Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 7 Article 7

Fall 2013

The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response

Mirae Yang

Recommended Citation

Mirae Yang, *The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response*, 11 Nw. J. Tech. & Intell. Prop. 707 (2013).
http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss7/7

This Comment is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized administrator of Northwestern University School of Law Scholarly Commons.

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response

Mirae Yang

September 2013 VOL. 11, NO. 7

© 2013 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property

Copyright 2013 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 7 (September 2013)

The Collision of Social Media and Social Unrest: Why Shutting Down Social Media is the Wrong Response

By Mirae Yang*

I. INTRODUCTION 708
II. THE RECENT HISTORY OF SOCIAL MEDIA'S EFFECT ON SOCIAL UPRISINGS ACROSS THE WORLD AND THE GOVERNMENT'S SUBSEQUENT REACTIONS 708
A. Arab Spring 708
B. London Riots 710
C. United States 710
III. WHY SOCIAL MEDIA? SOCIAL MEDIA'S ABILITY TO FUEL SOCIAL UPRISINGS 711
A. Facebook and Twitter 712
B. Blackberry 713
IV. SHUTTING DOWN SOCIAL MEDIA IN THE UNITED STATES 714
A. Executive Power Under Youngstown and the Communications Act of 1934 714
B. Current Litigation—Kill Switch 716
C. Executive Order 719
V. IMPACT OF SHUTTING DOWN SOCIAL MEDIA 719
A. First Amendment Violations 719
B. Economic Consequences 721
C. Setting Dangerous Precedent 722
D. Restricting Social Media is Ineffective 723
VI. A PREVENTATIVE RESPONSE 724
A. Private-Public Partnership 724
B. Recognizing the Value of Social Media 725
C. Enhance Law Enforcement's Capabilities to Anticipate and Quickly Respond to Violent Disorder 726
VII. CONCLUSION 727

* J.D., 2013, Northwestern University School of Law.

I. INTRODUCTION

¶1 With the growing availability of Internet access across the globe, social media has transformed the traditional relationship between government authority and its citizens by providing the people with an innovative and powerful means to harmonize their efforts in expressing their political and social concerns. The importance of safeguarding Internet availability is more critical than ever before as access to the Internet is now the means by which the world communicates, stays informed, and engages in daily tasks.[1] In the face of potential social unrest fueled by social media, the United States must take a preventative approach, one that matches our policy of Internet freedom with technology. It is paramount that the United States refrains from adopting the oppressive policies of other governments by shutting down the Internet or restricting access to social media.

¶2 This Comment examines the United States' ability to shut down social media in response to potential violent social unrest and the effect of such a shutdown. Part II describes the recent history of social media's effect on social unrest across the globe. Part III explains social media's role as a powerful communication tool, capable of fueling social and political change all over the world. Part IV considers whether the United States federal government has the legal authority to shut down social media if faced with a situation similar to the London riots. Part V then analyzes the dangerous impacts of such government action, while Part VI proposes a preventative approach to address future attempts in the United States to stop social unrest. Part VII briefly concludes.

II. THE RECENT HISTORY OF SOCIAL MEDIA'S EFFECT ON SOCIAL UPRISINGS ACROSS THE WORLD AND THE GOVERNMENT'S SUBSEQUENT REACTIONS

A. Arab Spring

¶3 The "Arab Spring" refers to the recent wave of democratic uprisings that began in Tunisia and spread across the Arab nations.[2] Using various social media platforms as their primary mode of communication, the civilian uprisings called for an end to the oppressive policies and corruption of their existing governments.[3]

¶4 In Tunisia, protests began following the attempted suicide in Sidi Bouzin by Mohamed Bouazizi on December 17, 2011.[4] The riots ultimately led to the overthrow of President Zine El Abidine Ben Ali as he fled to Saudi Arabia on January 14, 2011.[5]

---

[1] *See* Karson K. Thompson, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate*, 90 TEX. L. REV. 465, 491 (2011); 157 CONG. REC. S910 (daily ed. Feb. 17, 2011) (statement of Sen. Collins) ("It is essential that the Internet and our access to it be protected to ensure both reliability of the critical services that rely upon it and the availability of the information that travels over it.").

[2] *See* Raymond Schillinger, *Social Media and the Arab Spring: What Have We Learned?*, HUFFINGTON POST (Sept. 20, 2011, 3:59 PM), http://www.huffingtonpost.com/raymond-schillinger/arab-spring-social-media_b_970165.html.

[3] *See id.*

[4] Bouazza Ben Bouazza & Elaine Ganley, *Jobless Youths in Tunisia Riot Using Facebook*, MSNBC (Jan. 11, 2011, 5:18 PM), http://www.msnbc.msn.com/id/41026780/ns/technology_and_science-tech_and_gadgets/t/jobless-youths-tunisia-riot-using-facebook/ (Mohamed Bouazizi was a twenty-six-year-old man with a university degree who lit himself on fire when police confiscated the fruits and vegetables he was selling without a permit.).

[5] David D. Kirkpatrick, *Tunisia Leader Flees and Prime Minister Claims Power*, N.Y. TIMES (Jan. 14, 2011), http://www.nytimes.com/2011/01/15/world/africa/15tunis.html?pagewanted=all.

Tunisian protestors utilized social media, including Facebook and Twitter, as their primary outlets to communicate and organize their demonstrations.[6] The Tunisian government responded with increased efforts to control the Internet by blocking numerous websites covering the protests and recording users' Facebook passwords to delete Tunisian activists' accounts and protest pages.[7]

¶5 Less than a month following the successful uprising in Tunisia, protests in Cairo, Egypt began on January 25, 2011 as Egyptians gathered to demand the end of Egyptian President Hosni Mubarak's regime.[8] On February 11, 2011, after eighteen days of revolting, "a largely secular, nonviolent, youth-led democracy movement" successfully removed Mubarak from office.[9] Following Tunisia's lead, digital revolution continued as the Egyptian revolution used Facebook, Twitter, and YouTube to "organize the revolutionaries, transmit their message to the world and galvanize international support."[10] In response, the Egyptian government blocked Internet access and cell phone service across Egypt by forcing its Internet service providers to withdraw data access routes into and out of Egypt.[11]

¶6 Although countries such as China, Iran, Thailand, and Tunisia have all censored social media platforms in times of social unrest, the Egyptian government's complete shutdown of almost all Internet activity was a "new phenomenon."[12] The unprecedented action was particularly surprising because, unlike other authoritarian regimes, Egypt originally had liberal Internet censorship policies, which was in part how it positioned itself as a thriving communications sector and a regional hub for Internet investment.[13] Moreover, by unplugging itself from the Internet, Egypt undermines its position as one of the major conduits connecting the region to the rest of the world.[14]

---

[6] Tim Lister, *Tunisian Protests Fueled by Social Media Networks*, CNN (Jan. 12, 2011, 9:13 PM), http://www.cnn.com/2011/WORLD/africa/01/12/tunisia/index.html.

