Information Technology, Private Actors, and the Responsibility to Protect.

Kirsten Martin, Ph.D.
George Washington University

Forthcoming in *Responsibility to Protect and Private Actors* (Cambridge Univ. Press)

> The Internet is no longer just an essential channel for commerce, entertainment and information. It has also become a stage for state control — and rebellion against it.[1]

The UN's Responsibility to Protect (R2P) focuses attention on the responsibilities of the global community to intervene and prevent human rights violations. Introduced in 2001and gaining in popularity, the *Responsibility to Protect*, suggests two sets of responsibilities: "(1) the responsibility of a state to protect its citizens from atrocities, and (2) the responsibility of the international community to prevent and react to massive human rights violations."[2]

While the focus of R2P has rightfully been on sovereign states both to protect their citizens and to prevent and react to human rights violations in other states, the role of private actors has been under examined. Obvious examples are where communities hold firms responsible for providing weapons to brutal regimes or ignoring the plight of the vulnerable in local communities. More generally, firms, as private actors within the international community, create responsibilities within R2P based on the consequences of their actions and their roles within the local communities: firms may engage in communities in conflict where human rights abuses occur and voluntarily take on a role as a member of the local community.

This chapter seeks to better understand how private actors can contribute to the prevention, cessation, and aftermath of R2P events such as the violation of human rights. Specifically, I focus on firms in the information and communication technology industry (ICT) such as telecommunication and Internet communication technology who provide products and services normally provided by state actors and that impact the ability of human rights abuses to occur.

The goal of this paper is to develop a framework for the ethical analysis of global information technologies with an understanding of firms' obligations within R2P. The introduction of Internet and telecommunication technologies to countries with authoritarian governments has facilitated the imprisonment of dissidents and the surveillance of citizens while also empowering users and protestors facing human rights violations. When established information technologies are introduced to new communities, such as when Google introduced their search technology to China or when Twitter was introduced to Iran, new patterns of use prove difficult to analyze.

---

[1] Markoff, John. "Iranians and Others Outwit Net Censors." *The New York Times*, Apirl 30, 2009. http://www.nytimes.com/2009/05/01/technology/01filter.html?fta=y

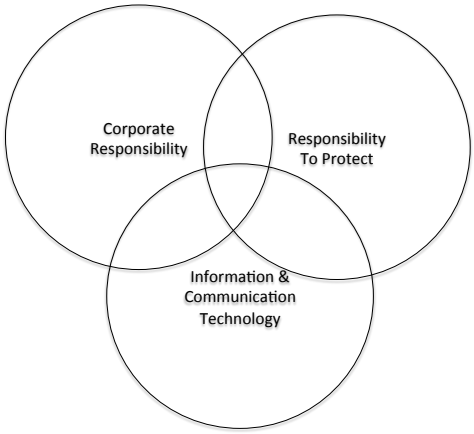
[2] Payandeh, M. (2010). With Great Power Comes Great Responsibility-The Concept of the Responsibility to Protect within the Process of International Lawmaking. Yale J. Int'l L., 35, 469. http://www.yjil.org/docs/pub/35-2-payandeh-great-responsibility.pdf

This chapter proceeds as follows. First, I explore the intersection of corporate responsibility, R2P, and ICT. Second, I develop the framework for the ethical analysis of ICT generally and use examples of Google in Chine and Safaricom throughout. Third, I illustrate the utility of the framework with the case of social networks and the Arab Spring of 2009.

Corporate Responsibility to Protect through ICT

Increasingly, information and communication technology firms find themselves as a ***tool for freedom and human flourishing as well as a possible tool for government atrocities.*** Social networking site WeChat was used to organize strikes against Taiwanese company who failed to pay into retirement fund while the Chinese government also monitors and deletes poses on social news/politics about recent protests.

This chapter sits at the intersection of corporate responsibility, the Responsibility to Protect, and information and communication technology as shown in Figure 1. Each is explained below before introducing the framework for assessing information and communication firms' corporate responsibility within R2P.



Corporate Responsibility

Corporations have responsibilities across stakeholder groups that transcend the mere obligation to be profitable. Firms exist through the mutually beneficial and sustainable relationships with stakeholders such as employees, suppliers, communicates, customers, shareholders, governments, NGOs, and even competitors. And firms have corresponding responsibilities to those stakeholders: in order for those stakeholder relationships to remain mutually beneficial and sustainable, firms consider not only the consequences to those stakeholders but also principles of fairness in making decisions.

Firms take on these obligations based on four possible roles:

1. Firms take on responsibilities when they voluntarily enter into a relationship with a stakeholder or enter a community as part of an implicit social contract. For example, when Target opens a store in Washington, DC, Target takes on responsibilities as a member of the DC community.
2. Firms may create a product or service that has the possibility for good to help the vulnerable. For example, Home Depot provides a service with unique ability to help in a disaster and the firm takes that responsibility seriously to pre-stocking supplies ahead of a storm.

