Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk

Sarah Myers West, *Annenberg School for Communication and Journalism, University of Southern California*

Abstract

This paper seeks to provide insight into how digital activists navigate the risks posed to them in online environments. I examine how a group of activists across ten different non-Western countries adapt and respond to threats posed by two types of powerful actors: not just the state, but also the technology companies that run the social media platforms on which many activists rely to conduct their advocacy. Through a series of interviews, I examine how resistance against censorship and surveillance manifests through their everyday practices, not only by using encryption and circumvention technologies, but also by using commercial social media platforms to their advantage despite considerable ambivalence about the risks they pose.

1. Introduction

These are challenging times to be a digital activist. After being lifted by the promise of revolution, heralded by the Arab Spring, activists are facing a growing wave of risks both online and offline, as governments around the world respond to the invigoration of political resistance by instituting increasingly stringent controls over the information space (Deibert et al., 2010). A new wave of information controls has been instituted in authoritarian regimes and democratic nations alike: in China, free speech advocates once hopeful that the ascendance of Xi Jinping to the presidency would bring with it new democratic reforms found his plans to consolidate power included giving greater powers to government censors and creating a massive "public opinion monitoring" establishment to track the online activities of the public (Denyer, 2013). In the United Kingdom, Parliament passed a surveillance law, the Investigatory Powers Act, granting expansive powers to law enforcement for targeted interception and bulk collection of UK citizens' data (National Archives, 2016). Countries throughout Latin America and elsewhere purchased services from surveillance companies like Hacking Team, which offer the use of spyware to hack into and monitor the activities of journalists and human rights advocates (Perez De Acha, 2016). And in the United States, Edward Snowden revealed a massive state apparatus set up for the purpose of tracking the digital activities of citizens around the globe (Greenwald, 2013): from the National Security Agency to local police departments, surveillance of the online activities of activists is pervasive among US law enforcement and intelligence agencies (Joseph, 2015; Cagle, 2016; Fidler & Anderson, 2016).

Activism online can expose individuals to risks from a variety of sources: as the examples above show, states' use of censorship and surveillance is only growing over time, and is made easier and cheaper by the interventions of a commercial surveillance industry specializing in providing tools to monitor individuals that were previously only available to well-resourced nations (Deibert, 2013). Marczak and Paxson (2017) find that activists, NGOs, and civil society members in the Middle East and Horn of Africa are particularly vulnerable to government actors using social engineering techniques. At the same time, online harassment by people unaffiliated or indirectly linked to state officials has increased in its pitch (Mathias et al., 2015). This rise in trolling may lead not only to consequences for digital space by chilling speech, but increasingly serves as an indicator of threats to the physical self. These threats no doubt shape the tone and tenor of activism in ways that we are still making sense of, whether they lead them to increased caution in when and how they choose to speak, or, alternately, infuse activists' work with renewed purpose.

This paper seeks to provide insight into how digital activists navigate the risks posed to them in online environments. By focusing on how the interpretation of risk is infused into activist practices, I examined how activists adapt and respond to threats posed by two types of powerful actors: not just the state, but also the technology companies that run the social media platforms on which many activists rely to conduct their advocacy. Rather than examine these relationships from the perspective of the powerful – by focusing on how surveillance and censorship are conducted or how companies set their policies – I instead focused on the perspective of the user: how activists enact resistance through their everyday practices, using commercial social media platforms to their advantage despite considerable ambivalence about them.

Through ten interviews conducted with participants from Central Asia, Latin America, the Middle East, North Africa, South Asia and Sub-Saharan Africa, I found that the practices of social media companies do indeed present a new realm of risks for digital activists, even as they grant new opportunities – but social media users are responding in inventive ways to these threats. In this paper I trace through how those I interviewed make sense of and adapt to their threat environment.

To summarize my findings:

1. The interviewees actively engaged in threat modeling, constantly evaluating their risk environment and adapting practices accordingly. Among other things, this involved:
    a. Testing the boundaries of acceptable content
    b. Actively monitoring changes to corporate policies
    c. Selectively using channels to communicate depending on company policy and the political climate
2. Some expressed concerns about using anonymity and pseudonymity, particularly when adopted by users in their region without taking other steps to protect their digital security. For others, anonymity is essential to being able to engage in civic discourse.
3. Many appropriated the affordances of platforms to achieve their own ends. For example, one interviewee said that the limits to Facebook's language capabilities enabled people in their country to circumvent the real name policy.
4. In some cases, the interviewees pushed back on or expressed challenges adopting practices that are cited in the literature on digital activism. These included:
    a. The use of codes and subtext – several interviewees reported this practice, widely used in China, was a poor fit for their communicative environments.
    b. Encrypted messaging – though all of the interviewees were well versed in using encryption and encouraged their peers to do so, they reported sometimes being forced to adopt lowest common denominator tools to communicate with less technically savvy colleagues, and thus at times resorted to self-censorship.

1.1. Activism and the (Private) Public Sphere

The promise of different media technologies to democratize the speech of the everyday citizen has been a focus of communication scholars for decades (Gitelman, 2006). Particularly in its early days, the Internet was praised for its new democratic potential, allowing more individuals to speak freely and to be heard more widely than in the broadcast era (Rheingold, 2002), and offering new possibilities for acts of resistance (Jenkins & Shresthova, 2012, Negri, 1989, Shirky, 2008). Researchers generally concur that while they do not cause people to take the streets, networked technologies have indeed had a transformative effect on the means through which protests are carried out through the reappropriation of public space (Gerbaudo, 2012). Activists are able to reach broader publics, respond quickly and nimbly to environmental change, and take on distributed, networked forms (Castells, 2012, Bennett, 2003). Information technologies have thus become indispensable venues for the expression of dissent, dissemination of information and collective action (Youmans & York, 2012; Tufekci & Wilson, 2012).