[7] Nate Anderson, *Tweeting Tyrants out of Tunisia: Global Internet at Its Best*, WIRED (Jan. 14, 2011, 7:09 PM), http://www.wired.com/threatlevel/2011/01/tunisia/; *see* Alexis Madrigal, *The Inside Story of How Facebook Responded to Tunisian Hacks*, ATLANTIC (Jan. 24, 2011, 1:20 AM), http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/.

[8] David D. Kirkpatrick, *Egypt Erupts in Jubilation as Mubarak Steps Down*, N.Y. TIMES (Feb. 11, 2011), http://www.nytimes.com/2011/02/12/world/middleeast/12egypt.html?pagewanted=all.

[9] *Id*.

[10] Sam Gustin, *Social Media Sparked, Accelerated Egypt's Revolutionary Fire*, WIRED (Feb. 11, 2011, 2:56 PM), http://www.wired.com/epicenter/2011/02/egypts-revolutionary-fire/.

[11] *See* Christopher Williams, *How Egypt Shut Down the Internet*, TELEGRAPH (Jan. 28, 2011, 11:29 AM), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html; Christopher Rhoads & Geoffrey A. Fowler, *Egypt Shuts Down Internet, Cellphone Services*, WALL ST. J. (Jan. 29, 2011), http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html; Alexandra Dunn, *Unplugging A Nation: State Media Strategy During Egypt's January 25 Uprising*, FLETCHER F. WORLD AFF., Summer 2011, at 16 ("[The Egyptian government] first attacked content (information traveling through media and grounded, non-aggregated social networks), followed by general platforms (Facebook and Twitter), and then communication infrastructure (mobile telephone and Internet services).").

[12] Williams, *supra* note 11.

[13] *See* Andrew McLaughlin, *Egypt's Big Internet Disconnect*, THE GUARDIAN (Jan. 31, 2011, 4:30 PM), http://www.guardian.co.uk/commentisfree/2011/jan/31/egypt-internet-uncensored-cutoff-disconnect.

[14] *See* Rhoads & Fowler, *supra* note 11 ("Eight major undersea fiber links now run through the Red Sea and across the Sinai Peninsula, connecting the region to more developed links in Europe, and from there to the rest of the world.").

B. London Riots

¶7 What began as a peaceful protest in response to Mark Duggan's fatal shooting by Metropolitan police on August 4, 2011 erupted on August 6, 2011 into a full-scale riot leaving Tottenham, London in flames.[15] The violence and widespread looting quickly spread beyond Tottenham across several London boroughs and districts.[16] It was widely reported that rioters used social media, including Facebook and Twitter, to organize and encourage violence and protest throughout London.[17] BlackBerry Messenger (BBM) appears to have played a pivotal role by providing users with a more "covert social network" with untraceable and up-to-the-minute communication.[18]

¶8 In the aftermath of the riots, the British government explored the idea of turning off social networks to contain or stop the riots.[19] In a statement to the House of Commons, Prime Minister David Cameron stated that the "[f]ree flow of information can be used for good. But it can also be used for ill. And when people are using social media for violence we need to stop them."[20] He announced that the government was considering "whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality."[21]

C. United States

¶9 The United States has also recently experienced incidents of social unrest enabled by social media, though not on the scale of the riots in London or the protests in the Middle East.

1. San Francisco's Bay Area Rapid Transit

¶10 On August 11, 2011, the Bay Area Rapid Transit (BART) police shut down its underground mobile service for three hours to avert an anticipated protest against BART

---

[15] Sara Bolesworth, Barry Neild, Peter Beaumont, Paul Lewis & Sandra Laville, *Tottenham in Flames as Riot Follows Protest*, GUARDIAN (Aug. 6, 2011), http://www.guardian.co.uk/uk/2011/aug/06/tottenham-riots-protesters-police.

[16] *See England Riots: Maps and Timeline*, BBC (Aug. 11, 2011, 11:43 AM), http://www.bbc.co.uk/news/uk-10321233.

[17] *See, e.g.*, Mathew Ingram, *Network Effects: Social Media's Role in the London Riots*, GIGAOM (Aug. 8, 2011, 10:01 AM), http://gigaom.com/2011/08/08/network-effects-social-medias-role-in-the-london-riots/ (Twitter and Facebook were used to coordinate specific acts or gatherings.); William Lee Adams, *Were Twitter or BlackBerrys Used to Fan Flames of London's Riots?*, TIME (Aug. 8, 2011), http://www.time.com/time/world/article/0,8599,2087337,00.html (Twitter was used to encourage violence and spread unrest across Tottenham.).

[18] Josh Halliday, *London Riots: How BlackBerry Messenger Played a Key Role*, GUARDIAN (Aug. 8, 2011), http://www.guardian.co.uk/media/2011/aug/08/london-riots-facebook-twitter-blackberry; *see* Chris Taylor, *London Riots: BlackBerry Messenger Used More Than Facebook or Twitter*, MASHABLE (Aug. 8, 2011), http://mashable.com/2011/08/08/london-riots-blackberry-messenger/ (BBM was the most popular social media medium of choice for rioters to communicate).

[19] *England Riots: Government Mulls Social Media Controls*, BBC (Aug. 11, 2011), http://www.bbc.co.uk/news/technology-14493497.

[20] Prime Minister's Office, *PM Statement on Disorder in England*, GOV.UK (Aug. 11, 2011), http://www.number10.gov.uk/news/pm-statement-on-disorder-in-england/.