3. Firms may create a product or service that has the possibility for misuse that could cause harm. For example, mobile applications could be used to stalk victims of domestic violence through the unique design of the product.
4. Firms may be in a unique position through their knowledge and/or position within a network of stakeholders to enact change. For example, HB Fuller not only created a product – glue – that was used as a narcotic by children, the firm was also in a unique position in a developing country to be one of the only actors who was in control of their own destiny. This allowed HB Fuller the role of leader and the responsibility to enact change.

Firms regularly navigate multiple stakeholder relationships and corresponding responsibilities when doing business. The challenge is in maintaining those relationships across business lines, geographic boundaries, and cultural changes.

U.N's Responsibility to Protect

The U.N.'s Responsibility to Protect declares states have "the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity." Specifically:

> "Each individual State has the responsibility to protect its populations from genocide, war crimes, ethnic cleansing and crimes against humanity. This responsibility entails the prevention of such crimes, including their incitement, through appropriate and necessary means. … The international community should, as appropriate, encourage and help States to exercise this responsibility and support the United Nations in establishing an early warning capability."

Subsequent reports and analysis further emphasize the role of the international community to provide assistance to states as well as the role of the international community to take action to prevent and halt genocide, ethnic cleansing, war crimes and crimes against humanity.[3]

As noted by the Global Centre for the Responsibility to Protect, private actors play a pivotal role in R2P. The UN report allows for a variety of actors to provide assistance in capacity building to prevent atrocities (aka Pillar II) including the private sector. And effective capacity-building can supplement efforts by states to prevent the outbreak of atrocities and reduce need for collective action by the international community.[4]

R2P impacts firm's general corporate responsibility in two ways. First, as a member of the international community, corporations should assist in the prevention of atrocities through building capacity to protect populations even before conflicts break out. Second, firms have a responsibility during an atrocity to not only avoid assisting the perpetrator but also help the vulnerable and victim of atrocities. These obligations link back to the sources of corporate responsibility below and in Table 1:

1. Firms may engage in communities in conflict where human rights abuses occur and voluntarily take on a role as a member of the local community. The decision to engage in a community in conflict carries with it a responsibility to act like a member of that community, including building capacity in populations to prevent the outbreak of atrocities and providing assistance to halt atrocities.

[3] http://responsibilitytoprotect.org/implementing%20the%20rtop.pdf; http://responsibilitytoprotect.org/index.php/about-rtop/learn-about-rtop
[4] http://www.globalr2p.org/media/files/summary-of-the-r2p-report-2014-1.pdf

2. Firms may be in a position to help victims of human rights violations through their products and services. The creation of a product or service carries the possibility for good (help the vulnerable) in building capacity to protect populations.
3. Firms may contribute to violations of human rights by aiding bad actors through products and services. The creation of a product or service has the possibility for misuse (hurt the vulnerable) that could contribute to atrocities.
4. Firms may be in a unique position through their knowledge and/or position within a network of stakeholders facilitating to provide assistance during an atrocity or to build capacity to protect populations.

Table 1: Corporate Responsibility and R2P.

Corporate Responsibility	**Within R2P**	**Within R2P & ICT**
1. Role in the community Target in the local community.	The decision to engage in a community in conflict carries with it a responsibility to act like a member of that community – including building capacity to buttress atrocities and providing assistance during an atrocity.	Safaricom as an independently owned Kenyan company has an obligation as a member of the Kenyan community. Safaricom benefited from the close tie to Kenya and has an obligation – which they realized – to help the vulnerable and do no harm.
2. Position to help through products and services Home Depot and hurricane relief.	Firms may be in a position to assist victims of human rights violations through their products and services. Creation of product or service that has the possibility for good (help the vulnerable) in building capacity to protect populations	Safaricom held the market for SMS bulk messaging (95% in Kenya) thus positioning them as gatekeeper in the dissemination of SMS messaging in Kenya.
3. Position to harm through product and services Mobile Apps and stalkiing	Firms may contribute to violations of human rights by aiding bad actors through products and services. Creation of a product or service that has the possibility for misuse (hurt the vulnerable) and could exacerbate atrocities.	The use of SMS text messages to initiate human rights violations in the 2007 elections illustrates the possible harm from the use of Safaricom's technology.
4. Unique position based on knowledge or physical location	Firms may be in a unique position through their knowledge and/or position within a network of stakeholders facilitating to provide assistance and build capacity for prevention of atrocities.	Safaricom is not only positioned as a gatekeeper with their technology, but their unique market power within Kenya positioned them as a unique influence in policy negotiations with the government and mass media.

Information and Communication Technology (ICT).

Both corporate stakeholder responsibility within business ethics as well as R2P have highlighted the importance of information and communication technology (ICT).[5] The design of technology is value-laden in that features of the design influences the possible actions and decisions of users and other actors.

[5] ICT to include telecommunication services, web and cloud services, software, consumer end use devices, telecommunication components (GNI).

By understanding how a technology – including ICT – functions in its network of fellow technologies and users is critical to understanding if the technology is ethical and the firm is being responsible (Martin, 2008).