At the same time, some scholars have questioned whether freedom or resistance are even possible in digital space, arguing that the circulation of communication within a commercialized online environment is ultimately depoliticizing (Dean, 2005) and lacks the strong ties necessary for building solidarity and affecting change (Gladwell, 2010). Still others see digital media even more nefariously, anticipating that its proliferation will only lead to greater authoritarianism (Morozov, 2012) or the reduction of freedom to capitalist control (Chun, 2008).

Though this debate has shed meaningful insight into changes in activist practices, it could be complemented by a growing body of literature that explores changes in the political economy of the Internet that have significant consequences for the use of information technologies by activists. While for much of its history the networked nature of the Internet has resisted any single gatekeeper for information, the experiences of users online have increasingly become concentrated on a limited number of platforms that are privately owned (Zittrain, 2009).

While it is challenging to find comprehensive data on their user numbers – such data quickly becomes out of date where it's available – some initial figures are telling. For example, Facebook reported 1.79 billion monthly users as of September 2016 (Facebook, 2016), out of an estimated 3.2 billion Internet users globally

(ITU, 2015). Roughly sixty-three percent of those users return to the site on a daily basis (Constine, 2014). As of June 2017, Google captured 91.88% of the global search engine market share, dwarfing bing's 2.88%, Yahoo's 2.18% and Baidu's 1.45% (StatCounter, 2017). The concentration of web traffic on these platforms thus gives the companies that run them what Karine Nahon and Jeff Hemsley (2013) call a network gatekeeping function: they can regulate the movement of information in ways that can deeply impact the effectiveness of activist work.

The network effects of this concentration have made these platforms an attractive place for online protest: according to content analysis of 1,180 coded cases of digital activism from 151 countries by researchers at the University of Washington, there is a heavy reliance by digital activists on platforms run by Silicon Valley companies. Forty-eight percent of digital activism campaigns in the sample used microblogs, 97% of whom used Twitter. Half used social networking platforms, 99% of which used Facebook. Thirty-eight percent used video, 78% of which used YouTube. The numbers suggest a tremendous concentration of digital protest movements on a limited number of platforms (Edwards, Howard & Joyce, 2013), and abandoning the massive populations using them is easier said than done if the goal of an activism campaign is to reach a large and diverse global audience (MacKinnon, 2011, 157).

Though these online spaces are often praised for their liberatory potential, they are fundamentally dissimilar in significant ways to the public spaces that constitute "real life' spaces for protest – in reality, they are not "spaces" at all, but platforms run on market logics (Gillespie, 2010). While the makers of these platforms do not act as gatekeepers in the traditional sense, they do govern discursive space in other critical ways: through the architecture of their platforms, the ways in which they negotiate with governments, set their terms of service and enforce their policies (Gillespie, 2017). Many of the companies that operate these platforms are headquartered within a collection of municipalities in Northern California, and yet they are used by billions of users worldwide to discuss and debate issues of political importance as well as for everyday social interaction. There is no "digital street" on which protests can take place (Sauter, 2014).

This makes it particularly important to understand the role these companies are playing in intermediating social and political life, even more so outside of the United States. Historically technology companies have tended to align themselves with US First Amendment doctrine (Ammori, 2014), in part because the idea that "information wants to be free" promulgated by technology activists since Stewart Brand is very much aligned with their expressed corporate values. For example, Google's mission to "organize the world's information and make it universally accessible and useful" serves as an organizing principle both for the company's culture and for its investments. This position is also, of course, in the company's best business interest – increasing its user base and the production of content only serves to create more data to be monetized.

Though on the issue of free expression the mission and corporate incentives of many social media companies and those of digital activists are very much aligned, in other areas their objectives can be quite divergent, and none more so than on the issues of privacy and surveillance. Though digital activists tend to see the principles of privacy and open access as compatible aims, companies may not see these objectives as similarly aligned (Polletta et al., 2013). An illustrative example may be observed in the response to Edward Snowden's revelations of mass surveillance, which outraged activists and companies alike, but for very different reasons: for many activists the revelations illuminated a massive surveillance apparatus misappropriating the name of national security to invade the private lives of citizens around the globe. For technology companies, however, the revelations were a betrayal by governmental stakeholders who were at best adversarial stakeholders and at worst business partners, and they inconveniently foregrounded the fact that their business models are premised on the collection of user data for the sake of targeted advertising. Many leading technology companies are structurally aligned with government authorities on the issue of data collection (though they argue against this in public), because they both need to surveil their users. In this respect the work by activists who promote the protection of privacy is in tension with the business models of most Internet companies.

Another illustrative example of how these tensions may come into conflict may be seen in the example of Twitter in Turkey. During the Gezi Park protests of 2014 Turkish Prime Minister Recep Tayyip Erdogan instituted a ban on Twitter, which ultimately served only to draw more users to the site. There was a surge of 138 percent in the number of tweets from Turkish users, resulting in the hashtag #TwitterisblockedinTurkey trending globally (Alobeid, 2014). Twitter also actively sought to aid Turkish citizens in circumventing the ban by introducing its "Speak to Tweet" SMS system enabling them to send messages directly via their phones.