[21] *Id*.

police for fatally shooting a forty-five-year-old man.[22] In doing so, they denied potential protesters and train riders access to social media.[23]

¶11 The BART police justified the temporarily interrupted cell phone service in a statement claiming that protestors planned to disrupt BART service by using social media through their mobile devices to coordinate protests, which would jeopardize the safety of BART customers on the platform.[24] Indeed, while the British government first took the time to consider whether they had the *ability* to shut down certain social media services, an American transit company took unilateral action by restricting social media access without such debate.[25]

2. Flash Robs

¶12 The "flash robs" phenomenon—where social media is used to organize groups of teens and young adults to quickly ransack and loot various retail stores—began to occur sporadically throughout the United States over the past few years.[26] The spontaneity and speed of the attacks enabled by social media make it challenging for the police to prevent or stop the flash mobs in a timely matter.[27]

III. WHY SOCIAL MEDIA? SOCIAL MEDIA'S ABILITY TO FUEL SOCIAL UPRISINGS

¶13 Social media's role as a powerful communication tool has proven to be a vital instrument in fueling social and political change around the globe. However, critics have questioned the "outsized enthusiasm for social media" and expressed doubt regarding the extent to which social media has shaped the current social and political landscape.[28] They argue that social media does not produce the discipline and strategy that social change has always required.[29] This skepticism is shared by those who question the supposed "social media revolution" in the Middle East on the grounds that the fascination

---

[22] Eve Batey, *BART Defends Decision to Cut Off Cell Service After Civil Rights, FCC Concerns Raised*, SF APPEAL (Aug. 12, 2011, 3:15 PM), http://sfappeal.com/news/2011/08/bart-cell-fcc.php.

[23] *See id*.

[24] *See Statement on Temporary Wireless Service Interruption in Select BART Stations on Aug. 11*, BAY AREA RAPID TRANSIT (Aug. 12, 2011, 1:08 PM), http://www.bart.gov/news/articles/2011/news20110812.aspx.

[25] *See* Melissa Bell, *BART San Francisco Cut Cell Services to Avert Protest*, WASH. POST (Aug. 12, 2011, 5:12 PM), http://www.washingtonpost.com/blogs/blogpost/post/bart-san-francisco-cut-cell-services-to-avert-protest/2011/08/12/gIQAfLCgBJ_blog.html.

[26] *See* Ann Zimmerman & Miguel Bustillo, *'Flash Robs' Vex Retailers*, WALL ST. J. (Oct. 21, 2011), http://online.wsj.com/article/SB10001424052970203752604576643422390552158.html (noting the name "flash robs" describes the criminal incarnation of the "flash mob" phenomenon where individuals used social media to organize impromptu performances in public spaces).

[27] Margaret Rock, *Beyond Technology: How Flash Robs Cause Riots*, MOBILEDIA (Aug. 10, 2011), http://www.mobiledia.com/news/102144.html.

[28] *See* Malcolm Gladwell, *Small Change: Why the Revolution Will Not Be Tweeted*, NEW YORKER (Oct. 4, 2010), http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell?currentPage=all; Ramesh Srinivasan, *London, Egypt and the Nature of Social Media*, WASH. POST (Aug. 11, 2011), http://www.washingtonpost.com/national/on-innovations/london-egypt-and-the-complex-role-of-social-media/2011/08/11/gIQAIoud8I_story.html (arguing that the result of blaming social media for the recent social unrest is that "we ignore the powerful economic and political grievances that drive discontent").

[29] *See* Gladwell, *supra* note 28.

with social media takes the focus away from understanding the powerful social discontent that is driving revolution itself.[30]

¶14 Admittedly, it is a stretch to suggest that social media was the *cause* of the recent social unrest. However, critics will not be able to deny social media's ability to provide "real-time networked communication" that has helped fuel the revolutions.[31] According to Jared Cohen of Google Ideas, social media has been an "accelerant" on incipient revolutionary movements.[32] "[A]massing support, communicating with like-minded people, and spreading the word"—the most crucial elements of a protest—remain unchanged, but social media has expanded the available channels of communication to quickly convey beliefs that lead to a revolution.[33] In particular, social media has the unique ability to simplify and drastically reduce the time and costs of organizing a large group—a notoriously difficult task.[34] Certainly, the Egyptian government's unprecedented response of completely shutting down the Internet confirms its recognition of social media's capabilities.[35]

A. Facebook and Twitter

¶15 Facebook and Twitter as public forums have influenced the way in which the world views and understands the revolutions. In particular, the public forum created a "global watchdog" by permitting the world to watch protestors broadcast every moment of the revolution in real-time.[36] Indeed, though Facebook and Twitter may not have directly caused the revolutions in the Middle East, "the heat has never been turned up so quickly" for an authoritarian leader to step down as these social media platforms have "transferred the voice of international scrutiny from sovereign leaders to a community of millions."[37]

¶16 Moreover, Facebook and Twitter were crucial to Egypt's revolution because these new public forums allowed Egyptians to watch the revolution in Tunisia unfold, thereby providing the validation to identify themselves as part of a larger revolutionary

---

[30] *See* Caroline McCarthy, *There's No Such Thing as 'Social Media Revolution,'* CNET (Jan. 26, 2011, 4:00 AM), http://news.cnet.com/8301-13577_3-20029519-36.html?tag=mncol;txt.

[31] *See* Mathew Ingram, *It's Not Twitter or Facebook, It's the Power of the Network*, GIGAOM (Jan. 29, 2011, 4:47 PM), http://gigaom.com/2011/01/29/twitter-facebook-egypt-tunisia/ (arguing that due to the "power of the network," social media has played an incredibly important role in spreading the word and organizing protests).

[32] Doyle McManus, *Did Tweeting Topple Tunisia?*, L.A. TIMES (Jan. 23, 2011), http://articles.latimes.com/2011/jan/23/opinion/la-oe-mcmanus-column-tunisia-twitter-20110123 (noting that, though social media alone does not make a revolution, access to social media has empowered grass-roots movements by making it easier to identify each other and share information, both among themselves and with the outside world).

[33] McCarthy, *supra* note 30.

[34] Noah Feldman, *Twitter Can Start a Party but Can't Keep It Going: Noah Feldman*, BLOOMBERG (Oct. 2, 2011, 7:00 PM), http://www.bloomberg.com/news/2011-10-03/twitter-can-start-a-party-but-can-t-keep-it-going-noah-feldman.html.

[35] *See* David Kravets, *Amid Street Protests, Twitter Shuttered in Egypt*, WIRED (Jan. 25, 2011, 6:07 PM), http://www.wired.com/threatlevel/2011/01/twitter-revolution/ (The Mubarak administration's blocking Internet access "underscored the power of [Twitter] and other social networks as tools to both coordinate and disperse news of a citizen uprising.").

[36] *See* Caroline McCarthy, *Egypt, Twitter, and the Rise of the Watchdog Crowd*, CNET (Feb. 11, 2011, 2:12 PM), http://news.cnet.com/8301-13577_3-20031600-36.html.