Within R2P, the Institute of Human Rights and Business at the *University of Washington* school of law notes that information and communication technology is critical for realization of rights – civil, political, economic, social, and cultural. Firms with ICT must understand their communities need for free expression, privacy, security, safety, and free association and assembly while using their technology (Digital Dangers, 2014). ICT companies may face issues of protecting privacy rights and freedom of expression, as well as government requests to ICT companies for access to user data or the removal of material.

In this way, ICT hold a special place for both R2P as well as corporate responsibility and business ethics. The difficulty comes in deciding the standard by which to judge or assess the ICT across global communities. The tension of abiding by home-country principles versus host country rules runs through global corporate responsibility.

In addition, assessing technology across communities further complicates the analysis in that the technology itself may function differently in a new country. Currently, and as explored in this chapter, the introduction of ICT in authoritarian governments such as China and Iran has facilitated the imprisonment of dissidents and the surveillance of citizens while also empowering users and protestors to build provide support for citizens at risk. Yet, how to assess ICT is not always clear since both the technology and the surrounding stakeholder context are factors to consider.

Typically within the current ethical analysis of global innovation, the innovator is positioned as choosing between upholding one's values and becoming complicit in an immoral normative scheme in the foreign country. Solutions are framed as dichotomous based on incommensurable home country versus host country norms (Hamilton, Knouse, & Hill 2009) and, in the case of Google in China, the organization is forced to give justifications and excuses for their complicity with the Chinese government (Dann & Haddow 2008). Firms facing R2P obligations are left with little guidance other than to exit – which might leave a population vulnerable without needed information and communication technology.

Framework for Analyzing ICT

This chapter develops a framework for the ethical analysis of global ICT for use with R2P. Based on pluralism scholarship, the framework offered here suggests that technology should be examined by broadly considering the stakeholders of the technology, the roles and responsibilities of the actors within a particular community, and the alternatives to the innovation. The cases of ICT in authoritative regimes offer a mechanism to show the utility of such a framework. The version of pluralism utilized here requires a charitable read and open consideration of local contexts and an examination of the innovation in practice.[6]

[6] While approaches to pluralism vary, key to pluralistic approaches is a move away from positioning differences as incompatible. In other words, pluralistic approaches eschew either/or solution sets. Rather than one right answer, pluralism allows for multiple right answers and a range understandings or descriptions (Rorty, 1989; Skillen 1996).

First, understanding ICT across cultures and border requires understanding the roles and responsibilities of technology and stakeholders. For example, within Science and Technology Studies, Latour (2000) examines the distribution of roles and responsibility within an innovation system of a technology and stakeholders and the important influence a technology has on the responsibility of fellow members of a social system. Latour leverages the seemingly benign examples of door closer and automobile safety devices to illustrate how roles and responsibilities are allocated to both technological and human actors to accomplish a goal. For example, a door closer's default settings (e.g. holding the door open versus closed) impacts who is viewed as responsible for closing the door (Latour 2000). On one extreme would be a door designed with a doorman assigned to the job of closing the door, relieving both the door and those who pass through from shutting the door. However, a door with a hydraulic closer that shuts the door automatically relieves those who pass through from being responsible for ensuring that the door is closed and makes the role of doorman unnecessary. Importantly, different roles are not necessarily considered unethical only because the roles are different allowing ICT to take on important ethical roles in R2P.

In addition to accommodating the important impact of ICT on the actions of others, the pluralistic framework moves away from dogmatism. For example, James (1907) positions pluralism as a movement against intolerance. James uses the example of an artificial clearing in the woods as being viewed by a farmer, who completed the clearing, as a personal victory. However, in coming upon the clearing, James first describes his reaction to the scene as revulsion. James saw the clearing as hideous: "The clearing which to me was a mere ugly picture on the retina, was to them a symbol redolent with moral memories and sang a very paean of duty, struggle, and success" (James 1907, 134; Rorty 1989, 38). The question for James was not whether or not he and the farmer held the same principles and values, but how seemingly incommensurable views could be redescribed. Consider how Google was judged for taking on a different role in China. Rorty notes that James's pluralistic approach to this clearing is not a reality-appearance distinction, but another redescription or set of metaphors. Several descriptions of the same event are possible without asking which one is right (Rorty 1989). Redescriptions are a "tool rather than a claim to have discovered any essence" (Rorty 1989, 39).