Yet while on its face it appears that Twitter worked on the side of activists, Twitter's engagement in

Turkey was both political (facilitating free expression) as well as commercial (gaining users and site traffic). For the activists, Twitter became an important platform for the discussion of protests on the ground, and Twitter's active involvement helped to continue the flow of speech. But shortly after the ban was instituted, Twitter also sent representatives to meet with the prime minister's representatives, to the dismay of many activists in the region (Sepulveda, D., personal interview, 2015; Yeginsu & Arango, 2014). Political, commercial, and communicative goals were all tied up with each other over the course of the protests in complex ways.

The relationships between companies, governments and users introduce a significant change in the texture of the public sphere that is deserving of greater scrutiny: while 'public' in the sense of shaping civic discourse, the rules by which most of these platforms are governed are set by private companies and shaped by commercial imperatives. Much of the research into this subject has focused on the policymaking functions of technology companies and their orientation toward the public (York, 2010, MacKinnon, 2012, Gillespie, 2017). But less is known about how the policy decisions and design of social media platforms shapes how users perceive the role of social media, or how they make sense of the politics of platforms by enacting resistance.

Like Milan (2015), I take this social, micro-level interaction as a generative starting point for understanding activist practice. By grounding my study in user practices, I hope to bring to the forefront the ways in which commercial imperatives may be shaping digital activism – leaving open the possibility that while problematic, these are not necessarily mutually exclusive terms. As Antonio Negri (1989) argues, while the spread of technology maintains the overwhelming domination of global capitalism, it also makes subversion increasingly possible. Thus, to recognize how digital protest occurs on and may be shaped by commercial platforms is not to deny protest itself, but to recognize that the foundations underlying activism have become marked by a tension between political and commercial imperatives.

2. Methods

This project seeks to contribute both practically and theoretically to a better understanding of the work of digital human rights advocates. By focusing in on the digital activism community, I engaged with individuals who have been frequently targeted by regimes of information control. Additionally, the project seeks to augment existing research by adding a more globally representative and activist-focused perspective to a discussion that has largely focused on the companies as the primary actors.

I conducted semi-structured interviews with ten digital activists, purposefully interpreting this term quite broadly. I worked with Global Voices Advocacy (Advox), a citizen journalism platform dedicated to the promotion of free expression worldwide, as the primary conduit for conducting these interviews. Advox is unique within the digital activism community: many other digital rights organizations either do international work from headquarters in the United States or operate on a national level. By contrast, Advox is made up of a wide and distributed network of members in 120 countries around the world.

I have been working with Advox since 2011. In my work with the group, I have gotten to know a number of digital rights activists within the network online and in person: I attended the 10th annual Global Voices Summit in January 2015 in Cebu, Philippines, and collected participant observation data during the meeting that informed the scope of this project. Although I straddle the lines of being both a member of the community and a researcher, in the context of this project I have identified myself as the latter. Moreover, there is precedent within the community of PhD researchers conducting ethnographic work within Global Voices (see Tsui, 2010).

With the guidance of the director of Global Voices Advocacy, I spoke with ten Advox authors, selected from the broader pool of possible participants within Advox on the following criteria:

1. First, I limited the list of participants to those who have already published on these issues. This ensured that nobody was included who did not already have a public profile, and thus would be less likely to face additional risks by participating in the research.
2. Second, I selected participants who represented as diverse a group possible in terms of their geography.
3. From this list, several possible participants were removed because of tensions in the current political situation in their country.

This approach yielded a list of sixteen possible participants, of which ten consented to participate. The small size of this sample means my findings are not going to be representative of any larger population, however my aim is not to make generalizable claims about the activism community as a whole but rather to provide nuanced and grounded examples derived from the indi-

vidual experiences of particular activists. Those I interviewed hailed from a number of different parts of the world: Central Asia, Latin America, the Middle East, North Africa, South Asia and Sub-Saharan Africa. I identify them in this paper by region in an effort to obscure their identities.

Though some of them may self-identify as activists, others may not, preferring the term journalist or blogger instead. As such, I describe them throughout the paper as interviewees, so as not to attribute an identity category they may not choose to adopt themselves. I use numbers as an indicator of which interviewee I am quoting throughout the paper, to make it easier to identify them consistently without revealing their identities.

Interviewees were asked a series of questions focusing on their digital practices, as well as their views on digital platforms and privacy and free expression concerns (outlined in Appendix A). I conducted the interviews in a semi-structured format, using the questions as an open-ended guideline while adapting the course of the interview to explore themes presented by the participants.

Given the sensitivity of these issues, it was particularly important that I conduct the interviews in a secure manner, doing my best to ensure the interviewees' privacy was protected. As none of the participants are based in the US, the interviews were conducted using video or audio chat platforms. Encrypted communications were deployed wherever possible throughout the process of communicating with participants, and I took handwritten notes to ensure protection of respondent data. Any information regarding participation in the study was stored on an encrypted hard drive and will be deleted within five years of its collection. Though I received an exemption from my institution's Institutional Review Board, interviewees were provided a consent form detailing risks and benefits of participating in the study prior to granting their assent to an interview.

I analyzed the notes from the interviews using thematic content analysis, looking for emergent themes among the participants and to assess the issues they are most concerned with. In analyzing the questions that focus on practices, I found two theoretical frameworks particularly helpful.

First, I drew on Erving Goffman's *The Presentation of Self in Everyday Life* to make sense of two elements: how their presentation of self is tied to the navigation of risk, and to what extent it is shaped by the affordances and constraints of platforms. To contextualize these findings, I examined similarities and differences in their reported use of digital platforms, the extent to which they expressed concern about privacy and free expression issues, and the means they use to protect their privacy and guard against censorship.