[37] *See id*.

movement.[38] Social media's critical role in the Arab Spring was confirmed by a study that analyzed more than three million tweets and examined political conversations in the Tunisian blogosphere.[39] The study found that social media formed "transnational links" between international and local democratization movements as their stories circulated around the Arab region.[40] These new tools allowed leaders in neighboring regions to not only be inspired by the Tunisian revolution unfolding before their eyes, but they also helped those leaders learn effective strategies for successful organizing.[41]

B. Blackberry

¶17 In the aftermath of the London riots, BlackBerry was reported to be the social media platform that played the most substantive role in spreading the violence and looting because of its unique capabilities that allow its users to communicate both privately and instantaneously.[42]

¶18 BlackBerrys have recently become popular among the British youth, including members of urban gangs, in part because of the affordable handsets and free BlackBerry Messenger (BBM) network and in part because BBM allows them to be part of a much larger community.[43] Under the BBM service, once users exchange PINs, they are able to share messages to specific individuals or groups or to all of their contacts, [44] allowing information to spread not only instantaneously but also to a large amount of people.[45] Thus, BlackBerry provided a particularly effective organizational tool for inciting violence and looting as rioters used the BBM service to share the times and locations of riots, safe travel routes, and police activity.[46]

---

[38] *See* Ingram, *supra* note 17.

[39] *See* Philip N. Howard et al., *Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?* (Project on Info. Tech. & Political Islam, Working Paper No. 2011.1, 2011), *available at* http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

[40] *Id* at 23.

[41] *See id*.

[42] *See* James Ball & Symeon Brown, *Why BlackBerry Messenger Was Rioters' Communication Method of Choice*, GUARDIAN (Dec. 7, 2011, 10:00 AM), http://www.guardian.co.uk/uk/2011/dec/07/bbm-rioters-communication-method-choice; Melissa Bell, *In London Riots, BlackBerry Messenger Gets Starring Role*, WASH. POST (Aug. 9, 2011, 10:27 AM), http://www.washingtonpost.com/blogs/blogpost/post/in-london-riots-blackberry-messenger-gets-starring-role/2011/08/09/gIQAwxmW4I_blog.html; Olivia Solon, *Why Has BlackBerry Been Blamed for the London Riots?*, WIRED (Aug. 9, 2011, 10:06 AM), www.wired.com/business/2011/08/blackberry-london-riots/.

[43] *See* Halliday, *supra* note 18.

[44] *BlackBerry Messenger*, BLACKBERRY, http://us.blackberry.com/apps-software/blackberrymessenger/ (last visited Nov. 5, 2011) (BlackBerry Messenger is an instant messaging application only for BlackBerry phones. Users can "[s]end and receive messages in seconds, see when [their] contacts are typing, and know when [their] messages are delivered and read.").

[45] *See* Ball & Brown, *supra* note 42 ("Broadcasting on BBM was particularly effective in organising people on the streets and identifying targets with—as one rioter put it—'military precision.' The 'broadcast' feature allows users to instantly send the same piece of information to all their contacts, sometimes running into the hundreds."); Matthew Holehouse & David Millward, *How Technology Fuelled Britain's First 21st Century Riot*, TELEGRAPH (Aug. 8, 2011, 6:24 AM), http://www.telegraph.co.uk/news/uknews/crime/8687432/How-technology-fuelled-Britains-first-21st-century-riot.html.

[46] *See* Ball & Brown, *supra* note 42.

¶19 Furthermore, because the BBM network was originally intended for business communications where security is crucial, it provides a secure server that encrypts messages during transmission.[47] Thus, compared to Facebook and Twitter, where communications are public and can be monitored real-time by the police, BBM users are able to avoid government surveillance during communication.[48]

IV. SHUTTING DOWN SOCIAL MEDIA IN THE UNITED STATES

¶20 From shutting down the Internet in Egypt to blocking cellphone service in San Francisco, governments are faced with the repercussions of social media. While authorities in England are studying social media's role in fueling riots across the country, the United States government faces a reality that social media can incite violent mob behavior throughout the nation. If the United States finds itself in a position similar to the London riots, the government may arguably have the legal authority to carry out the British prime minister's proposition—to shut down social media platforms that are used to plan criminal activity.

A. Executive Power Under Youngstown and the Communications Act of 1934

¶21 The current state of the law does not directly address the scope of executive authority over the private sector to force a restriction on social media during a national security emergency.[49] In such a situation, the Supreme Court's majority opinion and concurrences in *Youngstown Sheet & Tube Co. v. Sawyer*[50] serve as guidance.[51]

¶22 In 1952, faced with an impending nationwide steelworkers' strike over the failure to settle a collective bargaining agreement dispute, President Harry S. Truman issued an Executive Order to ensure the continued operation of the steel mills.[52] Proclaiming "the existence of a national emergency" in the face of the United States' involvement in the Korean War, the Executive Order indicated that steel was "indispensable" to the United States, as a "work stoppage would immediately jeopardize and imperil [the] national defense . . . ."[53] President Truman invoked his authority "by the Constitution and laws of the United States" and as "President of the United States and Commander in Chief of the armed forces of the United States" to authorize the Secretary of Commerce "to take possession of all or such of the plants, facilities, and other property" of the steel mill companies that he deemed "necessary in the interests of national defense."[54]

---

[47] *See id*.

[48] *See id*; Peter Bright, *How the London Riots Showed Us Two Sides of Social Networking*, ARS TECHNICA (Aug. 10, 2011, 5:30 PM), http://arstechnica.com/tech-policy/2011/08/the-two-sides-of-social-networking-on-display-in-the-london-riots/ ("Unlike protestors campaigning for freedom and openness, for whom public visibility was important, privacy is a desirable characteristic for those engaged in criminality.").

[49] *See* John S. Fredland, *Building A Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies*, 206 MIL. L. REV. 1, 16 (2010).

[50] 343 U.S. 579 (1952).

[51] *See* Fredland, *supra* note 49, at 17.

[52] *Youngstown*, 343 U.S. at 582–83.

[53] *Id*. at 589–91.

[54] *Id*. at 591.

¶23 Justice Black delivered the majority opinion, ruling that President Truman did not have the authority to issue the Executive Order.[55] Justice Black dismissed the government's argument that the President's Commander in Chief powers supported the seizure, distinguishing "military commanders engaged in day-to-day fighting in a theater of war" from taking "possession of private property in order to keep labor disputes from stopping production."[56]

¶24 In his concurrence, Justice Jackson provided a three-pronged framework for evaluating the constitutionality of executive decision-making.[57] The framework provides that the executive power is at its "maximum" when the President acts with express or implied congressional authorization,[58] at its "lowest ebb" when he acts contrary to express or implied congressional will,[59] and in a "zone of twilight" when Congress is silent and the President and Congress have concurrent authority or the distribution of authority is uncertain.[60] Justice Jackson ultimately concluded that President Truman's seizure was in the lowest ebb of executive power, thereby justifying the judicial invalidation of the Executive Order.[61]

¶25 Applying the *Youngstown* framework, the President may have the legal authority to use the Communications Act of 1934[62] to temporarily shut down social media.[63] In fact, the Obama administration has acknowledged in public testimony that section 706 of the Act, codified at 47 U.S.C. § 606, already provides the Executive Branch sufficient emergency authority to take "extraordinary measures" when there are "imminent cyber threats."[64]

¶26 Section 706 of the Act provides the President with broad emergency powers when he declares that there is a "national emergency":

> Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all

---

[55] *Id*. at 589.

