network was migrated to Bahnhof, a Swedish webhost known for being built inside a Cold War nuclear bunker and also hosting WikiLeaks' data center. The technologists behind Bahnhof were based in Uppsala, Stockholm, Goteborg, and Lund—reflecting some of the Swedish cities that also host the country's most notable research spaces and clusters which LiberationTech members also overlap with.

However, the most notable personality behind Cryptocat was 21-year-old Nadim Kobeissi, a computer security researcher and hacker originally from Beirut, educated at the

Lebanese American University working out of Montreal. Describing himself as a "computer wizard with a strong sense of civil awareness," and then a college student in Canada, Kobeissi would spend his weekends in New York City with the "elders of his tribe" coding at code-a-thons. Some of these collaborative projects were sponsored by journalists like Julia Angwin, who has worked for the *Wall Street Journal*, the *Washington Post*, and the *San Francisco Chronicle*. The LiberationTech community assisted in designing this tool by helping to organize simultaneous coding events in Germany and the United Kingdom, particularly in London.

The cost of running this transnational coding and development operation was a mere $2,000 per year. Affiliated supporters of this platform also shared close links to WikiLeaks, Anonymous, and Telecomix—notable hacktivist organizations that have been targeted by the US government for being active in global political issues. The ideological motivation driving individuals like Kobeissi to create these political technologies were also deeply personal:

> *Money is great, money is amazing. It's not like money is something I don't understand. I understand what it is. [But] I care more about making something nice that people can use, and it's free and it makes a difference.*

Furthermore, the Arab Spring and Occupy protests provided additional context that made tools like Cryptocat seem important and necessary: "I myself only migrated from Lebanon to Canada two years ago. But I also want to draw attention to the fact that privacy technologies are becoming a need even here in Western society. This isn't about the Arab Spring, this is about the decaying state of digital privacy worldwide" (LiberationTech Email: March 3, 2012).

In addition to Cryptocat, the LiberationTech community took part in coding, producing, and security-testing several similar tools. CryptoParty was a grassroots and transnational attempt to introduce the basics of practical cryptography to the general public. This movement was conceived in late August 2012 in a casual Twitter conversation started by an Australian privacy advocate during the passage of the Cybercrime Legislation Amendment Bill 2011 in Australia. The proposed legislation was a threat to online users' autonomy, privacy, and safety in the heart of a respected Western democracy.

In response to this threat, a self-organizing movement immediately went viral via Twitter discussions, and dozens of CryptoParties were organized within hours in cities throughout Australia, the US, the UK, and Germany: "When I woke up in the morning, they were all there," said one of the organizers behind the movement. Soon, many more events were organized in

Chile, the Netherlands, and several Asian countries. The CryptoParty gathering in London was attended by more than 100 coders, several of whom were veterans of the Occupy London protests. The event grew so large that it had to be physically moved to the Google campus in East London's Tech City—the same location that housed the reception and networking functions for the AYM Summit in 2010.

As of October 2012 some 30 CryptoParties had been held globally, with notable supporters including the EFF and AnonyOps (a branch of the hacktivist organization), as well as NSA whistleblower Thomas Drake, WikiLeaks central editor Heather Marsh, and Wired reporter Quinn Norton. Global meet-ups around this movement have since gone viral all over North America, western and northern Europe, and Oceania, as well as in nondemocratic contexts like Tunis, Moscow, and Cairo, with several more requests for meet-ups in Dhaka, Tokyo, Singapore, Bangkok, Delhi, Kuwait, Abu Dhabi, Jeddah, Sao Paulo, and Bogota. Eric Hughes, the author of "A Cypherpunk's Manifesto" and the founding member of Piratbyrån (which in turn founded the Pirate Bay), have also come to regard CryptoParty as one of the most important civic projects in contemporary cryptography today. Some describe it as "a Tupperware party for learning crypto."

So beyond creating tools aimed towards protecting the civil rights of citizens in Western democracies, the LiberationTech community and its affiliated activist networks seem to be nurturing a DIY culture of technology-based interventions. The back-channel discussions shared through the LiberationTech community while these events were being organized, and tools developed, provide additional context for understanding how political technologists not only view the motivations and values of their work, but in important ways the users whom they intend these tools to be of value to. Unlike the state-based stakeholders discussed in Chapter 3, these political technologists and their civil society friends actively enroll users and citizens in crowdsourced work to dissect and innovate solutions for political challenges arising from digital infrastructure.

Designing with Peer-Users

Unlike state-based and private sector stakeholders, these technologists and civil society stakeholders see important ways that users can add value to internet freedom promotion. This community imagines the end user in three competing ways when discussing and designing its political tools: *average users*, *power users*, and *infrastructure-aware users*.

The first image of the end user is a fatalistic one which sees them as unwilling, even too ignorant, to even consider the political risks posed by the infrastructure that is supporting their political activities. Technologists who rely on this image tend to produce tools in the interest of power users instead, and seeing the average user as "dumb."

> The *average user (a very stupid, dumb user but with very strong political commitment in freedom fighting) will always trust the website/operator*. We CANNOT FIX that problem in any technical/cryptographic way. That kind of user will do whatever the 'server operator'/'website' will tell/ask him to do.
>
> *~ LiberationTech email: August 13, 2012*

The second image focuses on servicing power users—an industry term referring to users who have some technical skills. This view tends to observe the context surrounding users, more than simply fixating on the user, but puts the burden of having a deeper technical awareness on the user herself. This allows these technologists to understand that users' agencies are constrained by the infrastructure, but that it is still important to tweak and tinker with parts of the infrastructure that technologists can manipulate in the user's interest.

> *I get the problem here, I do: You most certainly don't want people to think your tool is 100% safe when it's not. But moving to a browser add-on only doesn't solve the main problem: That many, many, *many** people who need encrypted chat do not control/admin[ister] the device on which they want to chat. *[…]* Nevertheless, there are a lot of users who would benefit from *a little bit* of added security.
>
> *~ LiberationTech email: August 6, 2012*

Finally, the third image of the user focuses most explicitly on the infrastructure surrounding the users. It also acknowledges that the tools they are developing must be developed for a broad range of users, not an imagined, ideal power user.

> We *need an ecosystem of tools, not a magic bullet.* The Security Community as such has done much good over the years. However, security professionals who are unwilling to

> acknowledge that *different users have different needs, that online security exists within a larger constellation of risk analysis*, and that usability can and often does trump pure security even when viewed purely through risk analysis and outcomes are doing a grave disservice to both their field and their users."
>
> *~ LiberationTech email: August 6, 2012*

This complex understanding of users is also important because many of the technologists in this collective are also active movement leaders and political activists. Based on their field experiences organizing protests and mobilizing activists, some have significantly sharpened their level of sophistication from "basic users" to sophisticated power users that can now code and help design their own tools with the help of this community:

> I've gone from being a Facebook user to running OTR, PGP and Tor all in under a month. I'm trying to put in the time I have free—mostly between 1am and 4am—towards learning. [...] I'm a sole parent, without access to child support, no childcare and trying to support myself, my son, put myself through postgraduate studies and contribute to social movements. One year ago I didn't own a laptop. Everything I created online in the past 2 years prior was on the only thing I could afford—a phone.
>
> *~ LiberationTech email: October 9, 2012*

This point is worth elaborating on because it is the most pragmatic and best able to reaffirm the purpose of this community's specialized area of work. This approach towards understanding the malleability of infrastructure and the diversity of users supports the position that the community's work should focus on developing a host of tools that will exist in constellations and ecosystems that are changing based on the regulatory conditions effecting digital infrastructure.

Proponents of this final perspective focusing on infrastructure politics recommend incentivizing a "collaborative competition" model between the political technologists to come up with technical solutions. These collaborative competitions work best if they draw on the experiential knowledge of activists and dissidents, because it is these very users who require the tools being designed, and combine it with the technical expertise of coders and cryptographers. To do this, the top political technologists share a peer-review and open-source ethos which helps

impose quality controls and generate social trust in the community. These are essential norms in the innovation process they are working to cultivate. For example, as a counterpoint to the successful developments of Cryptocat and CryptoParty, we can examine the controversial development and deployment of *Haystack*—a controversial tool that the community seems to have concluded was a notable failure because it violated the community's important set of norms and practices.

Haystack was a similar cryptographic tool to Cryptocat and CryptoParty built specifically to support internet activism in the 2009 Iranian election protests. This became a particularly trying moment in the LiberationTech community because not only were there several security gaps and flaws in the software, it also put hundreds of activists and users, particularly in Iran, in grave danger. What seems to have offended this collective most was not that the tool itself was faulty, but rather the closed, secretive, and non-peer-reviewed development and deployment of the technology by its designers. The top technologists expressed deep resentment at the reduced collective legitimacy and increasing distrust such public failures collectively brought on the community and its practices, which hundreds of members had been involved in:

> Good crypto isn't about secret methods—it's open and peer reviewed. And this is not just about suppression—it's about people working in complete safety, gaining the trust of those who are not, and maybe getting those trusting others killed, tortured, imprisoned […]. So long as the code is obfuscated and [the developer] refuses to provide technical details to hackers who know their stuff [I] have to assume that Haystack does not exist. Shut up and ship.
>
> *~ LiberationTech email: August 17, 2010*

While our discussion and analysis thus far has focused on relationships between the tools, users, and designers, it is important to note that these processes also have taken place within the contexts of rapidly changing global political events and the movement of new stakeholders trying to change the infrastructure that these digital tools exist on. What is noticeably missing in the analysis of this community so far is reflection on the legislative or regulatory domains which shape the digital environments they are creating tools to be deployed in. In the past four years, these political technologists have had to address the needs of users in major crises, including Iran

(2009), the Middle East and North Africa (2011), and, most recently, Occupy Wall Street protests in North America and Western Europe (2012). How useful in the end do these technologists believe their tools for political impact to be, given the new ways in which state powers are also attempting to manipulate basic internet infrastructure? Do they have the capacity to shape the structure of the internet, through the technical interventions they are experienced in?

Working with Causal Complexity

These political technologists have a far more nuanced understanding of the causal importance of ICTs and digital media in organizing political change than the reductive ways in which they are framed in as being "digital optimists" or "digital denialists" allow for. Because their technical labor requires frequent interaction with users, these political technologists generally approach the question of impact by accepting "causal complexity" as a daily reality of their work. By this I mean that they rebuff claims suggesting that their tools lack importance by identifying the *mono-causal* logic underlying most dismissive criticisms. Here is one such example from a televised debate that reveals this common criticism, and a nuanced response by a community member:

> When you talk about the Arab spring, you can say that it's evidence of Google and Twitter liberating the world through information. But, the actual facts on the ground are that food prices rose by 30 to 50 percent in the previous year and you basically had people who had become more hungry than scared, who revolted. Then Eric [Google Chairman] goes around and says, "Let them eat iPhones," or maybe not… that's not precisely what he would say.
>
> —*Public debate*

> Sometimes people have to go to extraordinary lengths in order to obtain an "opposing viewpoint" for the purposes of "balance" in a public debate. In such circumstances I often feel that there may be a lesson to be learned. The difference in the debate isn't necessarily between liberation tech and a negative argument. Rather, against a palpable lack of nuance in some of the more effusive views often expressed even on this esteemed list.
>
> —*Technologist's reflection*

This lack of nuance that this technologist is critiquing involves, among other things, being unable to distinguish between "causal triggers" and "means of mobilization." Ignoring the causal conditions that might motivate civic actors to want to protest or revolt, like rising food prices, simmering frustrations, abusive governance, etc., should also contain and factor in the processes of organizing social and political events—processes that are importantly mediated by ICTs and digital media. This community has a far more nuanced understanding of the way complex interactions between the individual agency of users and the information infrastructure and ecology of tools either affords them new pathways or constrains their agency. In fact, some of the most cutting-edge thinking about internet freedom promotion is coming from this collective of political technologists.

Second, they also have a greater *historical* appreciation of the causal processes than they are credited for. Rather than only focusing on the "live moments" of protest activity, these political technologists also point out that ICTs have a long history of slow adoption even in the most repressive regimes. They go on to document several other cases from as far back as the 1970s, where information technologies have been involved in human rights violations, alongside democracy promotion work. One favorite example frequently cited by some of these technologists is IBM's direct involvement[17] in helping the National Socialist German Worker's Party in 1933 with obtaining punch-card technologies used to document and identify Jewish citizens during the Holocaust.

Third, they frequently use *comparative* perspectives to identify different cases across contexts to observe similarities and differences from actual events and experiences, not simply theoretically plausible cases. For example, in the debate focusing on Egypt and Tunisia, list members familiar with the long history of technology-mediated politics reminded others that in Pakistan, activists have frequently noted that blogs, alongside mobile phones, were an important tool for mobilization in recent years, and that Indonesian student activists had made use of SMS in mobilizations more than a decade before the Arab Spring in overthrowing the Suharto regime. In other words, it's the constellation of conditions of state power, security forces, technological development, levels of political repression, sophistication of state censorship, levels of poverty, political culture, and several other issues that need to be understood. Contrary to the public framing of their work as "techno-utopian" or, worse, promoting "slacktivism," the technologists

[17] See *IBM and the Holocaust* by Edwin Black (2001, Crown Books).

designing political tools seem to be engaged in a complex process that draws on users' experiences and appreciates the complex conditions under which their tools can work differently and in unexpected ways. Below are three expressions from the community which exemplify a complex-causal logic towards evaluating the importance of their tools:

1. "Really, to give a simplistic response, three words: Motive. Means. Opportunity. Food price is a motive. The internet tools were a means. The desperation produced was made into an opportunity by those who wanted to wedge activism out of a passive public for a very long time. […] And it would be criminal to look at such things with any less complexity, and reduction."
2. "I'd add strategic capacity, planning, dedication, imagination, hope, agency, etc. of the protagonists of the struggles. This is the 'civic intelligence' that is often lost when social struggles are described without giving due credit to the people who are struggling towards the change. (This often happens when words such as opportunity, technology, resource mobilization, etc. are used to depict activism.) It can suggest false determinism and misleading trivialization."
3. "My ultimate point is that what we are talking about here are tools, and any tool has its pluses and negatives. Just because there are people engaging in inaccurate hype about what a tool can do does not mean that the rest of us should not make them or promote them within responsible limits."

These three different points express a larger one: political technologists have a more nuanced understanding of the process of political change, because they are actively experimenting with affecting this process through their tools and their applications. Their understanding of technology is that it is value-neutral; rather, it is the affordances which can be designed into them, and the surrounding political and structural conditions in which those potentials can be realized, that will determine their utility and normative worth. Through their work in trying to design participatory tools, they are also learning that the regulatory environment and the basic infrastructure that supports their tools can be and is being shaped by more powerful actors than their tools and users are able to counter.

Sharing Best-Practices with Non-Technologists

In the previous two sections I have argued that political technologists actively look towards users to design their tools and practices, and that they have a complex-causal approach for understanding why their tools matter. But what do they do after forming these informed opinions through their research and development of new political technologies? While the above examples show the range of sophisticated thinking political technologists diligently and critically consider in evaluating the efficacy of the tools they design, their work has become even more important, because the community is often sought out by journalists and activists for advice on how best to make safe use of ICTs in repressive contexts. So they are also tasked with designing frameworks to help the affected public in some pressing circumstances.

For example, in January 2011 a Belarusian journalist asked the community about recent crackdowns and the technologies used or monitored by the regime to facilitate its repression. List members quickly chimed in, identifying the possible involvement of Ericsson in Belarus, while others produced evidence that Nokia Siemens Networks technologies were sold to Iran prior to the 2009 Green Revolution:

> We know of people inside Iran who in prison were shown an electronic map, showing exactly where their phones were at the time of certain demonstrations. *In Iran of course the operator is the regime and the regime is the operator!* When I was in Iran two years ago, I met up with three activists (women's rights activists) and none of them brought their cell phones to our meeting place. When I asked them why, they said they have learned—by trial and error—that it is best to turn off their cell phones, take the SIM card out and leave it at home because otherwise they are traced by the security forces.
>
> *~ LiberationTech email: January 17, 2011*

Similarly, in March 2011, while the Arab Spring protests were still ongoing, individuals working on the ground in Yemen, particularly a respected technologist of Yemeni origin, chimed in with ideas to set up communications platforms from within the country to support dissidents and activists. The strategy was complicated, and required balancing security concerns with a limited budget of less than $5,000 in a country that lacked the infrastructure to support basic communication platforms (e.g., power grids and internet cables). The technology-based solutions

proposed to solve the Yemeni activist's challenge included setting up pirate FM transmitters with a range of two kilometers, and alternative ideas of putting more high-powered transmitters 500 miles away in nearby southern Egypt to exploit more accessible communication channels.