Second, my research was informed by James C. Scott's (1990) analysis of power and resistance from below, what he describes as the infrapolitics of the powerless. Many studies approach research of surveillance and censorship with a focus on how information controls are a form of domination by the powerful. However, my experiences with Global Voices Advocacy suggested otherwise: the activities of the bloggers, journalists and advocates that make up the Global Voices community reflect a wide variety of approaches to enacting critiques of power despite the risk of doing so. Though they take forms different to the rumors, gossip, and folktales described by Scott, hidden transcripts, the term Scott uses to describe critiques made in the face of the powerful, are everywhere in the contemporary digital environment. Through memes, jokes, first-hand accounts, livestreaming and citizen media, netizens are continually inventive in finding new ways to speak truth to power.

In drawing on Scott, it's important to make clear that I am not making any insinuations about what kind of position the interviewees hold within their society. Instead, I draw on their accounts as representative of the ways in which all of us as users of social media platforms may find spaces for agency, regardless of how much or how little power we may hold as individuals, consumers or citizens. In this sense, Scott's intervention is a radical one: many studies of censorship and surveillance all too often operate from the position of the surveillor, rather than the surveilled. Taking Scott's cue, my approach in this project is to study the "contradictions, tensions, and immanent possibilities" that underlie the contemporary digital environment: how we might learn from the experiences and responses of these individuals as representatives of a wider range of cultural and political orientations.

This is a tall order for a relatively short paper, and I'm unlikely to achieve it. However, I aim to make at least a first foray into this effort by examining the practices of individuals who are well-versed in and thoughtful about navigating power relations and risks online.

3. The Transcript: The importance of social media to activism

All of those I interviewed placed social media and messaging platforms at the center of their communication practices, whether to socialize with their peers,

build advocacy networks, report on news from their region or simply as a means of self-expression. They tended not to concentrate their communications on a single platform, instead using a variety of platforms for different purposes: Facebook and Twitter were the only two used by all the interviewees, but other frequently used platforms included WhatsApp, Signal, Skype, and Telegram. The 'transcript' of their communications thus stretches across multiple platforms: looking at a single platform in isolation would give only limited insight into their practices. In keeping with this insight, throughout the findings I take a view of online communications that foregrounds social practices over the distinctions between particular platforms.

3.1 Perceptions of Digital Risk

Many of the interviewees spent a lot of time and energy making sense of the risk in their digital environments, building threat models, and calibrating their activities in response to them. These assessments of risk were highly nuanced, shaped by years of following the internal politics of their country, reports in the news, and monitoring the activities of other activists. Because of the public nature of social media platforms, they anticipated communications on these platforms were particularly likely to be monitored – although often they said that one or two sites (in most cases this included Facebook) received greater scrutiny by government officials while others may be more under the radar.

Several of the interviewees said they frequently tested the boundaries of acceptable communication as a means of assessing their risk, observing reactions to material they published and calibrating their public profile accordingly. One interviewee described the process of building an advocacy network:

> I wrote a critical article, no reactions, then started doing more to change tone, do interviews, then [my activist group] and Global Voices. I created the networks and people added their resources. Now we have a global network, and people now know what's going on in [my country] and why things are the way they are. 10

Another interviewee said that they had to continually monitor changes in the political environment, and remain cognizant of the likelihood of future changes to their level of risk. "They just keep moving the goal post," he said. "You have to keep assessing it according to the time you're in. You can say this is a subject that would be better left to another time…That doesn't mean you're totally safe, you might be targeted down the line." 2 Another interviewee describing similar dynamics added that this led to an increased level of self-censorship in their country. 5

Though different from region to region, several of the interviewees suggested that social media platforms were a tool of the government as much as they were a tool for advocacy: government agencies would monitor discussions on various social media platforms to identify opponents, and would at times use their own accounts in order to issue threats, something the interviewees were very much aware of as they used social media tools. 6 One practice in particular that was used in several regions was keyword monitoring, where government officials or other adversaries would run searches on social media platforms for keywords or hashtags and use them to attack opponents. In doing so, state actors repurposed affordances designed for community-building in order to harass and threaten users. Moreover, the interviewees said that the tools offered to them by companies in order to avoid harassment, such as reporting inflammatory posts or user accounts, were a poor recourse: as soon as an account was reported, another would crop up in its place, one interviewee said. 8 Despite this, they developed a number of inventive mechanisms for evading and combatting threats, which I discuss in more detail below.

In many instances, the concept of "the state" as an entity itself had blurred boundaries when translated to a digital environment – interviewees from several countries reported government supporters, guerillas, or trolls to be as likely to pose a threat as state officials. An interviewee from sub-Saharan Africa noted that members of their government had recently begun to use Twitter to harass opponents. They reported that trolling behavior by officials from their government was fairly unsophisticated; they used all capital letters and outdated language, and were easy to bait into arguments. 10 Still, though in their country civilians demonstrated greater sophistication in their use of social media, it was the state that remained the greater threat: "Society may make threats, but won't put you in jail", the interviewee said. They "just want you to stop. But government is the one that backs it up". 10

In another instance, an interviewee from the Middle East/North Africa (MENA) region suggested that former members of government could remain a threat even when out of office: "In context, lots of [our] political leaders were warlords several years ago – so exposing corruption can annoy their friends, which can mean being hurt or sued". 7 Yet another interviewee from South Asia said that at times in their country vigilantism by members of society could pose a greater

threat than state officials, perhaps because they are not bound by the law. In particular, they said that religious extremists would issue death threats and often carried them out, though this had calmed somewhat since the former majority party had left power. 8

The descriptions by the interviewees suggested that online and offline threats were often threaded together, and that perhaps the distinction between online/offline environments is losing its meaning. Threats in digital life could easily transform into physical harm, even serving as a barometer for the likelihood of a future arrest or the prospect of violence. But even when limited to digital space, the threats had real life consequences for the mental and emotional health of the interviewees that manifested in changes to their behavior.