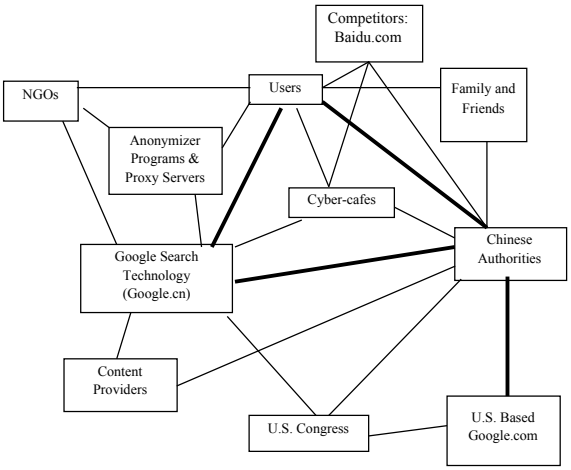
Important for the analysis of global Internet technology, these distinct descriptions warrant an examination *in and of themselves* and not necessarily in reference to one-right-description. In other words, the farmer deserves as much consideration as James in his description of the clearing. In regards to global information technology, disruptive innovations that cross borders into new communities deserve to be considered on their own merits as novel innovations and not solely in reference to a standard of use developed in a prior community or country – for example, the U.S. Therefore, the criterion for success, failure, or effectiveness of an innovation is not a stable, intrinsic property of the technology but rather a contingent property studied within a stakeholder community..

Based on broader pluralism scholarship, a pluralistic approach can be broken down into key components in order to build a framework for the ethical assessment of global innovation in general and Internet technology here.

1. Situate ICT in context.

Similar to James situating the clearing within the context of the farmer's world, ICT is best understood within the larger stakeholder community. Fully appreciating the ICT within the stakeholder community to identify and understand the participants in their environment, including stakeholders both influencing and influenced by technologies such as google.cn and Twitter. These material and nonmaterial actors within an innovation system *co-shape* each other (Johnson 2001), rely upon each other to complete tasks, and exist in a codependent relationship.

For example with Google in China, multiple governmental agencies, cybercafes, cyber police, regulated content providers, regulated access providers, NGOs, fellow citizens, users, users' families and friends, and even villagers without electricity impact are impacted by Google's search technology, google.cn, as in Figure 2.



The government was impacted by the increase in information traded among its citizens and, in reaction, increased its regulation of Internet providers and the surveillance and arrests of citizens through 30,000 Internet police and surveillance programs. This Great Firewall of China, the common name for the Chinese government's pervasive Internet surveillance and control, directly impacted all Internet activity, including google.cn (Canaves and Chao 2010).

In addition, NGOs and dissidents attempted to provide access to unfiltered information by developing tools such as proxy servers and anonymizer programs to circumvent government filters. *Fanqiang* supported a growing market for counter-surveillance software for Chinese users that was only bolstered when China blocked major sites such as Google's YouTube in March 2009 (Canaves & Chao 2010). Approximately one million people in China used a service provided by Global Internet Freedom (GIF) that was maintained by 50 volunteers around the world. The group was founded in 1999 by members of the Falun Gong sect living in the United States to provide unfiltered information about Falun Gong to China (Stone and Barboza 2010). In addition to proxy servers, virtual private networks, or VPNs, allowed citizens to access the Internet through alternative servers that supported anonymous and unfiltered access to websites. Super-users were creative, active, and knowledgeable citizens who became an integral part of searching online in China.

2. Analyze a range of roles and responsibilities.
Roles and functionalities of a technology vary based on the adopting community**.** Google.cn's role in China was complicated and can be described as contributing to three additional goals in China to the expected function as a search engine in less restrictive countries: (1) as a tool of censorship by Chinese authorities, (2) as a buffer between the government and the Chinese citizens, and (3) as an alternative gateway to information.

First, as has been widely reported, google.cn played an active role in government censorship by self-filtering search results. Blocking sites was not the primary method for controlling content by the Chinese; instead the Chinese authorities relied upon self-censorship by technologies such as google.cn. In this way, google.cn acts in *obedient complicity* (pp. 459) with Chinese censorship "in a manner that results in Chinese people being unable to have access to websites to which they arguably have a right of access" (Brenkert 2009, 460).

Second, google.cn provided enhanced anonymity for users as compared to alternatives. While alternative Internet technologies, such as Microsoft and Yahoo!, have proven to be less adept at protecting the identity of their users (Martin 2008b), Google, Inc. decided to maintain all personal information associated with e-mail and weblogs outside Chinese territory and outside the jurisdiction of Chinese authorities, thus allowing google.cn to differentiate itself from competitors and become an important part of citizens maintaining anonymity online.

Finally, google.cn supported Chinese users in accessing *additional* information normally censored by Chinese authorities. Google.com search technology was located outside Chinese territory, relied on a few fiber optic pipes to carry information to and from the user's computer in China, and was easily monitored and blocked through a few data checkpoints. However, google.cn resided within Chinese territory thereby avoiding some filtering routers and allowing multiple points of connection for Chinese users. Google.cn's presence offered not just a competitive alternative to Baidu and other search technologies, but also an important alternative route for users attempting to circumvent surveillance and censorship.

3. Compare descriptions and roles to alternatives in practice.
Finally, to enrich, enhance, and expand stakeholders is relative to alternatives in practice rather than in comparison to an objective standard of use from a previous community. Roles and responsibilities must be examined in comparison to alternative solutions rather than a single ideal based on previous patterns of use.