When these ideas were put to the community, some journalists from Yemen and a few local political activists were quick to respond. While the proposed ideas were creative in exploiting existing and neighboring infrastructure, past experiments where the strategies had been prototyped indicated that relying on empowering existing social actors would likely achieve the desired outcome. This counterproposition suggested using the same technology to help wire non-activists, such as international journalists, who could aid democratic dissidents in Yemen by sharing their local narratives with the global news community. This particular deliberation, like countless others, sparked a related series of discussions at the behest of several journalists who had joined the conversation. These journalists were also seeking practical solutions for the new challenges they were facing in their international work:

> I'm a Knight Journalism Fellow at Stanford this year, which means I have a year off from reporting to follow projects that interest me and help innovate in journalism in some way. […] I see a lot of work being done on how citizens/activists/bloggers and others can secure information on their end but I haven't seen much done on the other end by the news organizations. Sometimes they offer little more than an email address or Facebook page for submissions. So my project asks: If news organizations are to solicit content from people on the ground (and there are no signs this will stop), what can they do to make it safer for those submitting the information?
>
> *~ Query from Journalist*

> As mentioned before, GlobaLeaks might be what you are looking for. The basic idea if you want to enforce identification is to use the anonymous and encrypted submission channel, and then require identification on top/separately. Also, especially after looking at the AP guidelines: They don't reject all anonymous submissions, so what you actually might want is optional identification (in case the material is, say for AP, not "information" and "reliable" enough). Out of my head, one example would be: Message us on some other platform where you built up reputation or had to be identified

> (depending on the actual definition of identity for the news org!). 1. anonymous submission platform -> after submission, gives you a random string/number 2. to reveal your identity, you can then send that string separately to the newspaper on a site that required identification, e.g. on eBay, Paypal etc 3. only if the number is received, the submission is accepted.
>
> *~ Feedback from Technologist*

These examples show direct interactions between technology experts and technology users at a high level of expertise and sophistication that are far more detailed than ones reflected in public coverage. These feedback channels between civil society activists and political technologists illustrate the important work regularly done to assist a range of nontechnical specialists, including activists, journalists, and policy makers. In sum, these political technologists do more than create experimental prototypes of political tools, apply the lessons from their successes and failures to improve them, and appreciate the complex constellations of factors affording or limiting these tools' intended impact—they also work hard to teach best practices and brainstorm strategies and solutions on a case-by-case basis for desperate activists and journalists from some of the most repressive and dangerous political environments today.

Conclusion: The Limits of Crowdfixing the Political Internet

The LiberationTech collective profiled in this chapter helps to illustrate the ambitious and innovative work done by political technologists who are actively facilitating the creation of tools and advising the best practices surrounding some cutting-edge digital technologies. But despite the creative methods of designing and using ICTs by this community, and their sophisticated understanding of the causal consequences and limitations of technical solutions, they are increasingly finding themselves facing major obstacles. The underlying structure and institutional conditions that shape the internet are increasingly threatening to limit the usability and relevance of their work for two reasons.

First, in the process of developing tools, learning about their users' needs, and trying to better understand the environments in which their tools and users interact, they have increasingly come to notice the strategies by which state powers are subverting the basic infrastructure upon which both users and tools rely. Second, they have also been instrumental in identifying the

collusion, in several instances, of private corporations who have been hired or forced to do the surveillance and censorship work of state powers. Sometimes these infrastructure actors do not necessarily intend to work against their users' interests. But these technologists have also identified and tracked several incidents where private sector corporations, like Facebook, Twitter, Blogger, Flickr, and YouTube, have applied sweeping measures that inevitably endangered and harmed the very users they are deriving market value from.

For example, there have been many incidents where corporations like Facebook have interfered with activism pages using broad stroke measures, with disregard to its impact on the users. During the Tunisian revolution Ben Ali's regime was able to hack into hundreds of Tunisian Facebook users' accounts. When activists changed their names to fake ones to protect their identities, Facebook engineers in Palo Alto were asked to respond algorithmically and shut down all accounts with suspicious activity, particularly those violating Facebook's "real name" policy. What this meant for citizens in Tunisia was that one of their few reliable methods of finding each other and coordinating their activities was turned off, mid-revolution, from the opposite end of the globe. In thinking about the incredible powers corporations and states increasingly have to turn off vast communities and pieces of the internet infrastructure, LiberationTech technologists have taken note that:

> Instead of an unregulated, decentralized Internet, we have centralized platforms serving as public spaces: a quasi-public sphere. [...] But as private companies increasingly take on roles in the public sphere, the rules users must follow become increasingly complex. [...] At the same time, companies set their own standards, which often means navigating tricky terrain [...] Negotiating this terrain often means compromising on one or more of these areas, sometimes at the expense of users.
>
> *~ Research report authored, and shared by LiberationTech members: September 2010*

In addressing problems like these, producing new, safer, and more secure technologies does not seem to be making a difference. For example, the platform Diaspora, which received wide support in the Occupy movements as a replacement for Facebook, has run into several problems, because users attempting to access the platform eventually are forced to rely on internet service

providers and therefore are not able to escape the network structures that are insecure to begin with:

> There is no escape from that in the current network structure. There used to be, when the Internet was really "hands-off" and content-agnostic. But 1995 was a long time ago. Everything at the Application layer and up is subject to control by the layers below, and these layers are out of the hands of application distributors. ISPs can cut off spammers who originate non-locally-damaging traffic to meet the policy objectives or good-neighbor requests of peers. This power exists and can't be overcome.
>
> *~ LiberationTech email: September 25, 2010*

These new challenges arising from the basic layer of the digital infrastructure itself are proving difficult for cryptologists and technologists to design technical solutions for. The political economy of the internet infrastructure backbone does not incentivize ISPs and platform providers to consider their regular users' interests. Many political technologists are at a loss in thinking about how to encourage these infrastructure actors to take users' welfare more seriously. For example, there have been several instances where private sector ICT providers have overtly sold technologies built for the express purpose of surveillance and censorship to repressive regimes, without regard to how those tools are being used by governments to politically censor and target average users. At most these technologists have been devising ways to identify important breaches of users' rights and safety considerations.

As early as November 2011, the American company Narus came under fire from this community for providing Egypt with surveillance technologies, followed quickly by news that Microsoft had aided Tunisia in a similar fashion. But it was in July 2012 that community members further identified FinSpy, produced and sold by a UK company, and widely used in Egypt, Bahrain, Turkmenistan, the UAE, Ethiopia, Indonesia, Qatar, Mongolia, and other Arab Spring countries to target dissidents. The LiberationTech community did organize campaigns to raise awareness about these abuses of infrastructure. In the end, these reports were picked up by journalists and the news media, but public coverage does not seem to be doing enough. The company responsible for selling these tools actually originated in Germany, then moved operations to the UK, and based its servers in Beirut (presumably to serve its Middle Eastern

clients). Although the investigative work of the community revealed important details, the ultimate attempts to address the problem were not as successful:

> Unfortunately, market pressure (via boycotts or similar) rarely work out in these cases, as can be seen by his examples. When human rights and ethical problems present themselves and the market fails to do the right thing (stop the wrong actions from happening) then something other than the market must step in.
>
> *~LiberationTech Email: July 38, 2012*

In addition to the problematic and unregulated nature of private sector companies and their noncompliance with the public needs of their users, governments (both authoritarian and democratic) have made sophisticated advances in their co-optation and control of information infrastructure:

> Tools for circumventing censorship are indeed important for activists. But they do nothing to […] address a growing number of other ways that governments work to prevent activists from using the Internet to access information, get their message out, and organize.
>
> *~LiberationTech Email: November 19, 2010*

It seems, then, that the research labs and hackspaces used to design tools to circumvent censorship and surveillance software are no longer a viable area for these political technologists to invest in exclusively to enact their cyber libertarian values. Can these technologies, or at the very least the lessons learned from designing and using them, be useful for shaping public policy? In the preceding chapter (Chapter 3) I showed the ways in which these technologists' practices and norms have emerged though civil society-sponsored internet freedom agendas, such as the Silicon Valley Standard. But how effectively can these norms be implemented in real policy competitions? With their advanced technical backgrounds, do these political technologists and allies of civil society stakeholders have any more effective leverage over the private sector technology providers to rein them into internet freedom promotion?

In the following chapter (Chapter 5), I address these questions in the context of a real global communication policy negotiation that took place in December 2012. The United Nations-sponsored International Telecommunication Union (ITU) gathering, titled The World Conference on International Telecommunications is the most important field site for this investigation because it represents the first time in the past 25 years that nation states from around the world gathered to negotiate and update a major global communication treaty regime. In this *event analysis* of the WCIT-12 proceedings, I evaluate the consistency (or lack thereof) of the different infrastructure stakeholders to effectively promote internet freedom norms at the international stage. More importantly, the controversies surrounding this event are necessary for understanding the underlying political economic tensions that guide our stakeholders' political ambitions and commitments. If the efforts and lessons drawn together by political technologists discussed in this chapter can meaningfully inform internet freedom norms, we should be able to observe some of these norms and actors at work at the policy level, and if not, imagine the ways in which they could.

Chapter 5 – Seeing Internet Freedom like an Infrastructure Provider

"We know of people inside Iran who in prison were shown an electronic map, showing exactly where their phones were at the time of certain demonstrations. In Iran of course the operator is the regime and the regime is the operator!"

Abbas Milani, Iran Democracy Project (January, 2011)

In this study, I have argued that when identifying where the most important norms surrounding internet freedom work are being cultivated, it has not been state powers or the private sector, but a transnational network of civil society stakeholders that has generated the most democratically oriented ways of thinking about regulating digital infrastructures. In the previous chapter (Chapter 4), I expanded that argument by studying a small but important community of technologists that has been working hand in hand with civil society stakeholders to realize the benefits and risks associated with digitally-enabled organizing, and as a consequence have produced the most innovative practices and approaches to internet freedom promotion. In this way, I argued that civil society stakeholders are importantly positioned in the middle, between the political users who make use of digital media and ICTs in repressive states on the one hand, and the state powers that have controlling interests regarding digital infrastructures on the other hand.

But we still have not been able to effectively unpack the norms or likely behaviors of technology providers and the private sector. In the network analysis of stakeholder ties and exploration of distinct communities of practice that have emerged from these meetings, we found that there are two dominant and opposing camps: state-based approaches and norms exhibited in the London Agenda, versus the civil society produced ones exhibited in the Silicon Valley Standard (Chapter 3). But in both the analysis of the networks and the ethnographic exploration of key communities of practice, such as the political technologists from the LiberationTech community, the private sector stakeholders have not emerged as active participants in internet freedom promotion. In fact, our evidence seems to suggest the opposite: that the private sector that produces and provides various layers of digital infrastructures are easily coopted (at best) by repressive state powers, or are actively colluding in these anti-democratic manipulations of digital media and ICTs (at worst).

Moreover, in the last chapter (Chapter 4) it seemed that even the most innovative norms producers who are providing the cutting-edge thinking surrounding internet freedom and censorship circumvention are no longer able to rely on their cyber libertarian ideology to counter act repressive state powers or the private sector's collusion with them. So how coherent and coordinated are the democratically-oriented values of civil society stakeholders when it comes to effective policy development? Furthermore, to what extent can we expect the most useful norms coming from digital activists and political activists to be translated into real treaties and regulations? Most importantly, how might the private sector technology and infrastructure providers factor into all of this? In this chapter, I address these questions in the context of a real global communication policy negotiation that took place in December 2012: The WCIT-12 gathering in Dubai (UAE).

I justify the selection of this event as a conceptually and historically critical one for studying the formations of the internet freedom proto-regime in question. The United Nations-sponsored ITU gathering, titled The World Conference on International Telecommunications (WCIT-12) is the most important field site for this investigation because it represents the first time in the past twenty-five years that nation states from around the world gathered to negotiate and update a major global communication treaty regime: the International Telecommunication Union (ITU). In this *event analysis* of the WCIT-12 proceedings, I evaluate the consistency (or lack thereof) of the different infrastructure stakeholders to effectively promote internet freedom norms on the international policy-making stage, and focus most closely on the private sector stakeholders who have been using states and state-sponsored arenas as vehicles to have their needs addressed.

The controversies surrounding this event are necessary for understanding the underlying political economic tensions that guide our private sector stakeholders' political ambitions and (lack of) commitments to internet freedom promotion. This chapter (Chapter 5) combines the lessons from the analysis of Chapters 3 and 4 to test the capacities of various infrastructure stakeholders and their norms systems in a real-world scenario by unpacking the WCIT-12 treaty negotiations in Dubai, and magnifying our attention towards the actors that have been least well understood: private sector technology companies. This analysis also provides an opportunity to observe rogue nations that are not part of the internet freedom proto-regime (i.e., authoritarian

regimes), and states who might join if the internet freedom proto-regime is reshaped in a way that addresses their needs and concerns (i.e., developing countries).

5.1 When Regimes Collide: ICANN versus the ITU

The December 2012 WCIT meeting in Dubai was the first time in nearly a quarter century that over 180 countries sent delegations to negotiate a global standards-setting treaty for global telecommunications infrastructure. The ITU is an old and established international regime (unlike the internet freedom proto-regime in question) founded in the late 1800s to set standards for the "new media" and ICTs of that time: the telegraph. This event analysis covers the two-week period of treaty negotiations in Dubai but also examines the controversial six- to nine-month mobilization period preceding the WCIT gathering involving our stakeholders. Comparing this post-Arab Spring policy mobilization period with the outcomes of the Dubai negotiations allows us to test the provisions of this emerging internet freedom regime that Western democracies have been sponsoring. Doing so allows us to examine the norms and standards that the internet freedom proto-regime members seem to be backing in substance, at the level of global policy making efforts. Put more simply, the WCIT negotiation is an important arena for observing the successes and failures of the current state of the internet freedom proto-regime and its associated stakeholders. In the following section, I provide some background reasoning for why this event analysis is likely to tell us the most about private sector stakeholders.

The Windup for WCIT-12

In early 2012, while urgently packing for fieldwork in the Middle East, I was struggling to find a method to rendezvous with the tech-savvy political activists in the Middle East and North Africa. At the time I wanted desperately to begin by studying the digital activists from the Arab Spring, but I had never been to Beirut before; my trip to Tunisia was still five months ahead; and I had lost contact with the few fixers I knew in Cairo. My puzzle at that time was to better understand how political activists in the Arab Spring had acquired some of the highly sophisticated technical skills they needed to detect and/or evade their governments' superb online surveillance and censorship strategies. But this was turning out to be impossibly difficult task, and feeling at a loss, I thought of trying my luck in a roundabout fashion. I posted a query to the LiberationTech

list asking if the community knew of agencies or organizations that were funding "net activism" projects, thinking that maybe I could ask some funded groups and initiatives for some local leads in starting my fieldwork.

As is not out of the norm for the LiberationTech community, several helpful and qualified experts responded. A contact from the Bureau of Democracy, Human Rights, and Labor at the Department of State wrote back by morning, publicizing an SSI, or "solicitation for statements of interest," for internet freedom projects. The US State Department was urgently seeking proposals by the end of May. Another update, from Stockholm, hastily drafted in scattered abbreviations and incomplete sentences (due to a broken arm), came from the Democracy, Human Rights and Gender Equality program of the Swedish International Development and Cooperation Agency (SIDA). This read that SIDA would be publicizing at least three calls for special initiatives on democracy and freedom of expression in 2012. I was desperate to find some tech-savvy activists to interview, but why were these governments so eager to fund them? A technologist from San Francisco, writing from Scandinavia, later shared a bulleted list he had painstakingly put together identifying more than twenty Western governmental agencies and supporting philanthropic organizations. Something new seemed to be going on here, and my initial puzzle seemed to be missing a more obvious and interesting development. It seemed that no one really knew how many projects and SSIs were out there already, yet more urgent offers for funding were being sent from countries, including the US, Sweden, Ireland, and the Netherlands—and all were eager but at a loss to find these political technologists and tech-savvy political activists, just like me. More importantly, the new puzzle, which is now the central focus of this study, became: why and how did these states want to help them?