3.2 Assessing Company Policies

In keeping with the centrality of social media platforms to their communications, the relationships of major technology companies to governments around the world were the subject of particular scrutiny among those I interviewed. Monitoring where a company opens its offices was one tactic the interviewees used in order to make assessments about the likelihood they would work with the government. 8 One interviewee from the MENA region said that they also checked for their country's presence in the transparency reports published quarterly by many social media companies as an indicator of what might be going on behind the scenes. "We do know for sure the government is cooperating with social media. The ICT minister said several times the solution is not filtering the content, it's cooperating with the companies," they said. At the same time, they were sharply critical of the information provided in the transparency reports: "providing numbers is not enough. When it comes to content removal they block content based on local laws. It's kind of ridiculous because the laws are the problem, they violate the standards for international free expression". 8

Another interviewee emphasized the companies' economic interests as an actual benefit for them: because their country was a low priority for technology companies, and they anticipated it would be less likely for the company to comply with government demands – though they said this was something they nevertheless monitored. 7 An interviewee in a high-priority country (which had been in the news at the time of the interview for a block instituted on social media platforms) said that because they knew the technology companies were at odds with their government, they felt more comfortable using social media platforms despite remaining qualms with the companies' collection of their data. 4

Finally, some interviewees suggested that they anticipated that companies would have to comply with the government at some point, but that they believed they would do their best to operate in their users' best interest. "I think it's a trade off because they face limitations, just like us, a conflict of interest to operate in these countries to not doing anything at all," one said in an interview. "They will have to cooperate at one point, they would have to play ball… They'll try to keep operating to the maximum number of users but will have to make compromises." 2

3.3 Channel Selection

The perceptions of a company's compliance with government data requests played in to how the interviewees made choices about what to say and where. A basic practice adopted by many of them was being very selective in the choice of different channels for different kinds of communication. One said that they used Facebook primarily to communicate with an international audience, while they used Twitter to communicate with peers in their country. 6 Another reported finding a regional WhatsApp group to be an effective tool for networking, though they were conscious that the conversation was not encrypted, opting to take sensitive discussions offline or communicate one on one using an encrypted channel. 9[1]

Having an implicit awareness of the sensitivity of discussing political issues online was a crucial part of the interviewees' media practice. 9 "Even though I'm a digital activist I'm trying to keep my digital shadow as little as possible," said one interviewee. "I am really standing on a thin line right now. If I take one step further I could really get in trouble, but I'm ok for now." 4 Another said that while they were actively involved in discussions online, they opted not to make appearances in non-digital platforms, like television, which could raise their profile among government actors. 1

Several of those I interviewed were circumspect about the role of social media, saying the platforms made them feel like they could not be in control of their own data, but that they had to use social media in order to communicate with the public in their country. "You can't be a successful social network without spying on users," said one interviewee, 1 while another cautioned "Take it as free, but don't submit yourself to one or another and use it sparingly but effectively". 8 In

[1] WhatsApp has since rolled out end-to-end encryption; this was not in place at the time the interview was conducted.

particular, challenges navigating the privacy settings of social media platforms, particularly when translated into languages other than English, was cited as a point of frustration. One interviewee expressed frustration that Twitter did not translate its terms of service into their language, despite offers their group had made to translate them for the company on a volunteer basis. Another said "I don't think they are interested in allowing us to be in control," said one interviewee of Facebook's privacy settings. 3

Managing the visibility of their advocacy was also cited as a challenge by this interviewee. "It fosters a fake sense of community," they said of posting on Twitter:

> I say that because I sometimes realize there are a lot of people following me who I don't know and I don't like. I posted a complaint yesterday and it got 300 retweets. I started to get all these replies from people who have no comprehension, and I wanted to crawl up in a hole and die. It's not private and not the world, but it's a sense of community, but it's not a closed community. 3

4. The Presentation of Self in Digital Life: Evading Online Threats

The interviewees interwove their ever-evolving interpretation of threat in their environment into their online activities. In a sense, their practices are reflective of a Goffman-esque presentation of self in digital life: a performance of their identity that reflects the deep complexity of the encoding of their digital environment, and is imbued with technical, political, structural and cultural influences (Goffman, 1956). Their interactions are guided in visible and invisible ways by the design and affordances of the platform on which they occur.