[56] *Id* at 587.

[57] *Id*. at 635 (Jackson, J., concurring).

[58] *Id*. "A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it." *Id*. at 637.

[59] *Id* at 637. In this situation, actions "must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system." *Id.* at 638.

[60] *Id*. at 637. Here, "[a]ny actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law." *Id.*

[61] *Id*. at 640.

[62] Communications Act of 1934, 47 U.S.C. § 606 (1934).

[63] *See* Thompson, *supra* note 1, at 478–79.

[64] *Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 111th Cong. (2010), *available at* http://www.hsgac.senate.gov/download/2010-06-15-reitinger-testimony (statement of Philip Reitinger, Deputy Under Secretary, National Protection & Programs Directorate, Department of Homeland Security) ("Section 706 of the Communications Act and other laws already address Presidential emergency authorities and Congress and the Administration should work together to identify any needed adjustments to the Act, as opposed to developing overlapping legislation.").

> stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States . . . .[65]

¶27 Accordingly, under the *Youngstown* framework, section 706 puts the executive power at its apex because the President is acting "pursuant to an express or implied authorization of Congress."[66] Thus, the President only needs to declare that a threat of "national emergency" exists in order to exercise the legal authority to suspend social media.[67] Moreover, it is reasonably foreseeable that a President could make such a declaration if violent rioting and looting was widespread across the United States.[68]

¶28 On the other hand, it is arguable whether threatened or actual protests, or even riots similar to those recently seen in London, rise to the level of a "national emergency" meriting the suspension of electronic communications platforms. If not, the situation may be in Justice Jackson's "zone of twilight" where "any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law."[69]

¶29 Although Justice Jackson's concurrence may suggest that the Executive branch has authority to exercise some control over private entities in certain circumstances, the degree to which the President can exercise that power is unclear. Thus, *Youngstown* itself ultimately provides inconclusive guidance on Executive power during a national emergency similar to the London riots.

B. Current Litigation—Kill Switch

¶30 Recent cybersecurity legislative proposals have unsuccessfully attempted to grant the President a so-called "Internet kill switch"—the power to shut down or limit public access to the Internet during a national cyber emergency.[70] The term "Internet kill switch"[71] originally referred to the Protecting Cyberspace as a National Asset Act of 2010 (PCNAA),[72] which was introduced on June 24, 2010, by Senators Joseph Lieberman, Susan Collins, and Thomas Carper.[73] The PCNAA would have granted the President emergency powers over the Internet, including the power to declare a "national cyber emergency."[74] In such a scenario, private owners and operators of "critical

---

[65] 47 U.S.C. § 606(c).

[66] *See Youngstown*, 343 U.S. at 635 (Jackson, J., concurring). "A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it." *Id*. at 637.

[67] Thompson, *supra* note 1, at 478–79.

[68] *See Id.*

[69] *See Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

[70] *See* Jon Orlin, *In Search of the Internet Kill Switch*, TECHCRUNCH (Mar. 6, 2011), http://techcrunch.com/2011/03/06/in-search-of-the-internet-kill-switch/.

[71] Even though the bill did not have the words "kill" and "switch," the PCNAA became known as the "Internet kill switch" because it gave the President sweeping provisions to control the Internet, including the ability to shut it down. *See id*.

[72] Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. (2010).

[73] *Id*.

[74] *Id*. § 249(a)(1) ("The President may issue a declaration of a national cyber emergency to covered critical infrastructure if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation

infrastructure" would be forced to "immediately comply with any emergency measure or action developed" by the Department of Homeland Security.[75]

¶31 In response to the PCNAA, about two dozen groups, including the American Civil Liberties Union (ACLU), filed an open letter to Senators Lieberman, Collins, and Carper opposing the proposal.[76] In particular, the ACLU expressed First Amendment concerns that the "emergency actions that could be compelled could include shutting down or limiting Internet communications that might be carried over covered critical infrastructure systems."[77]

¶32 In 2011, shortly after the Egyptian government blocked its citizens from Internet access, a modified PCNAA was reintroduced to Congress as the Cybersecurity and Internet Freedom Act of 2011 (CIFA).[78] With the name of the bill now adding the phrase "Internet Freedom," CIFA made several additions to alleviate the concerns of civil liberty groups, including the explicit provision that "neither the President, the Director of the National Center for Cybersecurity and Communications, or any officer or employee of the United States Government shall have the authority to shut down the Internet,"[79] and that the government "must not encroach on rights guaranteed by the First Amendment to the Constitution of the United States."[80] The new bill added substantial limitations absent from the PCNAA, including limiting the duration of a "national cyber emergency" to thirty days from the date of a presidential declaration.[81] In addition, under CIFA, Homeland Security was tasked to "establish and maintain a list of systems or assets that constitute covered critical infrastructure" based on a number of factors.[82] Only this "covered critical infrastructure" would be obligated to comply with emergency measures when the President declares a national cyber emergency.[83]

¶33 However, the new CIFA still preserved the presidential emergency power provisions of PCNAA.[84] Following such declaration, Homeland Security is authorized to direct critical infrastructure owners and operators to "immediately comply with any emergency measure or action."[85]

¶34 CIFA continues to raise concerns among civil liberties groups and critics, as the proposed legislation would allow the government to restrict access to certain web content.[86] The Electronic Frontier Foundation expressed concern that "[t]he president

---

of the information infrastructure essential to the reliable operation of covered critical infrastructure.").

[75] *Id.* § 249(c)(1).

[76] Letter from American Civil Liberties Union et al. to Senators Lieberman, Collins and Carper (June 23, 2010), *available at* http://www.cdt.org/files/pdfs/20100624_joint_cybersec_letter.pdf.

[77] *Id.*

[78] Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

[79] *Id.* § 2(c).

[80] *Id.* § 2(b)(5).

[81] *See id.* § 249(b).

[82] *Id.* § 254(a)(1).

[83] *See id.* § 249(c).