Four months passed, and I met these three individuals at the Stockholm Internet Forum (SIF). SIF was one of the main gatherings where the members of the network of stakeholders examined in Chapter 3 had a chance to be in the same room, and the lack of stakeholder consensus was quite palatable. For example, during the live moments after his welcoming speech touting Sweden's unwavering support for freedom of expression, Syrian political activists shamed Foreign Minister Carl Bildt with cutting questions: Why was TeliaSonera, one of Scandinavia's largest mobile operators, being implicated in selling sensitive tracking tools to Middle Eastern and Eastern European regimes? How serious were these commitments from

Western governments to a democratic and free internet in the face of scandals like this? After all, the civil society members argued, this was a public company that the Swedish state shared ownership in.

Simultaneously, in the back rooms of the conference, several even more important side events were taking place. A corporate representative of a major Nordic telecom was speaking candidly: "We don't really understand what's happening, these international markets and political situations are very complex. These sensors are basic technologies, we didn't anticipate [authoritarian regimes' repurposing them]," said the legal spokesperson of a German subsidiary. A key member of the LiberationTech community pressed him further: "But why didn't you implement the best practices framework memo we have provided? At least then [after attempting to do so], if you still ran into problems, because these are new complicated challenges, as you say, there could be some credibility. As it stands, how do you expect us to take your [commitments] seriously?" An uncomfortable silence filled the panel of corporate technology representatives—meanwhile, a mixed group of twenty including LiberationTech policy experts, a group of Iranian exiles, and an international collective of citizen journalists curious about internet politics continued to scrutinize them.

Although SIF was sponsored by the Swedish Foreign Ministry, I noted a significant presence of technology policy and civil society leaders from San Francisco and Washington, DC. The main moderators guiding the discussions, policy experts who could speak to the diverse interests of the international gathering, were also DC-based, including Access, EFF, and CDT, to name a few. In the words of one attendee, Access "stole the show." I have mentioned Access in previous discussion—a Bay Area civil society startup that has rapidly risen to prominence after Iran's Green Revolution (my earliest interaction with them was in London at the AYM gathering in 2010). Members from Access were skillfully driving the conversation between the tough experiences of political activists from places like Syria and the esoteric world of telecommunications regulations and corporate policy norms. The relationships between civil society and internet governance work are not new, for example the Internet Governance Forum (IGF) does exactly that kind of bridging work through global summits like the World Summit on the Information Society (WSIS). But Access' entrance to the world of internet governance lobbying was new—a rare space and community that highlights the visceral impact of esoteric telecommunications laws on the daily livelihood of activists and citizens around the world.

Back to Stockholm, as early as this spring meeting where I was observing Access at work, it seemed that the policy experts and their discussions were regularly returning to some specific upcoming regulatory discussion meetings that the LiberationTech attendees were increasingly discussing starting from early 2012. Additionally, the stakeholders who would logically be concerned about this meeting would have been technology companies and in particular telecommunications corporation. Why were civil society stakeholders so agitated? These meetings where civil society actors were raising awareness included several internet governance gatherings in North America and Europe, a major meeting of the IGF in Azerbaijan, and one in particular that civil society members generally seemed to despise: the ITU's WCIT-12 gathering in Dubai. As I was following the aftermath of the SIF meeting through the summer of 2012, in July Access established an official full-time position for a policy expert to focus singularly on the upcoming WCIT gathering—six months ahead of it. *Why was it that WCIT in particular so disliked by civil society?* What did Access see in it as so important that it required a full-time paid staff member to monitor and organize for? The language and tone of the job description also clearly communicated an ominous opposition to it, framing the position as that of a watchdog. Another foreshadowing that seemed not inconsequential came in through the LiberationTech email list soon thereafter when a thread on the email list went viral—the subject: "UN Body Wants Control over Internet Governance."

So what is this ITU? Why were civil society, state, and private sector stakeholders comprising the internet freedom proto-regime equally concerned about this meeting, above others? What (as I will show next) do they mean by preferring a "multi-stakeholder" model over the ITU's? And what do they mean by claiming that the ITU was attempting to "hijack" the internet? The ITU matters to civil society because it is one of the few important international telecommunications regulation gatherings that all major parties, including governments and corporations, are invited to—except for civil society. Only after online petitions and mobilizations against it was the ITU leadership willing to open up. But "opening up" meant allowing civil society organizations to post some op-eds on its website. From the perspective of civil society stakeholders, the ITU is one of the oldest existing telecommunications regimes (as old as the telegraph) but one that, despite lacking in transparency, has set standards for telecommunications networks for well over a century.

Civil society organizations feel the ITU is so exclusive because nonmembers of state delegations were effectively unwelcome at the Dubai event. There is little question that civil society is not welcome at ITU discussions, and especially was not welcome at WCIT. Basic documents listing meeting times and discussion events were only available on password-protected pages of ITU in Dubai. Attendance costs to participate were prohibitive, ranging in the thousands of dollars per person. Civil society members who choose to attend nonetheless—which added up to mere thirty or so individuals (compared to the 2,000-plus delegation members representing world states and multinational corporations)—were easy to spot: all were outcasts at a coffee shop in the lobby of the Dubai World Trade Center—yards from the entrance, but denied any formal involvement or even the ability to observe the discussions about the world's largest telecommunications policy making event.

In sum, WCIT and the ITU organizers limited attendance to official members of country delegations—that is, wealthy multinational technology corporations that most civil society organizations could not compete with, given their meager resources. The ITU regime, in short, represented the antithesis of the purported future internet freedom proto-regime: an exclusive arena of world states being represented by an army of private sector companies and their lobbyists. How could internet freedom promoters, especially digital activists and civil society stakeholders compete? What more can the WCIT moment tell us about what promoting internet freedom means for different stakeholders, particularly multinational private technology stakeholders?

Derailing the Deliberations before Dubai

The six- to nine-month period leading up to Dubai was the outcome of several connected international mobilizations worthy of observation and analysis. First, although WCIT deals primarily with states, the various stakeholders invested in the activities of the ITU include wealthy multinational technology companies, including telecommunications infrastructure and content providers. The state actors and their delegations represent the world (all countries), including the contentious environment where several authoritarian regimes (Russia, China, Iran, and Saudi Arabia) appeared to be embroiled in a bitter dispute with a US-led coalition, including most of Western Europe. Lastly, another collective of third-party states were also involved, but

were dissatisfied with both polarized camps—these states included mostly emerging democracies and developing countries like India and Brazil.

In addition to the multipolar tensions between the private sector, civil society, and international powers, current events and ongoing conflicts, the then vivid backdrop of the Arab Spring and the ongoing atrocities in Syria, further added visceral context and tropes which shaped the discussions, understandings, and mobilizations leading up to Dubai. As early as June 2012, the *Wall Street Journal* began featuring coverage of the planned WCIT meeting framed in rather dubious terms. "The U.N.'s Internet Power Grab" was the headline of an article by Gordon Crovitz, an American media executive and former publisher of the *WSJ* and executive vice president of Dow Jones, in his weekly column "Information Age." Crovitz's framing signaled that countries like Russia, China, and Iran were actively working to "hijack" the internet, with the US at fault for its complacency in allowing the ITU to do so. However, looking more closely at the logic of this argument, the primary concern of WCIT dissenters like Crovitz was not the potential authoritarian takeover of the internet. Rather, the core problem seemed to be that ITU member states might "want to use international agreements to regulate the Internet by crowding out bottom-up institutions, imposing *charges* for international communication, and controlling the content that consumers can access online." (Crovitz 2012) This suggests that market-based disagreements over pricing protocols, more than the discourse of human rights abuses and civil rights violations, were the substantive contentions with regards to WCIT.

Dissenters of the WCIT meeting did not cite the clearly troubling proposals like those of Russia and Arab countries wanting to inspect private communications such as email, or Iran proposing rules to measure internet traffic along national borders. Instead, the ITU's state-led and private sector-backed meetings focused concerns about internet freedom to mean the plight of Google, Facebook, and Apple as the primary victims. The concern from the vantage point of these new "victims" was that the UN community (i.e., states) would gain power over allocating internet addresses and replace the California-based, US-dominated, and US Department of Commerce–contracted nonprofit ICANN's regulatory dominance on the global internet. This further suggests that the primary concerns about internet freedom at WCIT were not so much the human rights or civil liberties issues of users and citizens, but rather the possibility that the existing ITU regime was broadening its scope over digital infrastructure, competing with the existing ICANN multi-stakeholder regime. Despite the compelling backdrop of powerful stories,

images, and lessons regarding how authoritarian governments over the past several months had interfered with digital infrastructure to politically repress their citizens in the Arab Spring, Crovitz's primary concerns center ostensibly on the welfare of content providers like Google and Facebook.

This conflation of concerns about internet freedom was widely apparent in all of the mobilizing against WCIT. One month before Crovitz's call for action, Vinton Cerf, who with Bob Kahn is known as one of the "fathers of the internet" (together, they co-invented the internet protocol and transmission control protocol in the 1970s), also penned a similar op-ed in the *New York Times*, but somewhat more modestly warned of "a new front in the battle for the Internet." The concerns voiced by Cerf, now working as Google's "Chief Internet Evangelist," were very similar to Crovitz's, citing the fact that Google platforms, including Search, YouTube, Blogger, Gmail, and Maps have been blocked temporarily or permanently in over thirty of the 150 countries Google operates in. Like Crovitz, Cerf expressed concerns that the UN agency would expand the scope of its WCIT treaty to include internet regulation; that these decisions would be made by governments and would not allow for civil society participation; that countries like China and Russia were actively working to ban anonymity; and that their primary method for doing so would be by taking the regulatory power out of the hands of privately run multi-stakeholder organizations like ICANN, and centralizing them under the UN. But again, in rather explicit ways the commercial interests involved in the WCIT deliberations outweighed any substantive recognition of human rights abuses and civil liberties violations online. Human rights and users' civil liberties were invoked, but in name only.

Like Crovitz, Cerf also argued that the main threat involved the ITU potentially rendering the engineers and companies that have built the commercial internet (accounting for 13 percent of the United States' global economic) voiceless in its governance and regulation. Cerf was more open that Crovitz, however, to opposing perspectives, and noted briefly that several developing countries were unsatisfied with the existing framework because it favored the economic interests of almost entirely US-based large internet companies. Nonetheless, the private sector's intellectual sages had spoken, and a mass mobilization against WCIT was initiated. Following the May and June op-eds and ensuing debates sparked by these two prominent opinion leaders of the high tech sector, business experts and civil society leaders sounded the alarm in the US to begin mobilizing against the WCIT treaty gathering. This opposition began to organize around a

shared mobilizing trope embodying the story of David and Goliath: an age-old telecommunications regime, the ITU, sponsored by the hegemonic United Nations trying to hijack and control the global internet from an egalitarian multi-stakeholder community of private sector stakeholders.

Larry Downes, a prominent consultant and IT business strategist, writing for Forbes in early August, began the charge, asking: "Why is the UN Trying to Take over the Internet?" This refrain overlapped with previous claims, but praised both Republicans and Democrats in Congress, the White House, and the FCC, for finally getting ready to act. In August, Republicans at their national convention in Tampa for Mitt Romney, backed by technology trade associations and advocacy groups, adopted some of the strongest language regarding internet freedom to date: "We will resist any effort to shift control away from the *successful multi-stakeholder approach of Internet governance* and toward governance by international or other intergovernmental organizations […]. The only way to safeguard or improve these systems is through the private sector." By September, the Democratic Party also adopted new language in its presidential campaign for Barack Obama: "The Democratic Party is now firmly and forcefully on record in support of an open Internet as the source of new jobs, innovations, and ideas." Although US Republicans staunchly opposed net-neutrality rules back home in the case of the Stop Online Piracy Act and PROTECT IP Act (SOPA and PIPA), the overt support of both parties suggested an overwhelming consensus that US lawmakers were not interested in US-based private sector companies losing influence in global internet regulation abroad.

So in September 2012, a Senate panel approved an Internet Freedom Resolution, and in December, less than a week before the WCIT gathering, the US House of Representatives followed suit with a unanimous 397-0 vote preserving and advancing the multi-stakeholder model. The United States government and its entire high-tech industry were wholly and firmly committed against the ITU's WCIT treaty making, long before the negotiations had even started. Months later, in Dubai, two delegation attendees in Dubai from Brazil and India would comment: "How can this event, which requires unanimous approval, pass with the armies of US stakeholders here to oppose the meeting?" This was a question grounded in facts—the US delegation was the largest (excluding the UAE's host delegation), exceeding the median delegation size (n = 5) for member states by well over one hundred delegates (see Figure 7).

The US delegation made it very clear that it would not back any increase in "control of internet governance or content"—but what was meant by control was open to interpretation, although specific frames were being populated by the private sector and the US Department of State. Again, authoritarian countries including Russia, Iran, and China were framed as the primary belligerents, and the UN body was framed as a "slow-moving, expensive, secretive, jealous" entity. Here, in these moments where Western states wanted to oppose authoritarian states, the visceral images of brave democratic internet users working from within repressive countries were invoked in passing references to support claims of an "authoritarian takeover of the internet." However, it was also clear that despite invoking the fates of these citizens, the main victims in the minds of the state delegations and the private sector representatives comprising them were the likes of Google, YouTube, Facebook, and Skype—or, in other words, private sector web corporations that liked the internet and its current regulatory approach just as it was.

These reflections suggest that when only corporations speak for internet freedom norms at the policy making level, they mean internet freedom to be defined by its regulatory approach—namely which governance organizations should have ultimate authority over global digital infrastructure. But this has not stopped them from using tropes of democratization and the fates of brave dissidents, even in the most surrealist fashion:

> Ladies and Gentlemen, I'd like to conclude by turning to us, citizens of the world wide web of democracies, connected by optical cables, computers, but far more importantly, connected by values and the belief in the sanctity of the individual human spirit and freedom. […] In cyberspace, these countries are faced with the import of potentially disruptive liberal aspects of open societies. The means of expression, transparency and accountability empowered by a Google search, a YouTube video, or a tweet is direct threats to a restrictive political system; the World Wide Web turns them into domestic threats to the regime. So, these regimes must rely on filtering and blocking, using sophisticated monitoring and filtering software while co-opting internet companies to identify and round up dissidents tweeting or posting on Facebook. When these methods fail, they cut off the internet wholesale, as the Mubarak regime did in Egypt. We must choose between two paths—either we can change the nature of the internet by acceding to a Westphalian regulatory structure of internet governance, or we can change the world.