4.1 Anonymity and pseudonymity

A number of the interviewees were circumspect about the role of anonymity, while others saw it as critical. One interviewee from sub-Saharan Africa said that:

> From my experience more than half of social media accounts in [their country] are anonymous, and it contributes to the civility of the discussion. The [country] online community is anonymous, they communicate through anonymity. It's a kind of protection for people here. 10

Another interviewee said though they did not communicate anonymously for the most part, names themselves could be a kind of mechanism for hiding. This person remained largely invisible because they had a common name in their country and thus couldn't easily be Googled or otherwise identified among the many others with a similar name – something that helped them feel more free to communicate while staying off the radar of the political opposition. 6

For these interviewees, the ability to communicate anonymously was liberating, and an essential part of the continuation of civil discourse in an environment in which speaking out would likely lead to violence or arrest. "It's a kind of translation of the offline situation" one interviewee suggested. "People don't raise their voices when they talk politics, and they have to glance over their shoulder. There's a lot of fear and a lot of silence. This is translated into anonymity online." 10

On the other hand, anonymity was seen as troubling for others. One interviewee from Latin America observed that many Twitter users in their country adopted pseudonyms to discuss politics online, but failed to take other measures to mask their identity. This resulted in several cases in their identification by the state, leading to arrests. "Feeling you are safe when you are not, that's the most dangerous thing," they said. "You don't use a VPN, don't protect your machine. Just using a fake identity, it's not safe." 3 This suggests that the adoption of anonymity and pseudonymity in online environments is not entirely akin to the wearing of a mask: the hiding of one's identity online does not mean the erasure of the body it is tied to.

4.2 Playing with affordances: Facebook's real name policy

The adoption of a real name policy by Facebook, which ties a users' online profile to a name that can be verified by some form of identification, was regarded as a real hindrance for anonymity online by several of the interviewees. Though Facebook adopted the policy with the objective of encouraging civil discourse, the policy has negative downstream effects for activists by either leading to increased risk of surveillance and harassment or the likelihood of self-censorship. The example of the real name policy is an illustration of how the architecture and enforcement of platforms can have an exaggerated effect on the nature of social interaction: they contain affordances that ena-

ble or disallow certain kinds of behavior with clear downstream effects on discourse.

The interviewees did suggest there were creative ways of evading these controls: one noted that the enforcement of the policy was not as stringent in languages Facebook's content moderation team does not cover, citing the example of a friend who had submitted a cartoon in their language as a form of identification and had it accepted. 8 Their accounts suggested visibility was a double-edged sword, even more so when compounded by the complexities of evolving technologies and corporate policies. While appropriating the affordances of platforms (as in the case of the real name policy) in order to achieve their goals, they sought to say just enough to make their critiques public while evading the threats posed by government officials or trolls.

4.3 Codes and Subtext

Another approach adopted by some activists has been to use codes and subtext to speak only to those who understand how to decode their messages. I asked several of the interviewees about the use of coded language, such as the oft-cited example of the "Grass Mud Horse" mythology developed by Chinese netizens to evade government censors.[2]

Only a few of those I interviewed reported using similar practices to communicate over social media. More often, the interviewees reported such practices being either difficult to adopt in their countries or at odds with their advocacy work. Another described such a practice as self-censorship, saying "It doesn't really work when you're trying to advocate something. You have to use clear language to communicate to the majority of people." 2

Another interviewee said "It's hard, because language is a common thing, people may not know what you're talking about, and if they do then everyone knows." 3 As an example, the interviewee said netizens in their Latin American country sometimes used synonyms to avoid keyword monitoring by government-inspired trolls. During an economic crisis, netizens used the term "green" in place of the country's currency when tweeting about the country's economic struggles. Though the term was easily decoded by networks of readers and thus allowed conversations to continue behind the trolls' backs for a time, this proved only a temporary solution to avoiding keyword monitoring.

4.4 Going backstage: encrypted messaging

A final approach adopted by the interviewees is to make their discussions, particularly one-on-one conversations, completely inscrutable by surveillors by using encryption tools. In some cases, the interviewees were adamant about the imperative to use encryption – refusing to communicate with journalists unless they used PGP, 3 or expressing the need for more people to use encryption as a form of herd immunity to make everyone more secure. 7 Encryption seems to form a core element in what Goffman might call the backstage – a space for one-to-one communication not privy to the eyes of the public. Though most of the interviewees made some reference to a form of backchannel conversation, some expressed concerns about the security of these channels. They played an internal advocacy role within their communities in trying to encourage others to adopt safer, more secure modes of backstage conversation – using encrypted messaging tools rather than private messaging functions on social media platforms that could be easily intercepted by adversaries. However, in some cases a lack of technical savvy among their peers led to the adoption of the lowest common denominator among available technologies.

In other cases, they emphasized a need for visibility and transparency that worked against the use of encrypted messaging tools: in the words of one person:

> Privacy really means different things for different people. For us now in the [country] context, it's really a matter of breaking the fear… In our context right now, the more transparent you are the better you will be. That's how I define privacy. 7

For this interviewee, it seemed imperative that the hidden transcript be made more visible – that the end goal be to transform the information environment into one in which political speech is made safer by everyone's involvement in it. This reinforces the tension inherent in reconciling the imperative for privacy

[2] The "Grass Mud Horse" (caonima in Chinese, which sounds roughly like "fuck your mother") is a mythical species of alpaca invented by netizens to criticize the government. In its inventive mythology, the animal combats the incursions of "river crabs" (hexie, a homonym for the ideology of "harmonious society" deployed by Hu Jintao in connection with the intensification of online censorship) into its native grasslands (Wang, 2012). Users and censors thus engage in a dance, continually developing new terms to evade the censorship regime as the authorities dynamically shift their bans to fit the present moment.

through encryption technologies with the desire to reach broad audiences through social media platforms.