If the goal is *more access to news and communication between citizens*, google.cn and its competitors enhance the goal of providing the most information possible to Chinese citizens. If the innovation system's goal is *avoiding censorship and surveillance*, providing yet another route for users in China, google.cn does enhance and enrich the stakeholders in Figure 1 by making censorship and surveillance more difficult. If the goal is *to act as a buffer between Chinese authorities and Internet users in China*, google.cn played an important role shielding Baidu from the censorship battle (LaFraniere 2010). "Without Google, Baidu will be very easy to manipulate," said a 20-year-old computer science major at Tsinghua (LaFraniere 2010).

Finally, google.cn played a symbolic role in China. As noted by Hu Yong, a journalism professor at Peking University, "This is a matter of the future and whether the government's Internet policy wants to fight with the future…If this process goes on, more and more people are going to realize that their freedom of information is being infringed upon, and this could bring changes down the line" (LaFraniere 2010). Through google.cn, Google performed a role of a fellow agitator of the Chinese authorities.

Google.cn performs its role as a buffer between the government and Chinese citizens and as an important partner with competitors and proxy servers to provide a complex vehicle for the dissemination of and access to censored information. Privately developed proxy servers, anonymizer programs, and Chinese users work in conjunction with Google's search technology to give Chinese citizens access to censored material and support circumventing surveillance. While google.com is able to provide broad search results, the combination of google.cn, Baidu, users, super users, anonymizer programs, NGOs, and proxy servers provide parallel results for the Chinese citizens.

Framework for Responsible Management of ICT

	Corporate Stakeholder Responsibility		
	Place in Context of Stakeholder Relationships	**Identify Roles & Responsibilities of Actors**	**Compare to Alternatives in Practice**
Questions for R2P and ICT analysis	Who or what is influenced by your technology or influencing the effective delivery of your service?	What are the various roles your ICT plays in the stakeholder diagram?	Are you in a unique position to effect change? Are you a hindrance to change? Is a vulnerable population better off with your presence? Are atrocities more likely or more intense with your presence?
Within R2P Safaricom in Kenya	Safaricom. NCIC, Content Service Providers, originators of bulk SMS, competition, Communication Commission of Kenya (CCK), mainstream media, Kenyan citizens.	As gatekeeper to message Kenyans with 95% of SMS market and 65% of mobile phone market. As a possible vehicle for hate speech. As a citizen of Kenya (an independent Kenyan company).	2007 elections with uncensored SMS messages to Kenyan citizens provides the alternative to avoid.
ICT & R2P Twitter and Arab Spring	Twitter, proxy servers, multiple 'front doors' (s.a. websites, texts, phones, PDAs), Iranian citizens (word-of-mouth), NGOs, Tor, citizens in other countries (to hide locations). Twitter in Iran is illustrative of a technological infrastructure that works to circumvent an authoritarian government and provides an example of multiple routes as an effective strategy against censorship.	As access to censored information. As a route for news to be disseminated. As a mechanism for citizens to organize.	ICT within the Arab spring build capacity and assist victims of atrocities by providing a news outlet giving voice to those victimized and alerting the international community as to the situation. In addition, ICT supported freedom of movement and association to empower the vulnerable. ICT within the Arab spring build capacity and assist victims of atrocities by providing a news outlet giving voice to those victimized and alerting the international community as to the situation. In addition, ICT supported freedom of movement and association to empower the vulnerable.

Framework in Action: Twitter in Iran and the 2011 Arab Spring

While Internet technologies in China have drawn sharp criticism, information and communication technologies in other authoritarian countries have received praise for their ability to empower vulnerable citizens and work against atrocities by not only helping victims during an atrocity but also building capacity to protect vulnerable populations to prevent an atrocity.

Iran 2009. During protests over the Iranian national elections in 2009, foreign journalists were forced to leave Iran, and citizens became the primary providers of news and pictures (Stone and Cohen 2009). State-controlled telecommunications were shut down and then reinstated, with spotty availability for weeks. Eventually even texting became unavailable, and Twitter became the vehicle to disseminate news about the candidates and the election, as well as current and future protests (Stelter & Stone 2009).

The Iranian uprising in 2009 proved to be a precursor to the protests throughout the Middle East and northern Africa over the following two years. Similar to the start of the Iranian movement, a video of the beating to death of a 28-year-old businessman, Khaled Said, became a rallying point for protestors across Tunisia, Egypt, and Bahran. Khaled Said had been beaten to death by Egyptian police in the lobby of a residential building; the video was eventually posted on Facebook in June 2010 with the statement "We are all Khaled Said."

Arab Spring. Six months later, Tunisian protests began what became the Arab Spring. The Tunisian government shut down the television network and closed schools and universities in January 2011 as protests began to spread throughout the capital (Kirkpatrick 2011). Using Facebook and Twitter, protesters were still able to organize demonstrations, in which many individuals were arrested and killed by the Tunisian military.