> The enemies of open society prefer the former, the imposition of a regulatory system. Authoritarian regimes fear the West is attempting to orchestrate an Arab Spring or an Orange Revolution. This is why illiberal states want to develop new regulations for the internet, to put another brick in the wall (or is it another wall in the BRICs?), expanding their own Westphalian space to our common World Wide Web. This would be sovereignty on their terms, disabling the freedom and sovereignty of our citizens. This *December, in Dubai, the International Telecoms Union will hold its first world conference since 1988. The outcome of this conference, and related processes, will help determine the topography of the web for the next generation*. While this conference may fall into the domain of ministries of commerce and communications, make no mistake, there will be major ramifications with calls to limit free expression as we know it on the web today. The authoritarians will again present proposals that would undermine the current multi-stakeholder model of the internet, replacing it with a scheme that would allow them to expand their control of their own populations and economies, extending their control to undermine the freedom and openness we value today. They will claim that sovereignty in cyberspace is necessary to rein in cyber-crime and cyber-terrorism. The ITU will come up with new regulations. The Freedom Online coalition, to which my country, as the #1 in Freedom House' rating of freedom on the internet, belongs, opposes all attempts to limit free expression in any, but especially in digital form. We and other defenders of internet freedom will be at the ITU meeting but the authoritarians will be there in force too. They want to encroach on the territory of the free. They want to make their values truly universal. They will want to force their authoritarianism on us. Let's not let them do it.
>
> *~ The President of Estonia, speaking at Freedom House in Washington DC*

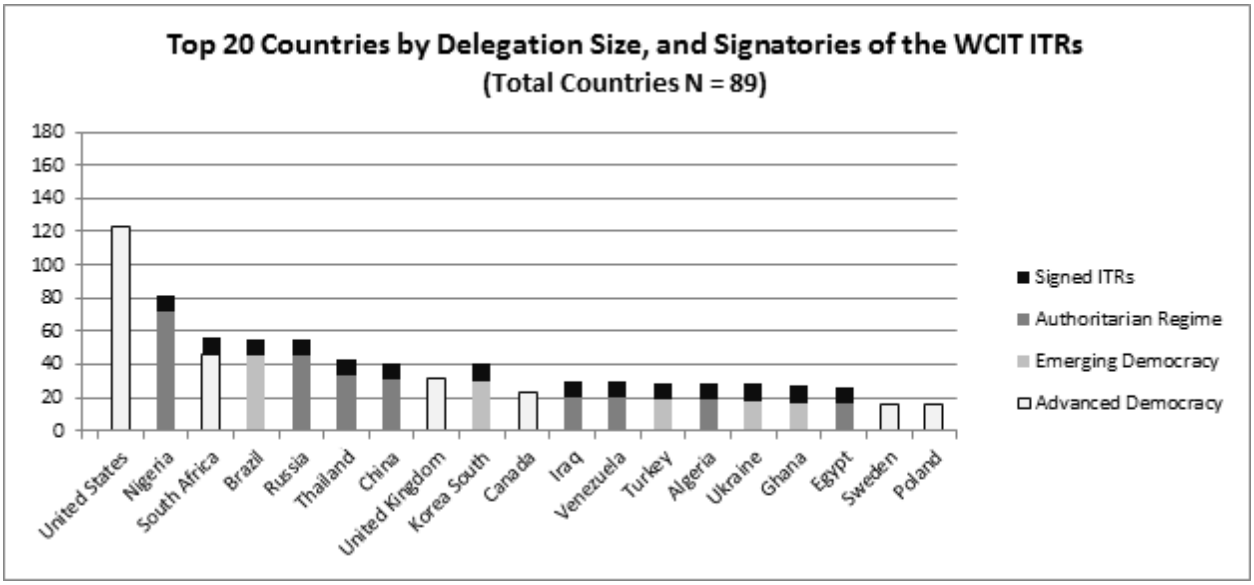
Several points in this speech are worthy of expanding on. First, President Toomas Hendrik Ilves of Estonia frames a binary opposition: one side consists of the FOC, including advanced industrialized Western democracies (Australia, Canada, Finland, France, the Netherlands, Ireland, the UK, the US, and Sweden). The other is represented by illiberal states from the Arab, post-Soviet, and emerging markets. Second, the former enjoys a utopian world wide web of open democracies (i.e., made possible by the current regulatory system), while the latter faces

existential political crises as a direct outcome of Google searches, YouTube videos, and tweets—a slate of American content-based private corporations are the force behind democratizing them. Third, this pole of a technological democratic utopia is contrasted with the dystopia of authoritarian regimes who want to change the internet. President Ilves concludes his depiction of this binary opposition by framing the WCIT meeting in Dubai as the key moment when "*they* will want to force their authoritarianism on us" and so we must "not let them do it."

The main conclusions to be drawn from understanding the wind-up period to the meeting in Dubai are the following. First, the WCIT gathering in Dubai represented an ideal case (conceptually speaking) to observe Western states and digital infrastructures providers at work in promoting internet freedom. Second, when they did so, the defining features and norms surrounding the promotion of internet freedom dealt narrowly with protecting the market hegemony of the Silicon Valley-based ICANN, over any centralizing regulatory approach that could empower states to regulate digital infrastructures. Third, when speaking of the different camps of states struggling with each other, there are at least three communities of interacting stakeholders (see Figure 7): Western democracies (focusing on protecting the market advantage of their high-tech sector companies, and therefore are against the ITU); authoritarian regimes (who want to centralize their power over digital infrastructure, and therefore use ITU as a vehicle); and developing countries (who do not aggressively want to centralize state control over the internet, but also do not care for the Western democracies' private sector hegemony over the global internet).

Put more simply, the opposition and eventual failure of the ITU's WCIT negotiations to generate consensus centered around two dueling forces: 1) private sector technology companies promoting internet freedom to mean securing their "multi-stakeholder" (read: non-state) dominance over digital infrastructures; and 2) authoritarian and developing states' support for the ITU as hoped to dislodge their economic and standards dependency on the Western-based high tech industry. Although authoritarian regimes were a more credible threat to end users' and private citizens' interests, nowhere was the opposition to the ITU substantively or meaningfully focused on the plight of digital activists and civil society stakeholders. In the remaining discussion of this chapter, I expand on the substance and meaning of what the collective resistance towards the ITU and WCIT actually means and what it helps us understand about how private sector stakeholders want to (i.e., not) promote internet freedom.

Figure 7: Top Country Delegations Attending WCIT



Note: Figure prepared by author based on data collected from the WCIT Leaks documents archive. Chart does not include the UAE (n = 160), which had the largest delegation reflected by its position as the host nation organizing the WCIT-12 negotiations.

5.2 The Private Sector: Coopting Internet Freedom with "Multi-Stakeholderism"

The US delegation and other Western democracies overwhelmingly opposed the ITU's treaty negotiations. Moreover, they also seemed to reject the ITU as a legitimate policy regime, and instead preferred a multi-stakeholder model supporting competing internet regimes (e.g., ICANN), arguing vehemently that it was inherently a more democratic process. There was, of course, the issue of the ITU not allowing civil society stakeholders into the discussions. However, this multi-stakeholder model also seems to overwhelmingly privilege the voices of the private sector, and furthermore has little of substance or interest to digital activists and civil society stakeholders. In other words, the internet infrastructure the world citizenry uses is mostly maintained by a set of standards-setting bodies that are mostly in the United States—more specifically, in California. That they would not like to see this position usurped by an expanding ITU regime is therefore unsurprising. So what are the other kinds of political contentions that can help us more meaningfully interpret how technology providers want to define the internet freedom proto-regime (if at all)?

While the technical and regulatory details debated in Dubai primarily focused on the economics and cost structures of internet regulations, several fault lines also emerged between private sector content-based companies (like Google and Facebook) on the one hand and the infrastructure providers and telecommunications corporations on the other. This is an important point: the private sector, like any set of stakeholders, is not a monolith. The deeper tensions surrounding internet regulation here are not about democracies opposing an authoritarian takeover of the internet—the tension is also between *content-provider companies* and the *infrastructure-layer providers* that support data transmissions, both of which comprise private sector stakeholders.

To break it down very simply, an infrastructure provider like Comcast is incentivized to demand more fees from content provider companies like Google who make use of the infrastructure-layer to run their services. Currently, companies like Google are reaping vast profits by running vast amounts of data traffic without sharing any of these profits with companies like Comcast who are providing highway infrastructure to transport those data. This is because the US has maintained a standard of "net neutrality"—the principle that all data are treated equally when sent over the internet backbone. For example, data for Netflix must travel at the same speeds and costs of data for Facebook. Although this may not seem to have any relation

to internet freedom concerns, examples from the standpoint of Arab Spring protesters show that they can: under the ITU regime, state powers were also negotiating fundamental redefinitions that could give states more power in deciding how to structure their IT systems by colluding with infrastructure-layer providers and violating net neutrality principles. In this battle between competing regimes, civil society stakeholders, then, could be incentivized to protect net neutrality as a core component of promoting internet freedom. More importantly, bringing the focus back to private sector stakeholders, we should at least recognize a core battle and tension between the Googles and the Comcasts of the private technology provider stakeholders.

Based on this understanding, my main argument moving forward in this discussion is twofold: first, constrained civil society stakeholders made a pragmatic decision to support the lesser of two less-than-ideal communication regimes—the ITU versus the multi-stakeholder model—both of which were dominated by competing types of technology stakeholders. This pragmatic decision by civil society meant joining forces with the private sector against the UN's ITU regime (which favored infrastructure providers), in favor of the multi-stakeholder model that also privileged the private sector (which favored content providers). Their motivation to do so was to keep internet governance clearly outside the domain of state-based stakeholders. Second, without much resistance from civil society stakeholders, *the private sector stakeholders were successful redefining internet freedom to mean promoting "multi-stakeholderism" and in particular a norm of net neutrality that served private sector economic interests at the expense of civic rights and democratic norms*.

Civil Society's Pragmatic Compromise

In the arena cultivated by state powers and the private sector, civil society stakeholders have performed pragmatically in the narrow choices available to promote internet freedom at the policy making level. Of the approximately 190 countries that were part of the WCIT-12 gathering in Dubai, approximately 185 also had over 1,500 registered civil society organizations behind the scenes opposing the WCIT negotiations. These civil society organizations were based in advanced democracies, emerging democracies, fragile states, and authoritarian regimes. By December 3, 2012—the date WCIT-12 negotiations began—these global civil society organizations had signed petitions registering their disfavor with the ITU's proposal to extend regulatory domain to internet infrastructure. Despite the lack of substantive attention to their

concerns being offered by the private sector (which also opposed WCIT), civil society organizations shared a concern that the ITU's potential regulatory impact on internet openness and innovation would not work in their favor, or keep internet costs low, or secure human rights online. For these reasons, civil society and the private sector became uneasy bedfellows with high-tech private sector stakeholders in opposing WCIT.

The most popular and comprehensive online petition that helped unite civil society's opposition was organized by OpenMedia.ca—a Canadian nonprofit advocacy organization based in Vancouver, established in 2008. This was not the first petition organized by OpenMedia that has had widespread success in online mobilization regarding digital infrastructures politics. In February 2011, OpenMedia was also the organizational machine behind "Stop the Meter," a petition signed by nearly half a million Canadian citizens to block new internet billing methods that threatened net neutrality. Like some private sector data-service providers that supported net neutrality, users and civil society were in favor of net neutrality for similar reasons. The 2012 campaign to oppose the ITU, titled "Protect Global Internet Freedom," was supported by major US-based civil society organizations including Access and the Center for Democracy and Technology (CDT). This petition was a landmark success, and included over 1,500 civil society organizations representing 185 countries worldwide. The largest sectors of civil society support came from advanced democracies (Canada, n=350, United States, n=200, United Kingdom, n=50, and Australia, n=50) and emerging democracies (Brazil, n=50, India, n=50, and Indonesia, n=50). But civil society organizations from repressive systems and authoritarian regimes also supported resisting the ITU (e.g., Russia, n=50) (see Figure 8). All of the civil society organizations signing this petition from around the world still favored resisting the WCIT arena, citing a wide range of concerns, including the promotion of net neutrality in international data traffic, but also resisting the involvement of states in defining internet regulations.

Mobilizing this broad base of support from global civil society organizations across democracies and authoritarian regimes required the support of powerful institutions and organizing efforts, like the Harvard Berkman Center-based Global Voices Online (GVO). The GVO community helped translate the petition and the problematic policy documents to share with global civil society organizations. As an important side-note, both Berkman and GVO are important communities that share strong ties with the community of political technologists

profiled in the previous chapter. So we should at least expect some familiarity with norms connected to internet freedom that also represent civil society stakeholders.

In August 2012, the CDT released a report titled "The Importance of Voluntary Technical Standards for the Internet and its Users," identifying the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Society, and the Internet Architecture Board (IAB) as some of the influential groups that have traditionally designed and regulated the internet thus far. The most substantive outcome of these reports was the conclusion that these standards ought to be voluntary to foster competition, open participation, and adoption:

> One of the main reasons why the ITU's renegotiation of its International Telecommunication Regulations (ITRs) has attracted so much attention is because the ITRs are a binding legal instrument on member states: when the ITU adopts changes to the ITRs, governments will be expected to enact corresponding changes in their national laws.
>
> *~ Statement by the Center for Democracy and Technology (June 20, 2013)*

The CDT and other civil society organizations shared a concern that the technological expertise of private sector corporations would be hierarchically subjugated to the interests of governmental representatives, particularly member states like the Arab states, Russia, and China. This could allow civil liberties and human rights issues like personal identity information to be made identifiable if states had more power over digital infrastructure. For this reason, influential civil society organizations like Access, the Committee to Protect Journalists, Human Rights Watch, Internet Democracy Project (India), Nawaat (Tunisia), Panoptykon (Poland), Reporters Without Borders, Thai Netizen Network, the Electronic Frontier Foundation, Global Voices, and OpenMedia were all encouraged to adopt policy frames and stances in opposition to WCIT.

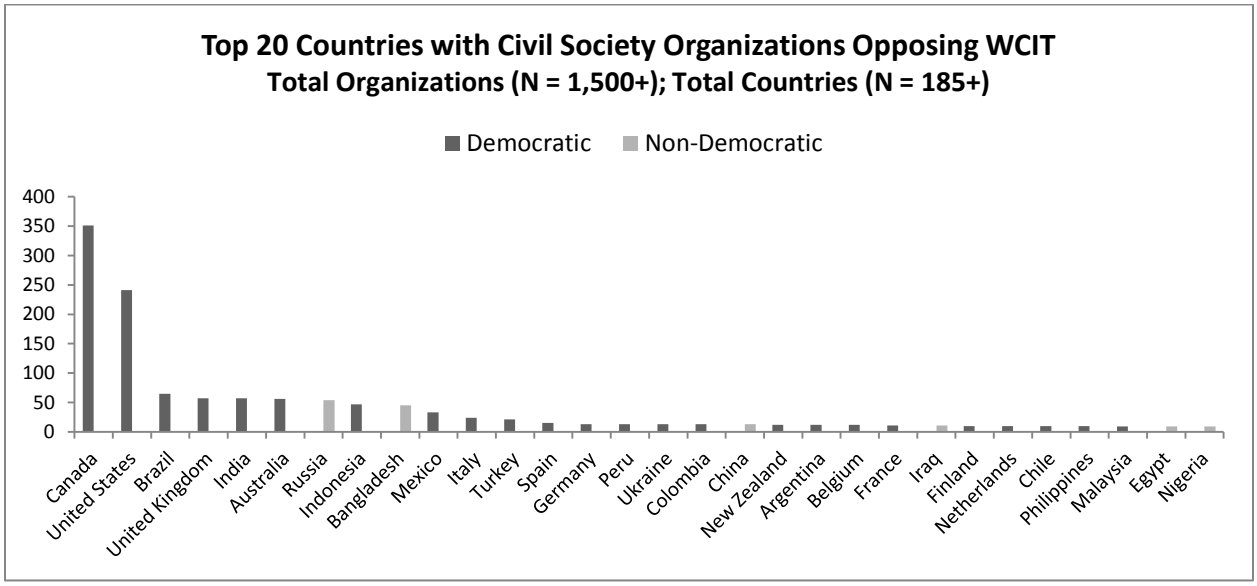
Civil society organizations also did not want any states, developing or authoritarian, to lobby and adopt standards and definitions that legitimized states' rights over digital infrastructures. Sally Wentworth, the Internet Society's senior public policy expert, said, "[Many developing countries] incorporate [treaties] whole cloth into national law […]. If you do business in countries that do that […] this will affect the legal and regulatory environment you work in."

Another respected network architect also noted, "At the end of the day, if they [the ITU] do enough things, they have taken over the Internet." These statements reflect key components of the ongoing debate that has long been taking place in North American and Western European countries in the form of the net neutrality battle since the early 2000s. But in the early 2010s, and especially at WCIT-12, these issues formally converged to extend into the borders of developing nations and nondemocratic regimes *because* of the proposed changing regulatory regime in question: from the multi-stakeholder dominance of the ICANN (controlled by private enterprises) to the top-down and exclusive framework of WCIT (dominated by states and telecoms) that significantly limited the power of private enterprise and civil society groups).

While the turnout of online support was clearly based in the experiences of civil society voices from advanced democracies, what is more telling is the highly sophisticated technological and policy-based background of these organizations. This issue suggests that civil society stakeholders based in advanced democracies are interested in supporting the human rights efforts abroad but want to do so by protecting digital infrastructures as a top priority. These elite civil society organizations wanted to take these negotiations seriously in order to oppose any increase in the UN or ITU's power in regulating the internet. This goal was based in the consideration that states should not be the purveyor of digital infrastructures—paralleling similar divisions between the separation between state agencies and news/broadcast media institutions (an older form of a public information system/infrastructure). The analogy here is that these civil society organizations wanted to treat digital infrastructures as *public information infrastructure*, and therefore keep states' hands off it at all costs, even if it meant giving private companies that power. Rebecca MacKinnon, senior fellow of the New America Foundation and respected member of the LiberationTech collective, reporting from the IGF in Baku, Azerbaijan, which took place in November 2012, a few weeks prior to WCIT, framed it this way:

> News organizations, press associations, and media assistance organizations around the world have also been slow to recognize how internet governance debates will ultimately affect their own work and sustainability. If they do not seek to influence the process and debates that will determine who shapes the future of the internet, they run into the serious risk that internet standards and regulations will evolve in a manner that will undermine journalistic freedom, public media, and non-commercial news outlets.
>
> *~ Rebecca MacKinnon, New America Foundation (November 7, 2012)*

Figure 8: Top Countries with Civil Society Organizations Opposing WCIT



Note: Figure prepared by author based on data collected from the WCIT Leaks documents archive.