5. Ambivalence in the (Private) Public Sphere

Ultimately, the accounts of those I interviewed suggested a deep ambivalence about the role of social media platforms as intermediaries for activism: on the one hand, several of the interviewees indicated the benefits of using social media far outweighed the harms. "I think we're underestimating the impact that social media has made," one interviewee from the MENA region said:

> I think it's much like when Gutenberg invented the printing machine. Before, having a voice meant having access to the means of creating media, which meant is was monopolized by elites. But it's slowly changing – someone like me could create a media network and have 200,000 followers. It's a tool of social change. People can create the change they want if they didn't have the chance in other manners. 2

Another person I interviewed from a Central Asian nation attributed the growing political consciousness of people in their country to the increased use of social media, arguing it served as an alternative news outlet in a country where all other media are state-run. 5

Others shared deep misgivings about the use of social media platforms. "It's not like Zuckerberg created Facebook for free expression. They did it to make money," 8 one interviewee said, while another joked "Being censored in [my country] makes you famous, so it might be a good thing for me". 4

Collectively, these interviews reflected a desire to balance the need for visibility with its consequences for user privacy. The practices adopted by the interviewees are designed to achieve greater individual control over their visibility as they navigate a complicated and ever shifting environment of digital risks: from being selective about which channels to communicate on and what to say on them, to adopting anonymity and using encryption, to using coded language to communicate in the face of adversaries, activists and everyday users are continually calibrating their presentation of self in order to evade threats.

Like states, social media companies have an asymmetrical influence over the shape of online discourse. Not only do they exert control over their policies and the features of the site, they also hold the benefit of being able to aggregate, monitor users' information, and control what information they are exposed to. Both companies and the state generate considerable threats to those I interviewed. The practices outlined above are an adaptation to these risks in order to maximize the benefits of social media for activism.

In the words of one person I interviewed:

> We don't have any option. Trusting a private company is the only option we had. We trust Google, Facebook, Twitter more than the…government. We know they are a legal threat, they give information to the government. But we don't have any option other than to shut up. The neoliberal capitalism has brought an opportunity for us. 10

6. Conclusion

This study reinforces the centrality of social media platforms to digital activism, but adds a new dimension to understanding their function by examining them through activists' perspective. By grounding the analysis in everyday practices, the interviews highlighted a discomfort on the part of users with the role social media companies play as intermediaries for activism: at any moment, the government could petition the company for their data, or use their posts as evidence to arrest them. But they pragmatically recognize the commercial imperatives of companies, accounting for the times at which these imperatives work in their favor and guarding against the times at which they could place them at risk by attending to the information available to them. Despite the critiques of some technoskeptics, these accounts suggest that resistance is indeed possible on commercial social media platforms, but is not without risk. Instead, the interviews foregrounded how corporate imperatives influence practices that are continually shaped and reshaped by activists as they navigate everyday life: practices that I suspect may be common to many users, though unique in their instantiations and shaped by the political, social and cultural dynamics of the user's community.

This study aimed to survey the landscape of how activists make sense of the nature of commercialized social media spaces, but is only an initial foray into a topic deserving of much greater scrutiny. A few possible threads to be further untangled include: discerning these dynamics more systematically with a larger pool of participants, tracing out the regional distinctions between activist social media practices, and examining how the exposure to risk may change in relation to shifts in the regulatory environment, particularly as governments around the world enact cybercrime and terrorism laws that enable them to punish activists for speaking out on social media. There is much work to be done in order to make sense of these issues from the perspectives not just of the platform creators, but those speaking on them.

References

Alobeid, D. (2014, Mar. 25). Turkey is all a-Twitter: The Politics of Social Media. *Brandwatch.* Retrieved from http://www.brandwatch.com/2014/03/turkey-is-all-a-twitter/

Ammori, M. (2014) The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter. *Harvard Law Review*. 127(8)

Cagle, M. (2016). Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color. *ACLU.* Retrieved from https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target

Castells, M. (2012). *Networks of Outrage and Hope: Social Movements in the Digital Age.* Polity Books: Cambridge.

Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso Books: London.

Constine, J. (2014, Jul. 23). Facebook Beats in Q2 with $2.91 Billion in Revenue, 62% of Ad Revenue from 1.32B Users. *TechCrunch.* Retrieved from http://techcrunch.com/2014/07/23/facebook-q2-2014-earnings/.

Chun, W. (2008). *Control and Freedom: Power and Paranoia in the Age of Fiber Optics.* MIT Press: Cambridge.

Dean, J. (2005). Communicative Capitalism: Circulation and the Foreclosure of Politics. *Cultural Politics. 1*(1): 51-74.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge: MIT Press.

Deibert, R. (2013). *Black Code: Inside the Battle for Cyberspace.* New York: Signal.

Denyer, S. (2013, Aug. 2). In China, Communist Party takes unprecedented step: It is listening. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/in-china-government-mines-public-opinion/2013/08/02/33358026-f2b5-11e2-ae43-b31dc363c3bf_story.html

Diaz, M. (2013, Apr. 25). Will the Revolution Still be Tweeted? Venezuela's Netizens Face Uncertain Future. *Global Voices Advocacy.* Retrieved from https://advocacy.globalvoicesonline.org/2013/04/25/will-the-revolution-still-be-tweeted-venezuelas-netizens-face-uncertain-future/

Edwards, F., Howard, P. N. and Joyce, M. (2013, Nov.) Digital Activism & Non-Violent Conflict. *Digital Activism Research Project*, University of Washington: Seattle.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K. and Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in the news feed. *Proceedings of the 33rd Annual SIGCHI Conference on Human Factors in Computing Systems, Association for Computing Machinery (ACM).*

Filder, M. and Anderson. C. (2016). Investigating Surveillance Around Standing Rock. *Just Security.* Retrieved from https://www.justsecurity.org/34449/investigating-surveillance-standing-rock/

Freedom House. (2013). *Freedom of the Press: China.* Retrieved from https://freedomhouse.org/report/freedom-press/2013/china

Gerbaudo, P. (2012). *Tweets and the Streets: Social Media and Contemporary Activism.* London: Pluto Press.