Shortly after the Tunisian uprisings, there were large protests in Egypt as well as smaller demonstrations in Bahrain, Jordan, Sudan, Yemen, and Libya, from January through March 2011 (Shadid & Bronner 2011; Gettleman 2011; MacFarqhar 2011). The original Facebook page dedicated to Egyptian Khaled Said was a focal point for dissidents to communicate and organize protests in Egypt, with over 500,000 users during the Arab Spring. Throughout these protests, social networking sites such as Twitter, YouTube, Flickr, and Facebook proved pivotal for citizens accessing censored information as well as communicating with fellow citizens.

While each country has a distinct political, economic, and demographic context for its uprising, several factors offer a common thread to tie these demonstrations and protests together and provide a link to the situation in China. First, each government sought the centralized control of information and news (Stelter & Stone 2009) by cutting long distance phone lines, restricting access by foreigners, and owning or heavily regulating communications such as television and radio. For example, in Tunisia, the television station was shut down immediately and the owner was arrested for 'grand treason' (Kirkpatrick 2011). In order to control the news, the Egyptian government owns 99% of all newspaper publishers and newsstands, and 72% of Egyptians watch the state owned television (Walker & Orltung 2011). Also, regimes would slow down the Internet to make connections frustrating for citizens. After the Iranian election, the state-controlled telecom provider went down completely for part of the day and then traffic

was slow for weeks (Stelter & Stone 2009). Dictators controlled the media and offered a "parallel reality" (Walker & Orltung 2011). Similarly, Chinese authorities monitored users accessing 'harmful' content that included material about democracy (e.g., freedom), religious cults (e.g., Falun Gong), or antigovernment protests (e.g., Tiananmen Square) (Martin 2008b). Chinese authorities even established reporting centers to encourage citizens to report "harmful" information (McMahon 2006). In addition, China had what was called the "50-cent party," comprised of Chinese citizens who were paid 50 cents per post to flood anti-government sites with pro-government messages (Shane 2011). Controlling the information and communication technology became a precursor to atrocities such as war crimes and crimes against humanity.

Second, each government imposed strict limitations on gathering and organizing leaving populations vulnerable to human rights violations by authoritative governments. Tunisia closed universities and schools at the beginning of their protests (Worth and Kirkpatrick 2011). Dissidents were imprisoned, tortured, and killed for expressing alternative views or attending protests against the regime. Governments used pervasive tracking of individuals both online and offline. Iran and Syria used surveillance technologies by Nokia and Siemens Network in 2009 as well as CacheFlow in 2011 to monitor the communications of citizens. Similarly, the Chinese government had a band of 30,000 Internet police to monitor its citizens as well as surveillance technology to ensure citizens were not breaking censorship laws.

ICT within the Arab Spring assisted victims of atrocities by providing a news outlet giving voice to those victimized and alerting the international community as to each situation. In addition, ICT facilitated freedom of movement and association to empower the vulnerable.

1. Situate Twitter in context: Twitter's Stakeholders. Twitter highlights the importance of stakeholders to a technology since the technology relies heavily on many other stakeholders to act as different front doors or gateways in order to function. Unlike other Internet technologies – such as social networking sites, traditional websites, search engines, blogs, etc – Twitter users have always been able to access Twitter feeds through multiple routes and platforms such as other websites, texts, phones, PDAs, and computers without users actually visiting Twitter's site. This tactic is normally not strategically advantageous, as Twitter cannot deliver reliable users to advertisers and hence cannot easily monetize their service (Sullivan 2009).

In Iran, Twitter's open architecture proved particularly resilient to censorship. When text messaging, Internet, and cellphone transmissions were unavailable in Iran during the political upheaval after the 2009 elections, citizens found ways to still communicate through proxy servers and software (Stone & Cohen 2009). Proxy servers are computers that are hidden or unknown to surveillance and redirect users to currently censored material. The Internet user visits the non-blocked proxy server located outside the country in order to be bounced to content normally blocked by authorities. In order to work, *multiple* proxy server addresses must be available to the user and not to the authorities. As noted during the summer 2009 uprisings after the national Iranian elections:

In the face of an increasingly restrictive Iranian government, which was censoring millions of websites, "more than 400,000 Iranians were surfing the uncensored Web" (Markoff 2009). Shiyu Zhou, founder of

the organization providing anti-censorship software and tools, said "In China we have sent mass e-mails, but nothing like in Iran…The Iranian people actually found out by themselves and have passed this on by word of mouth" (Smith & Cohen 2009). When the Egyptian government cut access to Internet, page views by Egyptians on Ultra Surf, a free proxy-based privacy tool, increased 10-fold to 7.8 million page views per day from only 76,000 the day before. In other words, Internet and information technology in Iran during 2009 and the 2011 Arab Spring was possible due to the many technologies and individuals providing multiple access points to the Internet, thereby making control by the governments much more difficult.

To increase the number of users, NGOs took an active role and developed training for citizens without access or knowledge of social networking sites. For example, Hiber was started by Jordanian Mariam Abu Adas for social media training in more remote areas during the Arab Spring. Such training was necessary for many citizens not familiar with social networking technology or how to use it safely without being monitored (Slackman 2011). Stakeholders, such as NGOs, the Global Internet Freedom Consortium, the Tor Project, or Psiphon, provided software to work around censorship and authoritarian governments, thereby allowing users to send untraceable messages and to reach censored websites (Markoff 2009; Stone & Cohen 2009).