Lobbying Western States to Support Net Neutrality

In the previous section, I have pointed out that most of the important decisions about internet standards in the multi-stakeholder model favored by private industry are effectively made by a small group of mostly American, and specifically California-based, decision makers. In effect, there is a global form of dependency that some states not in the center of the global economic system would seek to lessen, particularly developing economies. In this context, because the US has an undeniable advantage in—and monopoly on—most digital infrastructure decisions, even some advanced Western democracies in Europe generally lack an equally powerful footing in setting protocols and technical standards about the internet. For this reason, despite the overwhelming opposition to WCIT-12 by the US delegation, the position of EU democracies was not so unanimous during the period leading up to Dubai (but was eventually reigned in). To understand why and how this was done, we need to take a slightly different historical glance.

Since the commercial internet was privatized by the National Science Foundation and handed over to multi-stakeholder governance in the mid-1990s, the US has effectively maintained a global position as the global internet infrastructure's material and regulatory home (i.e., all the servers and undersea cables lead home to the US). One chairman of a UK-based cloud computing company voiced vocal opposition to the presumed standards dictated by US interests thusly: "The UK should have far greater control, either with or without the United Nations." But by the end of 2012, it was clear that the pack of advanced Western democracies had fallen in line. The UK-based International Cyber Security Protection Alliance (ICSPA) accepted the multi-stakeholder approach, arguing: "It is important for the UK, US and their allies to invest in supporting cyber development and defense to instill the ideal of a free and fair internet." What happened? How did this dispute within the FOC get resolved?

The effort to organize a coalition to oppose the ITU was taking place on several simultaneous fronts, and civil society's pragmatic compromise with the private sector was only one of those fronts that the private sector stakeholders won. The other major front for the battle against the ITU regime centered on convincing several advanced Western democracies to support the multi-stakeholder model over one centralized under UN bodies dominated by states. In October 2012, the Australian IGF's minister in charge of assisting "industry and innovation" came out vocally in support of the ICANN model, and several supporting civil society

organizations put forth additional reports and analyses forecasting the economic benefits of doing so:

> Plainly, the system ain't broke, so we don't need new sorts of regulation to fix it. […] Lest you think, by the way, that [they] have drunk the libertarian Kool-Aid, they do make a case for giving the government a role in maintaining the spectacular rate of Internet innovation. […] Investment in basic research needs to be reinstated to return to a level of growth that will meet the economic and social development goals OECD countries expect of the internet economy.
>
> *~ Quoted in US News (October 29, 2012)*

Comparatively, then, despite the dominance of the US in regulating the internet, the argument needed to be made that EU democracies could catch up, with specific strategies and policy arguments showcasing how they could do this. This task first and foremost required rejecting one of the strongest opponents from inside the EU community itself: the European Telecommunications Network Operators' Association (ETNO).

Established in 1992, ETNO is the main organization representing Europe's biggest telecommunications firms. Like the net neutrality debate that has taken place in the US since the early 2000s, the conflict of interests in OECD countries mainly revolved around ETNO's opposition to content-driven enterprises from the US (like Skype, Google, YouTube, and Facebook) that were using up ETNO's internet infrastructure without paying them dividends for doing so. ETNO telecommunications providers wanted greater leverage in setting tiered pricing for their traffic, since it is on their cables that Google and Facebook's traffic runs:

> [ETNO] is demanding that governments outlaw the introduction of 'network neutrality' rules, which are already in force in countries such as the Netherlands and Chile. These rules require operators to grant equal priority to all internet traffic, and prevent them from charging higher prices for 'fast lanes' and other premium services.[…] [O]perators cannot continue to invest in broadband infrastructure without a fairer share of the revenues it generates.
>
> *~ Quoted in The Economist (December 1, 2012)*

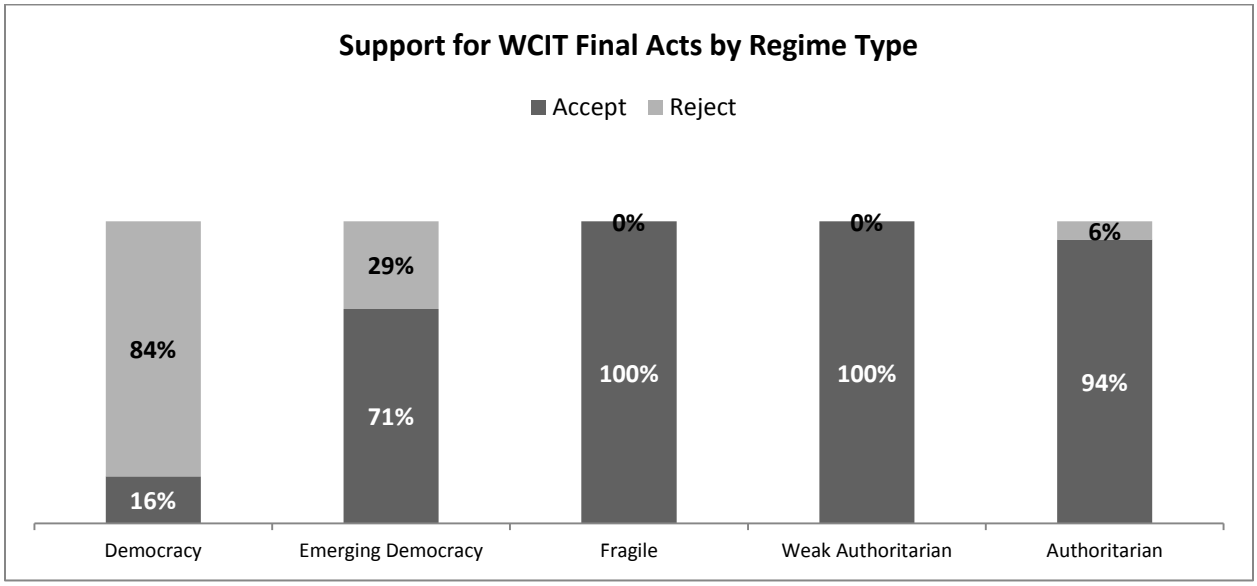
These telecommunications companies represented by ETNO were interested in a system where they would be able to benefit from taxing different lanes on the internet based on types of data, based on content or quantity of usage. One frequently used and useful analogy depicts companies like Deutsche Telecom and France Telecom as having built the "roads" for the internet and wanting to receive a return on investment from the "carmakers" like Google or Facebook for using up the "lanes" of the network. In summary, the overall reaction and coordinated campaign against the ETNO proposal can be summarized as consistent with net neutrality advocates and battles that have taken place in the United States:

> [ETNO is] trying very, very carefully *to use the language of "internet freedom"* and innovation, in order to then explain why the ITU should put in place a proposal that effectively forces local regulators to divert money from the companies who innovate, to the lazy monopolists. This is one of the reasons why so many folks interested in keeping the internet truly free and open are quite concerned about ETNO's proposal. It's not designed to benefit the Internet or to encourage innovations. It's just designed to divert money from those who innovate to the telcos who haven't had to innovate.
>
> *~ The Center for Democracy and Technology (September 10, 2012)*

So amongst the substantive discussion points raised by the CDT, several themes were sounded: first, the multi-stakeholder model governing the internet works and therefore doesn't need to be fixed or restructured in a more centralized format by the ITU; second, that discriminatory pricing tiers would negatively impact users by making some data or content more or less expensive to access; and third, that the internet ecosystem as a liberalized market was sufficient and had proven successful at cultivating innovation for content providers—i.e., future profit centers would be in the content and service side, not telecommunications. So, despite the seemingly obvious story that democracies were against the ITU and nondemocratic countries were for it, there was a complex economic battle taking place between telecommunications corporations and service-based corporations (see Figure 9). All of them, referring to the private sector stakeholders, from different opposing camps, were using the discourse of internet freedom

to fight for their economic self-interests. Oddly enough, the least likely direct beneficiaries of internet freedom were actually the citizens and users and their democratic interests.

Figure 9: Advanced Industrial Democracies' Opposition to the WCIT ITRs



Note: Figure prepared by author based on data collected from the WCIT Leaks documents archive, combined with Polity IV regime typology data.

Conclusion: Miscommunicating and Colluding with the Authoritarian Threat

Did a meaningful policy framework promoting internet freedom in the interests of users and citizens emerge from the private sector stakeholder community? Mostly the answer to this question is a unanimous no. In this chapter I have shown how the private sector stakeholders have internal divisions, and externally, are also not incentivized in any useful way to care about their users' welfare. In fact, the only glimmers of recognition and self-regulation are coming from the encouragement of civil society stakeholders who are allying with them pragmatically in the several contentions that the private sector faces with state powers on infrastructure regulation. But I have also shown the many ways in which internet freedom has been exploited by these actors towards altogether unrelated ends, like justifying the private sector's hegemony on infrastructure regulation but under the label of "multi-stakeholderism." In my concluding thoughts, I will end this chapter by introduce two very simple reasons why the private sector stakeholders cannot be expected to generate new norms for the internet freedom proto-regime: first, they actively misrepresent the authoritarian threat which weakens the justifications to establish a viable internet freedom regime; second, these stakeholders have routinely provided both expertise and technologies to dictatorships in both materially and technocratically.

As an initial illustration of the first point, take for example that the ITU Constitution itself allowed all states the right to stop any communications "which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency"—in short, states already had the sovereign right[18] to decide what constitute a threat to their security, order, and decency. But in this analysis so far, one of the most common tropes used by WCIT opponents was the threat that authoritarian regimes were about to hijack the internet. The Arab Spring provided an easy source of examples and visceral imagery to draw upon and elicit human rights and civil liberties concerns, and the private sector has exploited that imagery and its social capital to largely unrelated efforts. But beyond what technology providers promoted, how serious was this authoritarian threat? What, if anything, was new?

Authoritarian regimes had long used their powers to actively monitor and control internet use, especially in sensitive political cases. Further, the widely recognized exception allowing states to interfere with digital systems in the name of national security had also been routinely

[18] Let us not forget that states, being in a perpetual state of anarchy in international relations, have also more importantly always had the *power* to do so as well.

used by countries like the US and Russia alike to monitor data over Wi-Fi networks, track cell phones, and monitor content in the name of fighting internet-enabled terrorism. Simply put, the authoritarian threat was being exaggerated purposefully to oppose the ITU, and though it was not factually incorrect to say that it existed, nothing new was threatening internet infrastructure in the proposals forwarded by nondemocratic states—mainly because the ITU had no power to enforce or limit such control protocols. Civil society's pragmatic concern to not legitimize state power is understood, but this did not in any way affect the private sector.

For example, even the most outrageous proposals made by the harshest authoritarian regimes attending WCIT were not fundamental threats to the internet, particularly because states were already empowered to do what they wanted within their borders. But as civil society stakeholders lobbying against WCIT had noted, these moments were symbolically important because of the norms such moments promote and make acceptable:

> Proposals from Russia, China, and Arab countries may not be binding even if WCIT reaches unanimous approval—each state has voluntary compliance—but even the discussion of some of these problematic issues *would be the first time that the outright control of online communication would be discussed in the backdrop of a global treaty negotiation*. This is why WCIT must be opposed by civil society and democratic nations alike. The ITU and no other UN body should be entertaining and giving legitimacy to clear violations of human rights and civil liberties.
>
> *~ Participant interview at WCIT, Dubai (December 2012)*

Leaked proposals from the ITU's closed gathering in Dubai did reveal a broad consensus among the pack of authoritarian countries to endorse national control over internet providers, internet traffic, and internet engineering. While most states that had the technical and economic ability to impose such control were already doing so, official policy language was gaining strong momentum at WCIT in ITR proposals, such as the following: "Member States shall have the *sovereign right to manage the Internet within their national territory*, as well as to manage national Internet domain names." Another such proposal achieved particular notoriety among civil society and human rights observers—a plenary meeting document sponsored by Algeria, Saudi Arabia, Bahrain, China, the UAE, Russia, Iraq, and Sudan—complete with Microsoft

Word-tracked changes and comments. Another from the plenary meeting, the "Arab States Common Proposals" signed by Bahrain, Saudi Arabia, Egypt, the UAE, Iraq, Libya, Kuwait, Morocco, Oman, Qatar, Sudan, Tunisia, Jordan, Lebanon, the Comoros, Djibouti, and Somalia, was leaked as early as August. Modifications included the following:

1. "These Regulations recognize the right of any Member State, subject to national law and should it decide to do so, to require that operating agencies, which operate in its territory or provide an international telecommunication/ICT service to the public in its territory, be authorized by that Member state."—Mod 9
2. "Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance, and to regulate the national Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic."—ADD 31C
3. "Member States shall have the right to request information on the routes used, and may impose any routing regulations in this regard, for the purpose of security and countering fraud."—C68

Although authoritarian states were not winning new legally binding battles, they were generating explicit policy language and populating policy discussions with norms legitimizing state power as a necessary apparatus for the regulation of internet architecture and digital systems. This is why civil society organizations opposed not only the substantive proposals but also the ITU regime in general for making it possible for such language to be cultivated.

Some of the language proposed by states even promoted establishing a legal right and norm for member states to access international communications services. One of the most troubling articles proposed, Article 5B, stated that member states should take "necessary measures to prevent the propagation of […] electronic communications" which was open to interpretation and could include communications traveling over the internet. The same article also referred to "bulk" and "unsolicited" communications which empowers states to block protected content, thereby opening up legal methods to censor digital communications. For example, emails sent by human rights groups could be classified as bulk email and therefore a legitimate type of communications that states could legally block. But the larger point here is that while authoritarian states were organizing and introducing new potential threats, the private

sector and its vocal intentions to "protect the internet" did not connect substantively or logically to these real threats.

Secondly, beyond not substantively contributing to the internet freedom norms and standards in any sensible way, private sector stakeholders have actually been some of the most serious violators of internet freedom! Several methods and technologies have been identified as the material and technocratic tools of online political repression, including keyword-list blocking (e.g., blocking terms like "democracy"), domain-name system poisoning (misdirecting IP requests), blocking IPs (e.g., blocking activist websites identified as regime opponents), bandwidth throttling (limiting the amount of traffic to forcefully limit internet access during sensitive political events, like elections or protests), traffic classification (similar to bandwidth throttling, but a more sophisticated method for specifically limiting transfer of files like videos or documents), and shallow and deep packet inspection (identifying the specific content traveling through digital systems from senders and intercepting them before they reach the receiver). Most of these high-tech tools and their trades craft are designed in Silicon Valley and related corporations based in advanced industrialized Western democracies:

> US information technology companies, including Yahoo!, Microsoft, Google, and Cisco Systems, have provided willing, direct, sustained, or comprehensive support to […] Internet censorship and political control efforts.
>
> *~ Congressional Research Service report to the US Congress (R41120)*

For example, Yahoo! was complicit in the arrests of Chinese internet users by providing email account data to Chinese authorities, including data about Chinese journalists in Hong Kong. Microsoft shut down sites by political bloggers, blocked search terms like "democracy" in repressive countries, and cooperated in censorship policies in the deployment of its services as well. Content service providers have also been complicit in servicing the technology needs of repressive regimes. The likes of Cisco Systems, Juniper Networks, Nortel of Canada, and Alcatel of France have gone further by providing censorship infrastructure, filtering software, and surveillance systems.

So in conclusion, it seems, then, that the research labs and hackspaces generating the cutting-edge strategies and norms to help dissidents and democracy promoters in repressive

political systems are not being substantively engaged by private sector stakeholders. The political technologists and civil society stakeholders examined in the previous chapter (Chapter 4) were correct to realize their concern that designing tools and strategies was not enough. This chapter has shown us that when the substantive task of internet freedom promotion comes to the international policy-making stage, private sector multinational companies have a strong (and manipulative) upper hand. Furthermore, this event analysis of the WCIT proceedings and the politics and contentions surrounding the mobilizations up to that December in Dubai have shown us two very important realities. First, that multi-stakeholderism as a frame to generate new democratically-oriented norms is not a useful way of designing internet freedom policies in the interests of users and citizens because it serves the material conflicts and interests of the private sector at the expense of civic and political rights. Second, that digital infrastructures providers, be they *content providers* like Google, or *access providers* like ETNO, are not incentivized to define internet freedom from a normative stance to protect their own users, least of all democratic activists in repressive political systems. Worst of all, private sector stakeholders have actively manipulated the discourse and public sentiment surrounding internet freedom after the Arab Spring towards furthering their narrow economic interests, while simultaneously colluding with and helping authoritarian states improve their repression tactics.