Gidda, M. (2013, Aug. 21). Edward Snowden and the NSA files – a Timeline. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline

Gitelman, L. (2006). *Always Already New: Media, History and the Data of Culture*. Cambridge: MIT Press.

Gladwell, M. (2010, Oct. 4). Small Change. *The New Yorker.*

Goffman,E. (1959). *The Presentation of Self in Everyday Life.* Anchor Books: New York.

Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience.* Northeastern University Press: Boston.

Green, S. (1999). A Plague on the Panopticon: Surveillance and power in the global information economy. *Information Communication & Society, 2*(1): 26-44.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

International Telecommunications Union. (2014, May 5). ITU releases 2014 ICT figures. Retrieved from http://www.itu.int/net/pressoffice/press_releases/2014/23.aspx

Jenkins, H. and Shresthova, S. (2012). Up, up and away! The power and potential of fan activism. *Transformative Works and Cultures,* 10.

Joseph, G. (2015). Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson. *The Intercept.* Retrieved from https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/

Lam, O. (2014, Aug. 25). Leaked Documents Reveal How the Chinese Communist Party Channels Public Opinion. *Global Voices Advocacy,* https://advocacy.globalvoicesonline.org/2014/08/25/leaked-documents-reveal-how-the-chinese-communist-party-channels-public-opinion/

MacKinnon, R. (2011). *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* Basic Books: New York.

Marczak, W.R. and Paxson, V. (2017). Social Engineering Attacks on Government Opponents: Target Perspectives. *Proceedings on Privacy Enhancing Technologies* (2): 172-185.

Mathias, J.N., Johnson, A., Boesel, W.E., Keegan, B., Freedman, J. and DeTar, C. (2015). Reporting, reviewing, and responding to harassment on Twitter. *Women, Action, and the Media.* Retrieved from http://www.womenactionmedia.org/twitter-report/.

Milan, S. (2015). Mobilizing in Times of Social Media. From a Politics of Identity to a Politics of Visibility, in Dencik & Leistert, (Eds.), *Critical Perspectives on Social Media and Protest* (pp. 53-71). Lanham: Rowman & Littlefield.

Morozov, E. (2012). *The Net Delusion.* PublicAffairs: New York.

Nahon, K. and Hemsley, J. (2013). Going Viral. Cambridge: Polity Press.

National Archives. (2016). Investigatory Powers Act 2016. *Legislation.gov.uk.* Retrieved from http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

Negri, A. (1989). *The politics of subversion: A manifesto for the twenty-first century.* Blackwell: Oxford.

Perez de Acha, G. (2016). Informe: Hacking Team Malware Para La Vigilancia en America Latina. *Derechos Digitales.* Retrieved from https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

[English language summary at: Perez de Acha, G. (2016). The Rise of Surveillance Software in Latin America. *Derechos Digitales.* Retrieved from https://www.derechosdigitales.org/9884/the-rise-of-surveillance-software-in-latin-america/].

Polletta, F., Chen, P.C.B., Gardner, B.G., Motes, A. (2013). Is the Internet Creating New Reasons to Protest? in van Stekelenburg, J., Roggeband, C. and Klandermans, B., Eds. *The Future of Social Movement Research.* University of Minnesota Press: Minneapolis.

Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier.* Available online at http://www.rheingold.com/vc/book/

Sauter, M. (2014). *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet.* Bloomsbury Academic: New York.

Scott, J. C. (1990). *Domination and the Arts of Resistance: Hidden Transcripts.* Yale University Press: New Haven.

Sepulveda, D. (2015, Mar. 9). Phone interview.

Shirky, C. (2008) *Here Comes Everybody: The Power of Organizing Without Organizations.* Penguin Press: New York.

StatCounter. (2017). Search Engine Market Share Worldwide. *StatCounter.* Retrieved from http://gs.statcounter.com/search-engine-market-share.

Tor Project. (2015). Who uses Tor? Retrieved from https://www.torproject.org/about/torusers.html.en.

Tsui, L. (2010). A journalism of hospitality. (Unpublished doctoral dissertation. University of Pennsylvania, Philadelphia.

Tufekci, Z. and Wilson, C. (2012). Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square. *Journal of Communication.* 62(2): 363-379.

Tufekci, Z. (2014). Is the Internet Good or Bad? Yes. *Medium*, Retrieved from https://medium.com/matter/is-the-internet-good-or-bad-yes-76d9913c6011

Vaidyanathan, S. (2011). *The Googlization of Everything (And Why You Should Worry)*. University of California Press.

Wang, S. S. (2012). China's Internet lexicon: The symbolic meaning and commoditization of *Grass Mud Horse* in the harmonious society. *First Monday,* 17(1).

Yeginsu, C. and Arango, T. (2014). Turkey Greets Twitter Delegation With List of Demands. *New York Times.* Retrieved from https://www.nytimes.com/2014/04/17/world/europe/a-list-of-demands-greets-twitter-delegation-in-turkey.html.

Youmans, W. L. and York, J. C. (2012). Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social Movements. *Journal of Communication*, *62*(2).

Zittrain, J. (2009). *The Future of the Internet (and How to Stop It)*. Yale University Press: New Haven.