[84] *See id.* § 249(a)(1) ("The President may issue a declaration of a national cyber emergency to covered critical infrastructure if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure.").

[85] *Id.* § 249(c)(1).

[86] *See, e.g.*, Declan McCullagh, *Internet 'Kill Switch' Bill Gets a Makeover*, CNET (Feb. 18, 2011), http://news.cnet.com/8301-31921_3-20033717-281.html?part=rss&subj=news&tag=2547-1_3-0-20; *see also* Meredith Jessup, *Committee Passes Plan for Internet 'Kill Switch' in ~~Egypt~~ - U.S.*, BLAZE (Jan. 29,

would have essentially unchecked power to determine what services can be connected to the Internet or even what content can pass over the Internet in a cybersecurity emergency."[87] The ACLU agreed that the modified proposal "still gives the president incredible authority to interfere with Internet communications."[88]

¶35 The bill was referred to the Committee on Homeland Security and Governmental Affairs in February of 2011.[89] As of May 2011, committee hearings had been held, but no major action has occurred since then.[90]

¶36 The Cybersecurity Act of 2012[91] was introduced on February 15, 2012, "[t]o enhance the security and resiliency of the cyber and communications infrastructure of the United States."[92] This latest version eliminates language that authorizes the President to declare a cyber emergency.[93] On July 19, 2012, after considerable negotiation, a revised version of the Cybersecurity Act of 2012[94] was introduced in a good faith effort to address the concerns of the bill's opponents.[95] The legislation gave Homeland Security the authority to intercept communications transiting federal networks, create mechanisms for more information sharing between government and the private sector, and set voluntary cybersecurity standards for companies that operate critical infrastructure.[96]

¶37 Despite President Obama's op-ed[97] advising Congress to pass the bill, on August 2, 2012, the Senate voted 52-46, falling short of the required 60 votes to invoke cloture.[98] The cybersecurity legislation failed in the Senate for a second time when a procedural motion to move the Cybersecurity Act forward was rejected 51-47 on November 14, 2012.[99]

2011, 1:52 PM), http://www.theblaze.com/stories/committee-passes-plan-for-internet-kill-switch-in-egypt-u-s/.

[87] McCullagh, *supra* note 866.

[88] *Id.*

[89] *Bill Summary & Status, 112th Congress (2011-2012), S. 413*, LIBRARY OF CONGRESS, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00413:@@@L&summ2=m& (last visited Apr. 5, 2012).

[90] *Protecting Cyberspace: Assessing the White House Proposal: Hearing Before the S. Comm. on Homeland Sec. and Governmental Affairs*, 112th Cong. (2011), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg67638/pdf/CHRG-112shrg67638.pdf.

[91] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012).

[92] *Id.*

[93] *See* 158 CONG. REC. S617 (daily ed. Feb. 14, 2012) (statement of Sen. Joseph Lieberman) ("One myth about this bill is that it contains a kill switch that would allow the President of the United States in an emergency to seize control of the Internet. There is nothing remotely like that in this bill.").

[94] Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012).

[95] *Lieberman, Collins, Rockefeller, Feinstein, Carper Offer Revised Legislation to Improve Security of Our Most Critical Private-Sector Cyber Systems*, U.S. SENATE COMMITTEE ON HOMELAND SEC. & GOVERNMENTAL AFF. (July 19, 2012), http://www.hsgac.senate.gov/media/majority-media/lieberman-collins-rockefeller-feinstein-carper_offer-revised-legislation-to-improve-security---of-our-most-critical-private-sector-cyber-systems-.

[96] Siobhan Gorman, *Cybersecurity Bill Blocked as Hopes Dim for Compromise*, WALL ST. J. (Aug. 2, 2012, 7:41 PM), http://online.wsj.com/article/SB10000872396390443866404577565121771512102.html.

[97] Barack Obama, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://online.wsj.com/article/SB10000872396390444330904577535492693044650.html.

[98] *See* U.S. Senate Roll Call Votes 112th Congress – 2nd Session, U.S. SENATE, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=2&vote=00187 (last visited Apr. 5, 2012).

[99] *See* U.S. Senate Roll Call Votes 112th Congress – 2nd Session, U.S. SENATE, http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=2&vote=00202 (last visited Apr. 25, 2013); Josh Smith, *Cybersecurity Bill Fails to Advance in Senate, Again*, NAT'L J. (Nov. 14, 2012, 6:20 PM), http://www.nationaljournal.com/tech/cybersecurity-bill-fails-to-

C. Executive Order

¶38 On July 6, 2012, President Obama signed an Executive Order stating that "[t]he Federal Government must have the ability to communicate at all times and under all circumstances to carry out its most critical and time sensitive missions."[100] The order lays out guidelines that government agencies must follow to maintain communication networks during natural disasters and security emergency.[101] However, there has been concern over Section 5.2 of this order, which authorizes Homeland Security to "'oversee the development, testing, implementation, and sustainment'" of emergency measures on "'non-military communications networks,'" including private systems.[102] Skeptics fear that this clause authorizes the government to seize control of all wired and wireless communications in the United States during a national emergency, thereby giving the President "'control over the internet'" beyond the nation's needs in such extreme circumstances.[103] White House officials have responded by explaining that the new order merely updates an executive order signed in 1984 to reflect modern communications technology.[104] They claimed that the order does not expand the government's authority.[105]

V. IMPACT OF SHUTTING DOWN SOCIAL MEDIA

¶39 Governments that have faced social unrest enabled by social media have reacted by restricting social media in hopes of stopping the protests, but their actions have caused disastrous problems in the short-term and pose long-term consequences.

A. First Amendment Violations

¶40 Although the government may have the legal authority to temporarily shut down social media platforms under specific and limited circumstances, difficulty arises in striking the right balance between the government's obligation to preserve public safety with an individual's First Amendment right to expression. After the recent decision by BART officials to shut down underground cellphone service and restrict social media access,[106] BART officials justified their actions as an attempt to protect public safety[107]:

---

advance-in-senate-again-20121114.

[100] Exec. Order No. 13,618, 3 C.F.R. 273 (2013).

[101] *See* Dara Kerr, *Obama Signs Order Outlining Emergency Internet Control*, CNET (July 10, 2012, 9:43 PM), http://news.cnet.com/8301-1023_3-57469950-93/obama-signs-order-outlining-emergency-internet-control; Adi Robertson, *Obama Clarifies Plan to Keep the Internet Running During Emergencies in Executive Order*, VERGE (July 10, 2012, 5:29 PM), http://www.theverge.com/2012/7/10/3149831/obama-national-security-emergency-preparedness-internet-order.

[102] Kerr, *supra* note 101.