Chapter 6 – Digital Infrastructure Politics in the Post-American World

The network of Western democratic states behind the initial promotion of internet freedom discussions was formally launched soon after major Arab Spring protests subsided in December 2011 at The Hague by Dutch foreign minister Uri Rosenthal. The most public structure of this coalition, the Freedom Online Coalition, was an overt response to the Arab Spring protests that began in December 2010. Beyond the 100 million USD to promote internet freedom-related research, development, and intervention projects, and the 10 or more independent but coordinated stakeholder summits that have been conducted and sponsored since, what can we say about internet freedom promotion after the Arab Spring? To start, we can begin by noting that this internet freedom proto-regime falls outside traditional contours of internet regulation work.

Using the 2011 popular movements for democratic change in the Arab world as a point of departure, this study has traced this new international network of digital infrastructure stakeholders engaged in policy entrepreneurship promoting an internet freedom regime. These *state-based*, *civil society* and *private sector* stakeholders were initially introduced to each other under the auspices of the Freedom Online Coalition meetings sponsored by a pack of advanced industrialized Western democracies led by the US, after the Arab Spring revolutions. The politics of internet freedom examined in this study connect with but extend far beyond the boundaries of the standard institutions, like the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Internet Governance Forum (IGF), the Internet Society (ISOC), or the UN's International Telecommunication Union (ITU).

In this transnational network ethnography, I have traced these stakeholders' communities of practice and activities to help explicate their normative frameworks and underlying reasons for pursuing internet freedom work. The main outcome is that powerful actors like states and multinational corporations are treating digital infrastructures in very political ways. Furthermore, civil society observers are struggling with these stakeholders to secure some democratic needs for users and citizens, who are increasingly using it as a public information infrastructure to enact their public and civic interests. Observing these disparate stakeholders between December 2010 (when the Arab protests began) and December 2012 (when the WCIT negotiations in Dubai concluded), it a cohesive and actionable internet freedom policy regime has not yet emerged. Generously, we can say that the efforts constitute a proto-regime in formation. But to establish

and stabilize an effective regime that best serves the political, perhaps democratic, interests of global digital media users, several key features of this regime have not yet been reconciled. What are these conflicts of interests and competing goals?

We can address this core question in this study because the Arab revolts have now brought these stakeholders and their competing interests to the forefront of public global communications policymaking. ICT tools and their undergirding infrastructure have become increasingly recognized as an important part of the modern causal recipe and process behind contemporary democratization successes and failures. This study sought to empirically investigate the following sub-research questions:

- Who are the new stakeholders involved in and being engaged to define the issues and contours of internet freedom policy? (Chapter 3)
- Where is the substantive intellectual and experiential knowledge being drawn from to construct the new norms and types of policies about digital infrastructure? (Chapter 4)
- How coherent and coordinated are these norms when it comes time to promote internet freedom on the global stage of policy making and treaty negotiations? (Chapter 5)

In this chapter (Chapter 6), I consolidate and address those important themes, to address the final research question: *What are the best prospects and new challenges that continue to face these stakeholders in better scoping this proto-regime to effectively promote a consolidated and user-centered internet freedom policy agenda?*

First, there are several enduring conflicts of interest that must still be reconciled for this proto-regime to emerge. The dependence on state-actors as being the main drivers of an internet freedom regime has not bided well (especially since they are the stakeholders most likely to violate internet freedom principles). Additionally, the ineptitude of the private sector actors to take internet freedom promotion seriously or consistently is an enduring threat to the viability of any so called "internet freedom" policy regime. So we must clarify the status of these roadblocks in the political economy of internet freedom work, and identify alternative avenues for civil society activists to find workarounds that may be realistically achieved within the parameters of the strategies have been observed through this investigation.

By doing so, there is reason to be hopeful: a key contribution of this study has been to realize how civil society actors and tech-savvy digital activists have effectively turned esoteric infrastructure politics into an international public issue concerning civic life. Before the Arab

Spring, much of the discussions surrounding technology and internet policy norms were engaged by business or policy actors, not social and political activists. This new reality presents several opportunities where new alliances can be forged between Western democratic states and politically-minded and tech-savvy civil society activists. The policy formation period after the Arab Spring has forged a growing global public recognition that digital infrastructures undergird modern processes of political change.

Moreover, this reality has implicated state powers and technology providers as often colluding stakeholders that have manipulated digital infrastructure in political ways with severe negative consequences for digital dissidents and democracy promoters abroad. The study of digital infrastructure politics is necessary to understand how the technological affordances that have come to empower (and sometimes threaten) mediated political participation also depend on the complex transnational political economy that undergirds digital tools and online environments. A significant gap in comparative political communication scholarship can be bridged productively with this new insights offered by taking digital infrastructure politics seriously.

Thus, investigating the ongoing developments around internet freedom policy promotion is not the only starting point for doing so, but there are several reasons why it is a logical one to begin with. First, internet freedom promotion is important for understanding how the new digital infrastructures that support political communication and participation in both democratic and nondemocratic regimes continue to emerge as a consequence of ongoing transnational political economic struggles. Second, it is necessary to advance our research agenda to anticipate and critically assess the developments of this broad policy arena particularly by understanding the new actors doing this work, like tech-savvy activists. Third, doing so will allow us to go beyond describing how our modern public communication systems are, towards better understanding how these systems come to be through historical conditions, political perspectives, and the intentional and powerful actors constructing them (Hallin and Mancini 2004).

Three Impasses and Opportunities for the Internet Freedom Proto-Regime

Activists and dictatorships have come to see digital technologies as political goods that can be used (and constructed) as both democratic scaffoldings and as authoritarian panopticons. The common struggle has been one pitting citizens and civil society actors against state powers and

their security forces to control the political uses of digital infrastructures. But the important thread uniting these opposing stakeholders (state powers vs. civil society) has been the technology companies (i.e., the private sector) that own and maintain key pieces of digital infrastructures. It is the case that unpacking internet freedom politics today requires investigating at least three core categories of stakeholders: state powers, civil society, and the private sector.

In addition to explicating the activities and interests of these three stakeholder communities, I sought to unpack the different ways in which these actors defined, and therefore fought over "digital infrastructure." In Chapter 1, I articulated that state actors tend to view internet freedom as the task of safeguarding *critical infrastructure*. Private sector stakeholders tasked with innovating and implementing digital infrastructures view it as a *consumer good,* and the digital activists who use it for political organizing treat it as a *civic tool* in their growing digital repertoire of mobilization strategies.

Recognizing these competing lenses of digital infrastructure(s) helped to illustrate that state actors' main interests and concerns regarding internet freedom promotion have revolved around the threats of *cyber terrorism and cybercrime*. Private sector stakeholders instead tend to color their approach to internet freedom promotion as safeguarding *multi-stakeholderism and network neutrality* as the main challenge, but these concepts do not translate well in speaking to the needs of citizens and activists. However, the main concerns behind private sector stakeholders revolve around the protocols affecting data traffic, and decisions structuring data pricing on digital infrastructure. Therefore, between states' securitization concerns and providers' profit-maximization incentives, citizens' and activists' goals of *regulating political surveillance and monitoring political filtering* has been doubly challenging work.

How have these competing understandings of digital infrastructure and reasons for doing so shaped the norms introduced to internet freedom promotion? First, *state powers* have been crucial stakeholders because they have the political power to organize and broker interactions among all stakeholders. Although the private sector and civil society have also brokered their own multi-stakeholder gatherings (such as Google, and Access, respectively), advanced Western democracies have been the most dominant and effective organizers of these arenas pertaining to internet freedom. The United States has been the core global leader of this pack of states, and the United Kingdom and Germany have been important international allies legitimizing the issue. Smaller states dependent on their high-tech industries (including Sweden, the Netherlands, and

Ireland) have also pursued ambitious involvement in the US-led internet freedom work because their domestic economies rely heavily on exporting ICTs and infrastructure internationally, but have tended to follow and borrow the agendas of internet freedom work promoted by the US. State powers are also important because they are the key stakeholders opening doors to civil society leaders and digitally savvy political activists (i.e., inviting them to attend internet freedom forums). State actors are the key conveners of internet freedom arenas and have the power to bring together civil society and technology providers to the same table and broaden the diversity of useful understandings surrounding digital infrastructures.

Beyond state actors, the private sector, or *technology providers*, was the high-tech sector of multinational corporations who have innovated and implemented digital infrastructure. They have the core user base of millions of digital media users, which includes the civil society actors who use these providers' digital infrastructures to engage in digital political communication and political organizing work. The norms that seem to unite technology providers include concerns about intellectual property rights when they export their proprietary technologies and software outside of their home countries. However, when observing technology providers in internet freedom forums, their incentives to participate stem from public pressure exerted on them by digital activists documenting their involvement in human rights abuses. Their incentive to join the tables set by state actors is primarily an outcome of public shaming and lobbying work done by civil society and human rights watchdogs—otherwise they have little incentive for pursuing internet freedom discussions.

Finally, consistently the most dynamic and important community of stakeholders has been the energetic technology-savvy transnational *civil society* activist network that has recently arrived on the international policy scene. These relatively new set of actors seem to have agitated rather recently, particularly during the aftermath of the Arab Spring protests. When dealing with internet freedom promotion, these stakeholders do not appear to be congregated in any particular nation-state. Rather, they seem to be constituted by a vast transnational network of issues-based experts and political activists who have found digital rights to be an important domain for them to address. This stakeholder community of infrastructure activists is also the only set of actors attempting to inject the internet freedom discussion into the news agenda of international media and journalistic coverage. These civil society actors seem newly charged with advanced

technical expertise about the inner workings of digital tools and infrastructure that is surprisingly sophisticated and unexpected.

In sum, we can observe here that the three categories of stakeholders are important for different reasons, but must work together to establish a coherent internet freedom regime. Some of them have more incentive to participate because their needs are higher (i.e., civil society). Others, like the private sector do not have an overt reason to participate, but are necessary for reigning in. State powers seem like the best positioned stakeholders to bring both civil society and private sector actors together to the same table, which they have been doing. So how consequential and impactful has this been in generating and consolidating new policy norms?

1. Competing Communities: State-Based and Civil Society Stakeholders

In the preceding section, I reviewed three main categories of stakeholders involved in defining and competing to shape the internet freedom proto-regime. How have these stakeholder's involvement shaped the current structure and consolidation of norms? In Chapter 3, I outlined the two large clusters representing communities of practice that have emerged between state-based and civil society sponsored networks. Furthermore, I articulated the most cogent norms that these distinct communities of practice seem to be pushing forth are in direct competition of each other. Finally, I also noted in this analysis that the private sector technology providers had failed to produce any discernible norms—rather, they have been normatively impotent in the regime formation efforts. In other words, state-based and civil society stakeholders have successfully put forth different kinds of norms to define internet freedom, but technology providers have reneged on their responsibilities of this shared normative project.

I also showed that while there have been at least ten key stakeholder conventions organized by Western democratic states since the Arab Spring, two core normative issues seem to have balkanizing the two largest communities of stakeholders (state-based vs. civil society interests). I demonstrated this balkanization of norms by discussing two policy agenda outcomes that elegantly express the divergent norms. Firstly, the *London Agenda* curated after the London Conference on Cyberspace, an event initiated and sponsored by state-based actors. The norms of this community of stakeholders focus primarily on issues of network security from the perspectives of state powers. Second, I contrasted this normative framework with the first gathering of the Silicon Valley Human Rights Conference and the comparable *Silicon Valley*

Standard – a competing norms framework that differs importantly from the concerns expressed by states, and more directly speaks to the needs of users and citizens.

The state-based London Agenda expressed a set of norms focused on securing and safeguarding digital infrastructure as a "critical" resource of the state itself. States have cultivated the idea that the internet is a fundamental infrastructure (i.e., the "internet backbone") that is at stake and needed protection, as opposed to the users (the perspective of human rights and civil society observers) or the technology designers and regulators (the perspective of corporations and providers). The authors of the London Agenda (i.e., states) also outlined five critical themes to define internet freedom which narrowly concern themselves with state sovereignty in cyberspace. Civil society issues, in the rare occasion that they were raised, were discussed in a highly constrained fashion that lacked the level of nuance afforded to cybercrime issues dominated by state and industry stakeholders. Therefore, states have helped to cultivate public awareness about internet freedom issues, but unsurprising, cybercrime and cyberwar norms have come to dominate their agenda. Civil society's user-level perspectives did not receive any serious attention nor were norms and frameworks developed to address users' needs. Across all policy documents only three normative concerns areas were consistently presented and concerned the welfare of states and providers [but not citizens]: a) cyber espionage; b) cyber terrorism; and c) cyber crime threats.

In contrast to states, the norms cultivated by civil society tend to focus on entirely different issues, and have been arrived at through a very unique process of norms consolidation worth noting. First, as we saw in the network distribution of internet freedom stakeholders, civil society actors were the most influential overall cluster in the global network of stakeholders. Most importantly, it was the LiberationTech-affiliated cluster of policy experts and digital activists that predominantly held the most influential positions in various think tanks and global NGOs interested in internet freedom promotion representing civil society. In counterpoint to the London Agenda, this cluster of stakeholders was formulating its own set of norms and standards, called the "Silicon Valley Standard." This set of norms, developed jointly by technology providers and designers on one hand, and civil society and digital activists on the other, contrasted directly with the state-centric norms consolidation process reflected in the London Agenda.

From the perspective of convention organizers and key figures, the Silicon Valley Human Rights Conference seamlessly integrated established and influential technology policy advisers (e.g., Electronic Frontier Foundation, Citizen Lab, Global Network Initiative, etc.), major governmental representatives in key agencies engaged with foreign policy issues (e.g., the US State Department), indigenous activists experienced in digitally enabled political organizing within repressive political systems (e.g., the Guardian Project, SMEX, Diaspora, etc.), and public policy heads of private sector companies (e.g., Facebook, Google, Twitter, etc.). This has allowed for a far more heterogeneous set of expertise from technology designers, users, and regulators to be confronted and reconciled. Instead of pushing state-determined concerns about technologies onto stakeholders, the Silicon Valley Standard emerged as an outcome of the meetings and discussions itself, and summarized fifteen major norms and issues adopted at the conclusion of the stakeholder gathering from fifteen working groups.

In other words, civil society norms were crowd-sourced directly from a range of stakeholders and experts by directly consulting members of the private sector and civil society actors who attended the deliberations. There was a clear recognition that technology companies do in fact enable, support, or threaten the end user's (i.e., internet users) freedom of speech, access to information, and freedom to associate, and thereby share a burden of responsibility towards their users (something the London Agenda did not do). Therefore, privacy of users (but not necessarily their anonymity) should be the point of focus from the outset when discussing internet freedom, and total transparency of how social data is collected, processed, and protected should be encouraged.

Civil society stakeholders have also championed the idea that the best knowledge in dealing with new challenges related to internet freedom should also come directly from the frontlines, i.e., the users themselves. In other words, technology companies should regularly monitor the human rights impacts of their tool deployment and update their policies and procedures. This push to adopt human rights as a framework at the policy and practice level of the private tech industry, championed for Ruggie's "Protect, Respect, Remedy" approach to be adopted by the UN as Guiding Principles on Business and Human Rights. Thus, the Silicon Valley Standard acknowledged that human rights concerns should also be built directly into the technology innovation and research and development phases from the outset. To do so,

technology companies should be responsible for innovating basic levels of security tools and protocols through better encryption software.

So it seems that when states define the norms behind promoting internet freedom, they focus narrowly on securing the internet backbone from terrorists and criminals by pushing their norms onto other stakeholders. When civil society and digital activists define the norms, they take a much more nuanced and even-handed approach that works to enlist stakeholders with distributed responsibilities that embrace the multi-layered nature of digital infrastructures. Nonetheless, it is most notable that the private sector has been merely a passive participant in constructing any of these norms—these stakeholders have neither introduced, nor developed any of these ways of promoting internet freedom. Technologies providers again simply seem to be passively ignoring the internet freedom norms consolidation process overall and thereby evading their responsibilities in constructing internet freedom promotion.