The ability to access Twitter through multiple points proved critical with a government focused on curtailing communication. When one communication technology was disabled by the government or became just too dangerous, an alternative was still available to utilize Twitter for communication. For example, when cell phone and Internet service was disabled, social networking technology such as Twitter or Facebook relied on 'old media' technologies using a satellite to remain available (Farrell 2011). Al Jazeera, a global television station, also proved helpful in disseminating information by showing videos taken by protestors (Worth & Kirkpatrick 2011). Therefore, when Internet connections would become unreliable, previously posted videos were still available on television.

2. Analyze a range of roles and responsibilities. Within a controlling, authoritative context, ICTs take on decidedly different roles than in a more open environment by providing (a) access to censored news, (b) a route to disseminate news to outsiders, and (c) a mechanism for citizens to organize. These roles are critical to preventing atrocities through building capacity to protect populations even before conflicts break out as well as help the vulnerable and victim of atrocities.

During the Iranian protests over the 2009 elections, foreign journalists were forced to leave Iran and citizens became the primary providers of news and pictures (Stone & Cohen 2009). Suddenly, Twitter became the vehicle to access news about the candidates, the election, as well as current and future protests. By allowing access to censored news, "new kinds of social media are challenging those traditional levers of state media control and allowing Iranians to find novel ways around the restrictions" (Stone & Cohen 2009). Social networking technology provided access to information not controlled by the state or other controlling regimes. Realizing the important role of Twitter in accessing information, the U.S. State Department began a Twitter feed in Arabic and Persian and soon followed with feeds in Chinese, Russian, and Hindi (Preston 2011; Landler & Kwolton 2011).

In addition to providing access, social networking technologies and the community of stakeholders provided a mechanism for news to be disseminated. The 40-second video of Neda Agha-Soltan's death that began the protests in Iran was sent to a series of individuals who then posted it on Facebook. A self-immolation video in Tunisia was similarly disseminated on Facebook rather than through traditional media outlets. While in the U.S. mainstream media was the largest user of Twitter (Bilton 2011), the role of Twitter in the Middle East was as an alternative news source, used also by journalists to source and verify stories (Stelter 2011). As noted by James E. Katz, director of the Rutgers Center for Mobile Communication Studies, the most powerful weapon in getting around the "manipulation of the old centralized technologies" became the tiny camera inside cell phones (Preston & Stelter 2011).

Finally, Facebook and Twitter were the primary tools for activists to gather, mobilize, and protest (Preston 2011). The system of social networking sites provides multiple avenues for communication, which then becomes difficult to control. Hashtags on Twitter help spread protest information (Preston 2011). Twitter users asked supporters to form an online attack on Iranian government servers, and a Facebook site gained more than 70,000 supporters for "April 6 Youth Movement" (Preston 2011). The site of the Khaled Said beating video, "We are all Khaled Said," in June 2010, remained the largest dissident Facebook page during the Arab Spring (Preston 2011), and a Facebook group called Moroccans Discuss the King had 3,000 members in 5 days. Women, who could not meet unaccompanied, could chat online (Slackman 2011), and social networking technologies provided new means for ordinary people to connect with human rights activists (Preston 2011).

Within a system of technology and stakeholders, each social network technology performs a role with associated responsibilities that impacts the roles and responsibilities of fellow stakeholders. Proxy servers and multiple access points gave users access to Twitter, thereby relieving Twitter from the task of ensuring its website was always accessible within tightly controlled countries. Twitter and other social network technologies gave users an outlet to disseminate news, thereby relieving journalists the role to be the sole source of news during the protests. Social networking technologies worked jointly with a larger system of stakeholders, NGOs, citizens, cameras, satellite phones, etc – to increase access to censored information, allow wide dissemination of information, and support citizens in organizing.

3. Compare descriptions and roles to alternatives in practice. Twitter and social network technologies, such as Facebook, made key decisions in accessing and disseminating news as well as allowing citizens to gather and organize. There were some slight modifications; for example, Facebook upgraded security for all users after Tunisian government officials used a virus to obtain local Facebook passwords (Preston 2011). However, Google and YouTube were even more willing to embrace their roles in activism during the Arab Spring. First, when the Internet was unavailable, Twitter specifically created Speak2Tweet allowing people to leave voicemail messages that would be filed as a Twitter update. This modification made even access to the Internet unnecessary in order to disseminate news via Twitter. Later, Twitter added a local number for Speak2Tweet for Egyptians so that long distance telephone access was not even necessary. In addition, YouTube worked with Storyful, a social media news curation service, to help people retrieve and share thousands of videos pouring in from Tahrir Square during the Egyptian uprising, thus helping citizens organize more easily (Hauser 2011).