[103] *See* Robertson, *supra* note 101.

[104] Eamon Javers, *Obama's Internet Order: Power Grab or Simple Update?*, CNBC (July 11, 2011, 4:15 PM), http://www.cnbc.com/id/48151460/Obama039s_Internet_Order_Power_Grab_or_Simple_Update.

[105] *Id.*

[106] *See supra* Part II.C.1.

[107] *See* Letter from Bob Franklin, BART Board of Directors President, to BART Customers (Aug. 20, 2011), http://www.bart.gov/news/articles/2011/news20110820.aspx.

> To protect public safety and provide safe and efficient public transportation, BART has restricted access to the "Paid" and "Platform" areas of its stations to BART station employees and ticketed passengers who are boarding, exiting or waiting for BART trains. BART's temporary interruption of cell phone service was not intended to and did not affect any First Amendment rights of any person to protest in a lawful manner in areas at BART stations that are open for expressive activity. The interruption did prevent the planned coordination of illegal activity on the BART platforms, and the resulting threat to public safety.[108]

¶41 Despite the fact that, following the action, no protests were held at BART stations and no injuries resulted, BART's unprecedented actions[109] drew heavy criticism from civil rights activists.[110] The ACLU expressed their concern that a government's ability to shut down an entire communications network because it does not agree with the content is an "insult to our constitutional protections for free speech."[111] The ACLU sent a letter to BART officials arguing that, based on a First Amendment analysis, BART's action restricting all access to mobile communication was an unconstitutional reaction to passenger safety concerns.[112] The ACLU argued that "speech does not lose its protection merely because it may lead indirectly to disruption."[113]

¶42 First Amendment scholars agree. Gene Policinski, executive director of the First Amendment Center at Vanderbilt University, says, although the "[g]overnment can legitimately stop speech for public safety purposes," they cannot do so on "mere speculation."[114] Rita Kirk, director of the Cary M. Maguire Center for Ethics and Public Responsibility at Southern Methodist University, said "[t]he BART action to restrict free speech so that the actions of a few could be curtailed is not warranted."[115]

¶43 Moreover, consumer advocates and digital civil-rights groups have filed an emergency petition with the Federal Communications Commission (FCC), asking them

---

[108] *Id.*

[109] According to the ACLU, BART is the first known United States government agency to block cell service for the purposes of disrupting a political protest. Nicole Ozer, *No More Cell Phone Censorship on BART*, ACLU (Aug. 15, 2011, 3:15 PM), http://www.aclunc.org/issues/technology/blog/no_more_cell_phone_censorship_on_bart.shtml.

[110] *See* Terry Collins, *BART Cell Phone Shutdown: Safety Issue or Free Speech Violation?*, HUFFINGTON POST (Oct. 15, 2011, 6:12 AM), http://www.huffingtonpost.com/2011/08/15/bart-cell-phone-shutdown-free-speech_n_927294.html; *see also* Eva Galperin, *BART Pulls a Mubarak in San Francisco*, ELECTRONIC FRONTIER FOUND. (Aug. 12, 2011), http://www.eff.org/deeplinks/2011/08/bart-pulls-mubarak-san-francisco. In light of the recent events in Egypt, critics were quick to draw comparisons between BART's "shameful attack on free speech" to that of the former Egyptian president, Hosni Mubarak, who ordered a similar shutdown of cell phone service in response to peaceful, democratic protests. *Id.*

[111] Ozer, *supra* note 109.

[112] Letter from Abdi Soltani, Exec. Dir., ACLU of Northern Cal. & Alan Schlosser, Legal Dir., ACLU of Northern Cal., to Kenton Rainey, Chief of Police, BART (Aug. 15, 2011), *available at* https://www.aclunc.org/issues/technology/blog/asset_upload_file335_10381.pdf.

[113] *Id.*

[114] Patrik Johnsson, *To Defuse "Flash" Protest, BART Cuts Riders' Cell Service. Is That Legal?*, CHRISTIAN SCI. MONITOR (Aug. 12, 2011), http://www.csmonitor.com/USA/Justice/2011/0812/To-defuse-flash-protest-BART-cuts-riders-cell-service.-Is-that-legal.

[115] Daniel B. Wood, *BART Puts Social Media Crackdown in "Uncharted" Legal Territory*, CHRISTIAN SCI. MONITOR (Aug. 16, 2011), http://www.csmonitor.com/USA/Justice/2011/0816/BART-puts-social-media-crackdown-in-uncharted-legal-territory/%28page%29/2.

to investigate BART's actions and declare that local law enforcement lacks the authority to wholly deny or suspend communication services.[116]

¶44 In response to outcry from civil liberties groups, BART's board members adopted the Cell Service Interruption Policy[117] in December of 2011.[118] The BART board adopted a policy where BART would have the authority to temporarily interrupt cell phone service when it "determines that there is strong evidence of imminent unlawful activity that threatens the safety of District passengers, employees and other members of the public . . . ."[119] Though the policy is not without problems,[120] a BART spokeswoman indicated that under the new policy, in a situation similar to that of August 2011, BART would not have shut down the cell phone service.[121]

¶45 With the FCC reviewing whether BART can intentionally interrupt Internet and cell phone services in anticipation of protests,[122] such actions raise serious constitutional and policy issues.

B. Economic Consequences

¶46 In addition to raising civil liberty concerns, shutting down the Internet, even temporarily, may result in severe economic consequences as highlighted by the experiences in Egypt. In the wake of the Egyptian government shutting down the Internet, James Cowie of Renesys, a New Hampshire-based firm that tracks Internet traffic, wrote, "[e]very Egyptian provider, every business, bank, Internet cafe, website, school, embassy, and government office that relied on the big four Egyptian [Internet Service Providers] for their Internet connectivity is now cut off from the rest of the world."[123]

¶47 The Organization for Economic Cooperation and Development (OECD) reported that Egypt will experience a pronounced economic impact as a result of its actions.[124] The OECD estimated that Egypt had incurred costs of at least $90 million (3–4% of GDP) from lost revenues as a result of shutting down telecommunications and Internet services for five days, accounting for approximately $18 million per day).[125] In addition, they predicted that Egypt will face long-term economic impacts from the loss of business

---

[116] *Petition to FCC to Declare BART Actions Unlawful*, CENTER FOR DEMOCRACY AND TECH. (Aug. 29, 2011), http://www.cdt.org/report/petition-fcc-declare-bart-actions-unlawful.

[117] *Cell Service Interruption Policy*, BAY AREA RAPID TRANSIT, http://www.bart.gov/docs/final_CSIP.pdf (last visited July 29, 2013).