2. Avenues Forward: Enjoining Civil Society with Political Technologists

The big finding from Chapter 3 was to identify the relative sizes, positions, and relationships between the communities of stakeholders working to promote internet freedom. Moreover, this analysis led me to identify that the core ideas, norms, and practices for promoting internet freedom were originating not from the powerful Western democratic states convening the meetings, but rather the transnational network of tech-savvy civil society and digital activists that were already somehow energized on these issues. Again, civil society-led initiatives, as exhibited in the Silicon Valley Standard, produced the most interesting sets of ideas and norms to draw other diverse stakeholders together.

The analysis in Chapter 4 pushed this line of inquiry deeper to investigate the origins and capabilities of civil society stakeholders. In contrast to state-based stakeholders, civil society actors seemed to view digital infrastructure as a much more malleable environment and therefore able to be redesigned with new affordances that promote internet freedom both through its architecture, and through its regulations and policies. In Chapter 4 I extend the stakeholder analysis from Chapter 3 to ethnographically investigate the most novel and important category of civil society stakeholders that seemed to be contributing the "first fix it, then regulate it" approach to promoting internet freedom. To do so, I focused on the community of technology designers and political hacktivists working on self-described "liberation technologies" projects—

discussions, tools, and practices aimed explicitly at helping dissidents and human rights activists use digital infrastructures and ICTs for their political goals.

In this analysis, I examined the political technologists originating in the LiberationTech online discussion community and the work, practices, and ideas they had cultivated since as far back as 2008. These activists represent a core sub-culture of tech-savvy helpers working alongside civil society and political activists providing them with technical help and strategic insights to navigate the opaque world of infrastructure politics. To review, I will now summarize who these individuals are, which organizations and institutions they are grounded in, in order to contextualize the contributions they are making to internet freedom promotion work.

This technical community shares a set of normative beliefs about the political significance of communications technologies and digital informational tools they wanted to examine and design that state actors tend to under-state, and technology providers tend to undermine. They shared a complex causal understanding that these political technologies can have important impacts on the users employing them. They also shared strong notions of community standards regarding open software and peer-reviewed processes for the development, deployment, and uses of said tools. Finally, they shared concerns about the policy developments surrounding political technologies at the hands of both private sector technology corporations and state-based governmental agencies, with a presumption that the welfare of users also depends on the regulatory norms surrounding digital infrastructures within which ICT tools and web-enabled practices are embedded.

Furthermore, approximately 85 percent, or the overwhelming majority of them, can be described as technical engineers skillful in information technology design and programming, and several of whom describe themselves as hackers working in the IT security industry. These members have all attended an overlapping small number of research institutions and conferences. These labs and discussions have allowed this collective to train and acquire its technical skills and specialized knowledge base. They work and share information on the same email list and discussion networks, but they also extend these collaborations offline to the conferences and trade shows they jointly frequent. The core network of supporting institutions where they meet or learn their trade includes mostly North American universities and some Western European ones more peripherally.

Beyond advanced research universities, the San Francisco–based Electronic Frontier Foundation (EFF) and the Washington, DC–based New America Foundation (NAF) represent some of the most important policy incubation spaces to which LiberationTech members have graduated. They have "graduated" in the sense that, at some point before taking these policy positions, they spent time in programs like Harvard's Berkman Center for Internet and Society; Stanford's Center for Democracy, Development, and the Rule of Law; MIT's Media Lab; and Yale's Internet and Society Project where they developed their thinking and relationships to digital politics work. Collectively, these new policy institutions seem to connect, and increasingly house, the most active members of the discussion community designing political technologies.

Overall, all of the top locations are based within the political borders and economic systems of Western democracies. All of these locations are strictly bound to the most industrially advanced Western democracies, and include the United States, the United Kingdom, Canada, Germany, the Netherlands, and Sweden. Although the top ten cities around which the labor of political technologists are concentrated including the examples stated previously, the technology industries of the United States remain the home of the vast majority of this work. Silicon Valley, which continues to have the largest presence of both venture capital and social entrepreneurship projects, is the single most important location of socialization in influencing the ideologies and tactics of these actors. These political technologists in the aftermath of the Arab Spring are becoming central to the designing and shaping of the policies and regulatory frameworks surrounding internet politics.

What are the practices and ideologies that seem to define these important civil society activists? This community of practice can hold its own position comparable to advanced private sector technology providers (but at a much lower scale) when it comes to creating their own technical and digital toolkits. They have applied their technical abilities to build crowd-sourced programs to directly assist political activists behind the lines. They also function as reliable and secure technology advisers informing the practices of digital dissidents and international journalists reporting on digital repression and offline oppression taking place in authoritarian regimes. They have also cultivated a clear standard in supporting transparency and peer-review behind all their internet freedom and censorship circumvention strategies, be it technical fixes or

legal frameworks. In contrast, state-based approaches tend to be far more opaque and unimaginative.

These political technologists have done the important detective work of identifying where censorship tools originate, and break stories about which governments are engaging in illegal surveillance practices. Furthermore, these political technologists have a deeper appreciation for the different kinds of real users that are impacted by, and require internet freedom norms cultivated into policy. For example, state-based approaches define internet freedom from a broad and vague approach servicing the interests of macro entities, like governments. In contrast, these political technologists provide purpose-built norms specific to "average users," "power users," and "infrastructure-aware users" to name a few. At the very least, this facilitates the recognition that there are different digital constituencies with different risk environments requiring appropriate internet freedom assistance. This complex understanding of users is also important because many of the technologists in this collective are also active movement leaders and political activists. For example, many of them have been active members of the Occupy Wall Street movements.

Lastly, these political technologists actively seed and disseminate their expertise to different stakeholders hitherto not involved in internet freedom promotion, specifically journalists and movement leaders. These direct interactions and diffusion of ideas between technology experts and technology users at a high level of expertise and sophistication helps to explain the process by which esoteric internet regulatory politics are rapidly becoming a public agenda item in many countries. These feedback channels between civil society activists and political technologists illustrate the important work regularly done to assist a range of nontechnical specialists, including activists, journalists, and policy makers.

In sum, these political technologists do more than create experimental prototypes of political tools. They also apply the lessons from their successes and failures to improve them, and appreciate the complex constellations of factors affording or limiting these tools' intended impact. They work hard to teach best practices and brainstorm strategies and solutions on a case-by-case basis for desperate activists and journalists from some of the most repressive and dangerous political environments today. The presence of these technical experts that have seemed to have allied themselves with tech-savvy civil society stakeholders is an important

source of the new thinking and norms being introduced to internet regulation and internet freedom promotion work.

3. Enduring Challenges: The Private Sector and Recalcitrant Internet Regimes

In the previous section, I argued that states have provided the forums to draw together the other stakeholders involved in internet freedom related activities, specifically civil society and the private sector. However, the biggest challenge still facing the internet freedom proto-regime has been the lack of mechanisms to draw in private sector technology providers that create the material infrastructure comprising ICTs. Therefore, in Chapter 5, I investigated the activities of the private sector in the lead-up to the December 2012 WCIT policy making treaty in Dubai to observe what interests these elusive stakeholders tend to pursue.

I justified the selection of the WCIT event as a conceptually and historically critical one for studying the formations of the internet freedom proto-regime in question. The United Nations-sponsored ITU gathering, titled The World Conference on International Telecommunications (WCIT-12) was the most important field site for this investigation because it represented the first time in the past twenty-five years that nation states from around the world gathered to negotiate and update a major global communication treaty regime: the International Telecommunication Union (ITU). In this event analysis of the WCIT-12 proceedings, I evaluated the lack of consistency of the different infrastructure stakeholders to effectively promote internet freedom norms on the international policy-making stage.

In this event analysis, the private sector not only eluded its responsibilities in securing internet freedom for its' own users, but furthermore exploited the political economy of the internet regulatory environment to co-opt the internet freedom proto-regime for its purposes. Civil society actors are cognizant of this but unfortunately relegated to making pragmatic compromises, whilst state powers continue to accept the standards set forth by the private sector without much counter balance. The technology sector in the US actively lobbied both US Presidential campaigns in 2012 and won a landslide vote from Congress to vocally oppose the ITU gathering. During the negotiations in Dubai, the private sector also succeeded in equating internet freedom promotion with promoting multi-stakeholderism, thereby co-opting internet freedom proto-regime into an industry battle between the ITU and ICANN. The constrained civil society stakeholders were therefore pushed to make a pragmatic decision to support the lesser of

two less-than-ideal communication regimes—the multi-stakeholder model—because the risks of supporting the ITU introduced greater opportunities for states to develop greater legitimacy in managing digital infrastructures.

This pragmatic decision by civil society meant joining forces with the private sector against the UN's ITU regime (which favored infrastructure providers), in favor of the multi-stakeholder model that also privileged the private sector (which favored content providers). Their motivation to do so was to keep internet governance clearly outside the domain of state-based stakeholders. Civil society organizations did not want any state powers to lobby and adopt standards and definitions that legitimized states' rights over digital infrastructures.

With regards to internet freedom, the private sector stakeholders were merely using the discourse of internet freedom to fight for their economic self-interests. Technology providers, in short, they have actively serviced both authoritarian and democratic states' technocratic needs for digital infrastructure expertise. They have actively colluded with dictatorships and sold them sensitive surveillance and filtering technologies, and on the other hand, they have lobbied actively at "home" in democratic states to support multi-stakeholder internet governance. The effort to organize a coalition to oppose the ITU was taking place on several simultaneous fronts, and I documented this as starting as early as June 2012, six months before the treaty negotiations in Dubai.

Despite the seemingly obvious story that democracies were against the ITU and nondemocratic countries were for it, there was a complex economic battle taking place between telecommunications corporations and service-based corporations. The other major front for the battle against the ITU regime centered on convincing several advanced Western democracies to support the multi-stakeholder model over one centralized under UN bodies dominated by states. Private sector stakeholders accomplished this by convincing other stakeholders that the multi-stakeholder model governing the internet worked and therefore didn't need to be fixed or restructured in a more centralized format favored by the ITU; second, that discriminatory pricing tiers would negatively impact users by making some data or content more or less expensive to access; and third, that the internet ecosystem as a liberalized market was sufficient and had proven successful at cultivating innovation for content providers—i.e., future profit centers would be in the content and service side, not telecommunications.

How can a meaningful policy framework promoting internet freedom in the interests of users and citizens emerge from the private sector stakeholder community? Technology providers have actively argued for a self-regulatory approach (i.e., multi-stakeholderism), which has done little to promote internet freedom. In fact, private sector stakeholders are not incentivized in any useful way to care about users' welfares, especially if they are "foreign" political dissidents already living in repressive countries—after all, the paying client in this situation is the authoritarian regime, not its citizens. Beyond not substantively contributing to the internet freedom norms and standards in any observable way, private sector stakeholders have actually been some of the most serious violators of internet freedom!

Several methods and technologies have been identified as the material and technocratic tools of online political repression, including keyword-list blocking (e.g., blocking terms like "democracy"), domain-name system poisoning (misdirecting IP requests), blocking IPs (e.g., blocking activist websites identified as regime opponents), bandwidth throttling (limiting the amount of traffic to forcefully limit internet access during sensitive political events, like elections or protests), traffic classification (similar to bandwidth throttling, but a more sophisticated method for specifically limiting transfer of files like videos or documents), and shallow and deep packet inspection (identifying the specific content traveling through digital systems from senders and intercepting them before they reach the receiver). Most of these high-tech tools and their trades craft is designed in Silicon Valley and related corporations based in advanced industrialized Western democracies—a fact admitted in US Congressional research reports:

> US information technology companies, including Yahoo!, Microsoft, Google, and Cisco Systems, have provided willing, direct, sustained, or comprehensive support to […] Internet censorship and political control efforts.
>
> *~ Congressional Research Service report to the US Congress (R41120)*

In Chapter 5, I showed that when the substantive task of internet freedom promotion comes to the international policy-making stage, private sector multinational companies have a strong (and manipulative) upper hand. This event analysis of the WCIT proceedings and the politics and contentions surrounding the mobilizations up to that December in Dubai also demonstrated two important realities. First, multi-stakeholderism as a framework to generate

new democratically-oriented norms protecting digital activists is not viable because this approach exclusively serves the material conflicts and self-interests of the private sector at the expense of civic and political rights. Second, digital infrastructures providers, be they *content providers* like Google, or *access providers* like ETNO, are not incentivized to define internet freedom from a normative stance to protect their own users, least of all democratic activists in repressive political systems. Thus, civil society stakeholders still need work on pressuring the technology providers into action, and my suggestion in the previous discussion to ally with political technologists may be one way to elucidate the private sector's esoteric violations.

This is certainly a challenging task for civil society actors. On the one hand, state based stakeholders have not yet shown that they can reign in the private sector stakeholders, particularly because states lack the organizing norms and criteria to address users' internet freedom needs. On the other hand, private sector stakeholders have actively manipulated internet freedom discourse to serve their profit-maximizing incentives. Then, where must civil society activists now turn toward? To provide an important glimmer of optimism, in the following conclusion section I will showcase some new partnerships that the civil society stakeholders seem to be forged with the assistance of their tech-savvy political technologists in the context of the NSA global surveillance crisis.

Internet Freedom Promotion after the NSA's Global Surveillance Scandals

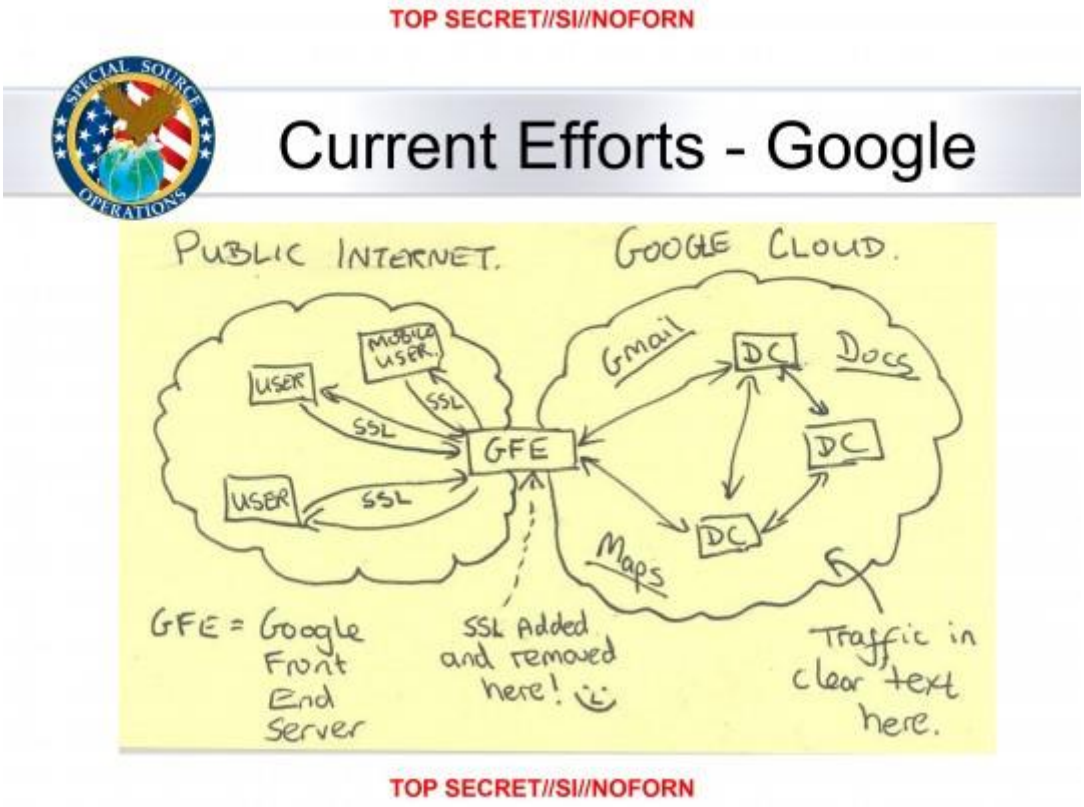
In late 2012, while the pack of Western democratic nations comprising the FOC internationally promoting "internet freedom" an American computer programmer and former NSA contractor leaked classified details about several advanced democratic nations engaging in mass surveillance programs. As it is now well known, the violating nations are the same, and the US was the leader in both cases. Although the leaker was not a prominent member of the civil society or political technologists communities identified in this study, his story is quite familiar.