Not all decisions supported the laudable goals of access to information and organization. Facebook shut down a popular protest page of Wael Ghonim, a Google executive who was a symbol of the revolt, when he used a pseudonym. While the requirement for real names helps Facebook ensure accountability in their users' statements and actions in a more open context, the requirement to use real names became a mechanism for surveillance in an authoritative regime. When the Egyptian government correctly identified Wael Ghonim and his role on Facebook, the executive was imprisoned for 12 days (Preston 2011). Similarly, Flickr removed pictures of Egyptian security police when the company realized that the individual who posted the pictures did not actually take the photos (Preston 2011). Requirements for identification and ownership did not support the role of these social networking sites in curtailing surveillance and disseminating news in Iran and during the Arab Spring.

Interestingly, the aftermath of the Arab Spring and Iran in 2009 suggests that the use of social networking technologies, such as Twitter and Facebook, is similarly complicated. These technologies also became actors in a system of surveillance by authoritarian governments. The Iranian government proved adept at using Internet technologies to go after activists and followed electronic trails left by activists online (Shane 2011). Iran also crowd-sourced the hunt for protestors by posting unidentified photos and soliciting input from the public in order to identify names. The very factors that brought Facebook and similar communication success have huge appeal to secret police as social network sites provide a dossier of activists for police. Facebook is a "great database for government now," noted Ahed al-Hindi, a Syrian activist (Shane 2011). Bloggers were imprisoned in Egypt for "insulting the military establishment based on 73 screenshots of blogs and Facebook pages" (Stack & Bronner 2011), and the Egyptian government monitored text, Skype, and email based on records found after the fall of the government (Stack & MacFarquhar 2011). Soon citizens became aware of social networking technology's dual role. In Egypt, demonstrators instructed that a 26 page anti-government leaflet be passed by email and by photocopying rather than by Twitter and Facebook in order to avoid the growing surveillance of the social networking technologies (Shane 2011).

Discussion and Conclusion

The framework offered here, grounded in the pragmatic tradition of pluralism, suggests global ICT should be examined by initially considering three factors: the stakeholders of the technology, the roles and responsibilities of the actors within a particular community, and the alternatives to the innovation. To illustrate the pluralistic framework. ICT, such as Twitter in Iran and the Arab Spring, is illustrative of a technological infrastructure that works to circumvent an authoritarian government and provides an example of multiple routes as an effective strategy against censorship.

While one can mistakenly focuses on Internet technology used as a tool for censorship by authoritarian governments, these technologies also play an important role in the technological infrastructure necessary for citizens to gain access to information and communicate with peers safely thereby paying an important role in R2P. While google.cn functions as both a buffer between Chinese citizens and their government as well as a partner with proxy servers and competitors to provide users multiple points of access to receive and disseminate information, Twitter plays an important role as a communication vehicle between Iranian citizens and to the international community. In both situations, the ICT firms worked towards the prevention of atrocities by building capacity to protect populations even before conflicts break out. In

addition, the presence of ICT helped the vulnerable and victim of atrocities and communicated the ongoing atrocities to the international community.

Given the role of proxy servers in the lives of citizens under authoritarian governments, maintaining multiple Internet gateways is critical to giving citizens alternatives paths to communicate. While taking on different roles in comparison to search technologies in the U.S., google.cn in China and Twitter in Iran perform valid, ethical functions in the global community. Google.cn functions as both a buffer between Chinese citizens and their government and as a partner with proxy servers and competitors in providing users multiple points of access to receive and disseminate information. Twitter plays a critical role as a communication vehicle between Iranian citizens and to the international community. In respecting different environments and patterns of use, google.cn, Twitter and other networking Internet technologies must be open to different stakeholders systems, alternatives, and roles and responsibilities to create solutions that enrich and enhance populations. In fact, to not change the role and functionality of a disruptive ICT may ignore the very real, situated demands on stakeholders for those at risk of atrocities.

This chapter contributes to a nascent discussion around corporate responsibility and R2P. Additional questions include:

1. Who needs protecting within the idea of R2P for firms? What are the criteria for vulnerable groups needing protection? The cases offered here are with the benefit of hindsight. And, with the case of Safaricom, a precedent was already set in 2007 highlighting the possible atrocities. However, pending atrocities are not always clear as evidenced by the backlash against Google with first in China.
2. Which firms or industries might play a role within R2P? This chapter focused on ICT, but the intersection between corporate responsibilities and the responsibility to protect needs further consideration.
3. What are the associated responsibilities of firms and managers when engaging in communities in conflict? This chapter outlines the sources of obligations for corporations generally and within the scope of R2P, however, more work should be done to specify the sources and the substance of obligations with R2P for corporations. The Digital Dangers (UW Law) project offers six risks ICT firms face including disconnecting or disrupting access, monitoring, evaluating, and blocking user content at request of third parties, selling dual use technology with possibility of misuse, complying with government orders, monitoring user content, and handing over user content and data to state. Yet ICT firms face these issues *in every country including the United States* and without imminent risk of genocide, war crimes, ethnic cleansing or crimes against humanity. More work is necessary to spell out the risks faced by ICT firms around R2P in particular. The Global Network Initiative is moving in that direction with practical advice for firms.