Edward Snowden was a hacker in his late-20s who was politically engaged, but tended to vote for third-party candidates, eventually settling for Ron Paul. Media personalities have commented this may indicate his libertarian political stances. And like our LiberationTech community, Snowden was also a long-time contributor and discussant on several technology and politics discussion boards, most prominently the Ars Technica chat-rooms. His consistent concerns there focused on the unregulated reach of state powers in infiltrating the very digital

infrastructures that increasingly houses the most intimate political and social experiences of private citizens. He was also an avid self-described "cyber libertarian technologist" – and often publicly displayed his support for the Electronic Frontier Foundation.

Snowden's leaking of classified details (see Figure 9) also helped to jolt the internet freedom supporters from civil society into action. As it turned out, while advanced Western democracies were actively promoting internet freedom issues, they were actively violating all of these norms in the most advanced, well-funded, and sophisticated ways in history. These norm violations and illegal wiretaps have not been used to brutalize citizens, as is routinely done in non-democratic states, but highlights a glaring violation of the most basic premise behind doing internet freedom work: preserving the privacy and security of democratic citizens. What are some dimensions and consequences of the 2013 global surveillance disclosures and ensuing controversy towards promoting internet freedom? To think about this, let's begin by grasping the breadth and depth of the NSA scandals.

Figure 10: Leaked Notes about NSA's Surveillance Diagram



Note: Figure retrieved from top-secret documents leaked[19] by Edward Snowden.

[19] "NSA Infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say" (The Washington Post, October 30th, 2013).

Western democracies comprising the Freedom Online Coalition have routinely violated all of the internet freedom norms they have been promoting since the Arab Spring—and the United States has led the way. Several US agencies have thus far been implicated, including Cyber Command, the Department of Justice, the FBI, the CIA, and the Department of Homeland Security. Several countries in the Freedom Online Coalition have actively partnered with these mass surveillance initiatives, including the security agencies from the United Kingdom, Canada, Australia, New Zealand, and Germany. The projects they have cultivated are extensive and unprecedented. The most publicly covered program, *PRISM*, is an ongoing clandestine mass electronic surveillance data mining program tapping directly into the public services of Microsoft, Yahoo!, Facebook, Google, Apple, and Dropbox, to name a few.

Boundless Informant, a project under the NSA, exploits internet metadata to understand live transmissions around the world, covering the US and Canada, Europe, Africa, Latin America, and Asia-Pacific countries. This is technically feasible because, according to the NSA's own leaked project slideshow, "much of the world's communications flow through the US." Indeed, Google currently serves 25 percent of all North American internet traffic and has data centers on four continents. This structural opportunity has been exploited by affiliated projects, like XKeyscore, to analyze internet data about foreign nationals across the world, Dropmire, to bug foreign embassies and NATO allies, and Fairview, to collect personal email data from foreign citizens, to name a few.

How have other state-based and private sector members of the Freedom Online Coalition, and associated democratic states, responded to these controversies? While the US Department of State has led the Freedom Online Coalition, the NSA has collected over half a million email addresses from Yahoo!, Hotmail, Facebook, and Google—daily. That amounts approximately to illegal collections of over 250 million private email address per year. India has asked its top 400,000 officials to curb use of Gmail, while also coercing Canada's BlackBerry service to give the government the ability to intercept messages. India now has the technical ability to track emails, attachments, and web browsing, in real time. In the US, the FBI has recently admitted that it has taken control of the Tor anonymity software used by Arab Spring dissidents. New Zealand is currently seeking tougher data protection laws to protect itself from US spying, while also recently legalizing domestic spying on its own citizens. Sweden has joined the "Five Eyes" spying partnership with other Western democracies to exploit its geo-strategic position

connecting data traffic from east and west, while the Minister of Foreign Affairs is publicly organizing support for internet freedom principles.

While the state-based members of the internet freedom regime have openly violated all of the norms binding this regime, private sector stakeholders have passively accepted their violations, sometimes with open acknowledgement. Executive Chairman of Google has noted that "Google policy is to get right up to the creepy line and not cross it," and simultaneously Google admitted to its Gmail users not to expect privacy when sending emails. Major telecommunications providers have also rarely, if ever, challenged NSA demands for metadata – putting them in league with the ISPs of Saudi Arabia or Iran. And Twitter has acknowledged that the US government makes the most data requests than any other country, citing it is required to follow federal orders.

All this has left the tech-savvy civil society stakeholders with the challenge of responding to state-based violators of internet freedom both at home and abroad, and the unregulated collusions to do so coming from the private sector. How have they fared in the recent NSA scandals? There seems to be a growing movement to force technology firms to publish more reports on the requests they are receiving from governments. Apple, Facebook, Microsoft, and Yahoo! have done so, but Google has not. Over 100 global civil society groups have released more principles to design human rights principles into government surveillance work, with Access and the EFF leading the pack. Without public pressure, these statements of principles, although substantive, may simply be ignored. But there are indications that the public is being mobilized to increase this pressure.

In Germany, Posteo, an encrypted local internet provider increased from opening 2,000 accounts per week to 20,000 since the NSA scandal broke—apparently German citizens have been flocking away from Gmail and Hotmail. Thousands have also turned up to protest, while half a million signatures have been collected by Stop Watching Us, and is being publicly supported by Republican and Democratic organizations in the US. Several civil rights organizations are also suing the US and Canadian governments in class action law suits to introduce legal restraints, but this will take time. Despite these seeds of change, public understanding of the privacy violations remains constrained to the small group of epistemic experts and political technologists.

For the broad work of promoting internet freedom internationally, perhaps the most dangerous consequence of Western democracies acting against their own purported norms is the new confidence they have given rising powers to do the same with impunity. In the latest international internet governance forum hosted in Brazil, BRICs countries have united around the idea of "independence through infrastructure." This movement and coalition includes emerging countries and authoritarian powers: Brazil, Russia, China, and South Africa, have announced a high-capacity undersea fiber optic cable that will directly connect them, bypassing and autonomous of American and Western information infrastructure:

> "[This is] allowing internet traffic to deliberately circumvent United States and European entry points. […] Indeed, the cable should greatly benefit connectivity in the developing world. Avoiding traffic flows through the U.S. and Europe will not in itself preclude state surveillance of communications, and could even open the door to surveillance by more governments."
>
> ~ Access blog [October 8, 2013]

Meanwhile, Russia is now reinvigorating its support for the ITU to have greater influence in managing the internet's technical standards – putting greater legitimacy into the shared hands of state-powers. Oddly enough, it seems that the very democratic state-based actors that initiated the internet freedom regime to curtail the authoritarian and non-democratic regimes have greatly empowered them to exercise greater control on the internet, in the name of state autonomy.

Ironically, it is perhaps a 1975 comment by Newsweek, about a previous era of mass surveillance and wiretapping, that most eloquently summarizes the negative consequence of charging state powers as the sole managers of new communications infrastructure:

> "But the central issue raised by NSA's huge eavesdropping network is not really whether the agency has over stepped its authority. The point is that the scientific capability for this wholesale monitoring now exists, and where the capability exists, so too does the potential for abuse. It is the old story of technology rushing forward with some new wonder, before the men who supposedly control the machines have figured out how to prevent the machines from controlling them."

~ Newsweek Magazine [September 8, 1975]

Whatever the final outcome of the viability of this internet freedom regime in addressing today's challenges, it remains important that political communications and global media scholars recognize the importance of the digital infrastructures. The internet of 1995 can no longer simply be categorized as a critical infrastructure for countries, or an infrastructure of economic globalization for businesses–it is also importantly a digital scaffolding and a public information infrastructure for internet users and political activists alike around the world.

REFERENCES

Adler, Emanuel. 2008. “The spread of security communities: Communities of practice, self-restraint, and NATO’s post-cold war transformation.” *European Journal of International Relations* 14 (2) (June): 195–230.

Al-Kandari, Ali, and Mohammed Hasanen. 2012. “The impact of the Internet on political attitudes in Kuwait and Egypt.” *Telematics and Informatics* 29 (3) (August): 245–253.

Al-Saggaf, Yeslam. 2006. “The online public sphere in the Arab world: The war in Iraq on the Al Arablya website.” *Journal of Computer-Mediated Communication* 12 (1) (October): 311–334. doi:10.1111/j.1083-6101.2006.00327.x.

Barlow, John Perry. 1996. "A declaration of the independence of cyberspace" *http://homes. eff. org/~ barlow/Declaration-Final. html*

Bellin, Eva. 2004. “The robustness of authoritarianism in the Middle East - Exceptionalism in comparative perspective.” *Comparative Politics* 36 (2) (January): 139–157.

Bellin, Eva. 2012. “Reconsidering the robustness of authoritarianism in the Middle East: Lessons from the Arab Spring.” *Comparative Politics* 44 (2) (January): 127–149.

Bennett, W. Lance, and Alexandra Segerberg. 2013. *The logic of connective action: Digital media and the personalization of contentious politics*. Cambridge University Press.

Brown, John Seely, and Paul Duguid. 1991. “Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation.” *Organization Science* 2 (1) (February): 40–57.

Castells, Manuel. 2011. *The rise of the network society – The information age: Economy, society, and culture*. John Wiley & Sons.

Cobb, Paul, and Erna Yackel. 1996. “Constructivist, emergent, and sociocultural perspectives in the context of developmental research.” *Educational Psychologist* 31 (3-4): 175–190.

Cochran, Molly. 2002. “Deweyan pragmatism and post-positivist social science in IR.” *Millennium-Journal of International Studies* 31 (3): 525–548.

Crovitz, L. Gordon. 2012. “The U.N.’s Internet Power Grab.” *Wall Street Journal*, June 17, sec. Opinion. http://online.wsj.com/news/articles/SB1000142405270230382220457747053285921029.

Dalacoura, Katerina. 2012. “The 2011 uprisings in the Arab Middle East: Political change and geopolitical implications.” *International Affairs* 88 (1) (January): 63–79.

Deakin, Mark, Patrizia Lombardi, and Ian Cooper. 2011. “The IntelCities community of practice: The capacity-building, co-design, evaluation, and monitoring of e-government services.” *Journal of Urban Technology* 18 (2): 17–38.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance*. MIT Press.

Drake, William J.. 1988. “Wattc-88 - Restructuring the International Telecommunication Regulations.” *Telecommunications Policy* 12 (3) (September): 217–233.

Dutton, William H. 1995. “The ecology of games.” *Communication Theory* 5 (4): 379–392.

Ehteshami, Anoushiravan, and Steven Wright. 2007. “Political change in the Arab oil monarchies: From liberalization to enfranchisement.” *International Affairs* 83 (5): 913–932.

Ehteshami, Anoushiravan. 2003. “Reform from above: The politics of participation in the oil monarchies.” *International Affairs* 79 (1): 53–75.

Gause, F. Gregory III. 2011. “Why Middle East Studies Missed the Arab Spring: The Myth of Authoritarian Stability.” *Foreign Affairs* 90: 81.

Haas, Ernst B. 1980. “Why collaborate: Issue-linkage and international regimes.” *World Politics* 32 (3): 357–405.

Haggard, Stephan, and Beth A. Simmons. 1987. “Theories of international regimes.” *International Organization* 41 (3): 491–517.

Hallin, Daniel C., and Paolo Mancini. 2004. *Comparing media systems: Three models of media and politics*. Cambridge University Press.

Hansen, Derek, Ben Shneiderman, and Marc A. Smith. 2010. *Analyzing Social Media Networks with NodeXL: Insights from a Connected World*. Morgan Kaufmann.

Howard, Philip N. 2002. “Network ethnography and the hypermedia organization: New media, new organizations, new methods.” *New Media & Society* 4 (4): 550–574.

Howard, Philip N. 2010. *The digital origins of dictatorship and democracy: Information technology and political Islam*. Oxford University Press.

Howard, Philip N., and Muzammil M. Hussain. 2013. *Democracy’s fourth wave? Digital media and the Arab Spring*. Oxford University Press.

Howard, Philip N., Sheetal D. Agarwal, and Muzammil M. Hussain. 2011. “When do states disconnect their digital networks? Regime responses to the political uses of social media.” *The Communication Review* 14 (3): 216–232.

Hussain, Muzammil M., and Philip N. Howard. 2013. “What best explains successful protest cascades? ICTs and the fuzzy causes of the Arab Spring.” *International Studies Review* 15 (1): 48–66.

Jenkins, Henry. 2006. *Convergence culture: Where old and new media collide*. NYU Press.

Kamrava, Mehran. 1998. “Non-democratic states and political liberalisation in the Middle East: A structural analysis.” *Third World Quarterly* 19 (1): 63–85.

Khondker, Habibul Haque. 2011. “Role of the new media in the Arab Spring.” *Globalizations* 8 (5): 675–679.

Langohr, Vickie. 2004. “Too much civil society, too little politics: Egypt and liberalizing Arab regimes.” *Comparative Politics* 36 (2): 181-204.

Lave, Jean, and Etienne Wenger. 1991. *Situated learning: Legitimate peripheral participation*. Cambridge University Press.

London Agenda. 2011. “London Conference on cyberspace: Chair’s statement.” https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

Ludlow, Peter. 2001. *Crypto anarchy, cyberstates, and pirate utopias*. MIT Press.

MacKinnon, Rebecca. 2012. *Consent of the networked: The worldwide struggle for Internet freedom*. Basic Books.

Meyer, Katherine, Helen Rizzo, and Yousef Ali. 2007. “Changed political attitudes in the Middle East: The case of Kuwait.” *International Sociology* 22 (3): 289–324.

Moravcsik, Andrew. 2000. “The origins of human rights regimes: Democratic delegation in postwar Europe.” *International Organization* 54 (2): 217–252.

Mueller, Milton L. 2010. *Networks and states: The global politics of Internet governance*. MIT Press.

Neff, Gina. 2012. *Venture labor: Work and the burden of risk in innovative industries*. MIT Press.

Neumayer, Eric. 2005. “Do international human rights treaties improve respect for human rights?” *Journal of Conflict Resolution* 49 (6): 925–953.

Omoush, Khaled Saleh, Saad Ghaleb Yaseen, and Mohammad Atwah Alma'Aitah. 2012. "The impact of Arab cultural values on online social networking: The case of Facebook." *Comput. Hum. Behav.* 28 (6) (November): 2387–2399. doi:10.1016/j.chb.2012.07.010.

Pollock, John. 2011. "Streetbook: How Egyptian and Tunisian youth hacked the Arab Spring." *MIT Technology Review*, August 23. http://www.technologyreview.com/featuredstory/425137/streetbook/.

Posusney, Marsha Pripstein. 2002. "Multi-party elections in the Arab world: Institutional engineering and oppositional strategies." *Studies in Comparative International Development* 36 (4): 34–62..

———. 2004. "Enduring authoritarianism: Middle East lessons for comparative theory." *Comparative Politics* 36 (2) (January): 127–138.

Ragin, Charles C., and Howard Saul Becker. 1992. *What is a case? Exploring the foundations of social inquiry*. Cambridge University Press.

Roberts, Nancy C., and Paula J. King. 1991. "Policy entrepreneurs: Their activity structure and function in the policy process." *Journal of Public Administration Research and Theory* 1 (2): 147–175.

Ross, Michael L. 2008. "Oil, Islam, and women." *American Political Science Review* 102 (1): 107–123.

Saleh, Nivien. 2010. *Third World citizens and the Information Technology Revolution*. Palgrave Macmillan.

Servaes, Jan, and Nico Carpentier. 2006. *Towards a sustainable Information Society: Deconstructing WSIS*. Intellect Books.

Shirazi, Farid. 2012. “Information and communication technology and women empowerment in Iran.” *Telematics and Informatics* 29 (1): 45–55..

Stommel, Wyke, and Tom Koole. 2010. “The online support group as a community: A micro-analysis of the interaction with a new member.” *Discourse Studies* 12 (3): 357–378.

Tyler, Joshua R., Dennis M. Wilkinson, and Bernardo A. Huberman. 2005. “E-Mail as spectroscopy: Automated discovery of community structure within organizations.” *The Information Society* 21 (2): 143–153.

Wasko, M. M., and S. Faraj. 2000. “‘It is what one does’: Why people participate and help others in electronic communities of practice.” *Journal of Strategic Information Systems* 9 (2-3): 155–173.

Young, Oran R. 1989. “The politics of international regime formation: Managing natural resources and the environment.” *International Organization* 43 (3): 349–375.