[118] *Extraordinary Circumstances Only for Cell Phone Interruptions*, BAY AREA RAPID TRANSIT (Dec. 1, 2011), http://www.bart.gov/news/articles/2011/news20111201.aspx.

[119] *Cell Service Interruption Policy*, *supra* note 117.

[120] *See* Parker Higgins, *BART's Cell Phone Shutdown, One Year Later*, ELECTRONIC FRONTIER FOUND. (Aug. 13, 2012), http://www.eff.org/deeplinks/2012/08/barts-cell-phone-shutdown-one-year-later (arguing that BART could abuse the policy's vague language to limit speech without real justification).

[121] Edward Wyatt, *F.C.C. Asks for Guidance on Whether, and When, to Cut Off Cellphone Service*, N.Y. TIMES (Mar. 2, 2012), http://www.nytimes.com/2012/03/03/technology/fcc-reviews-need-for-rules-to-interrupt-wireless-service.html?_r=0.

[122] *Id.*

[123] Dan Costa, *Egypt Flips Internet Kill Switch. Will the U.S.?*, PCMAG.COM (Jan. 28, 2011), http://www.pcmag.com/article2/0,2817,2376905,00.asp.

[124] *The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt*, ORG. FOR ECON. CO-OPERATION AND DEV. (Feb. 4, 2011), http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html.

[125] *Id.*

in other sectors affected by the blocked communication services, including IT services and the tourism sector.[126]

¶48 Compared to Egypt, the United States economy is arguably much more dependent on, and intertwined with, Internet-based services, which would make restrictions on the free flow of information even more dangerous.[127] This means that beyond the loss of e-commerce revenue, an Internet shutdown could hamper any business that operates any part of their supply chain through networking technology.[128]

¶49 Some suggest that the United States economy is flexible enough to absorb the costs of a temporary shutdown of the Internet similar to that in Egypt.[129] However, a larger risk exists of the government losing credibility with vital private entities. For example, Google recently closed its Internet search service in China partially because of the Chinese government's censorship of Internet content.[130] Google's retreat is telling because they have rejected China's Internet censorship even at the risk of having "essentially turn[ed] its back on the world's largest Internet market."[131] This is not to suggest that Google would remove its services from the United States in the event of a temporary Internet shutdown. Rather, this example highlights the fact that as businesses decide whether or not they will enter or continue in countries where access to the Internet could potentially be restricted, the United States economy risks losing such private entities if it decides to exercise control over the Internet.

C. Setting Dangerous Precedent

¶50 Shutting down social media in the United States not only undermines the country's efforts to promote democracy, but it also sets a dangerous precedent for authoritarian governments. Restricting Internet access detracts from the United States government's worldwide efforts to establish a network of organizations that could thwart authoritarian foreign governments' restrictions on the Internet.[132] As part of the Obama administration's drive to protect universal human rights, the State Department has been working to keep the Internet open by pressuring Arab governments to end their restrictions on social media.[133] As former Secretary of State Hillary Clinton laid out in her speech on Internet freedom, the United States is committed to ensuring that the "[I]nternet remains a space where activities of all kinds can take place," and is "open for the protestor using social media to organize a march in Egypt."[134]

---

[126] *Id*.

[127] *See* Jeremy Hsu, *U.S. Internet Shutdown Would "Paralyze the Economy"*, TECHNEWSDAILY (Jan. 31, 2011, 2:26 PM), http://www.technewsdaily.com/1973-internet-shutdown-economy-impact-110131html.html.

[128] *Id*.

[129] *Id*.

[130] Miguel Helft & David Barboza, *Google Shuts China Site in Dispute Over Censorship*, N.Y. TIMES (Mar. 22, 2010), http://www.nytimes.com/2010/03/23/technology/23google.html.

[131] *See id*.

[132] *See* Josh Rogin, *Inside the State Department's Arab Twitter Diplomacy*, FOREIGN POL'Y. (Jan. 28, 2011, 7:16 PM), http://thecable.foreignpolicy.com/posts/2011/01/28/inside_the_state_department_s_arab_twitter_diplomacy.

[133] *Id*.

[134] Hillary Rodham Clinton, Secretary of State, Internet Rights and Wrongs: Choices & Challenges in a Networked World, Remarks at George Washington University (Feb. 15, 2011), http://www.state.gov/secretary/rm/2011/02/156619.htm.

¶51 In fact, following Egypt's Internet shutdown, the State Department criticized Mubarak for his interference in digital communication, culminating with Secretary of State Hillary Clinton's public statement, "[w]e urge the Egyptian authorities to allow peaceful protests and to reverse the unprecedented steps it has taken to cut off communications."[135] As Queensland University of Technology associate professor Axel Bruns writes, "[c]racking down on social media at home while promoting it as a tool for democracy abroad simply doesn't make sense."[136]

¶52 Moreover, any measures to remove Internet freedoms will validate the Egyptian government's action of shutting down the Internet and affirm the Chinese government's continued Internet censorship. If the United States decides to shut down social media, these oppressive governments will quickly point to such behavior to justify their own repressive policies.[137] Governments around the world are waiting to see how the West will react to the challenges posed by the Internet so that they can "claim an international license for dealing with their own protests."[138] Thus, the domestic challenges posed by the Internet demand a "measured, cautious response" in the United States because their actions will likely affect the political behavior of foreign governments.[139]

D. Restricting Social Media is Ineffective

¶53 Despite efforts to restrict access to social media in the face of social unrest, such limitations may prove to be ineffective at fully stifling communications by protestors. This was the case in Egypt where the government's strategy of shutting down the Internet was not enough to stop the Egyptian people from sharing information to organize and mobilize in opposition.[140] In fact, the protests continued in spite of the Internet shutdown.[141] Activists used circumvention software to access blocked Twitter accounts and landlines to call friends abroad to tweet on their behalf.[142] When cell phone service was disrupted, people organized through word of mouth and by physically coming together, and they communicated with the world through dial-up modems and fax machines.[143] If anything, by shutting down the Internet, the Egyptian government increased the protestors' engagement in the uprisings by indicating just how "thuggish" it

---

[135] *Egypt Protests: Hillary Clinton's Statement in Full*, TELEGRAPH (Jan. 28, 2011, 5:51 PM GMT), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8289419/Egypt-protests-Hillary-Clintons-statement-in-full.html.

[136] Axel Bruns, *Don't Shoot the Instant Messenger: David Cameron's Social Media Shutdown Plan Won't Stop UK Riots*, CONVERSATION (Aug. 13, 2011, 4:03 PM), http://theconversation.edu.au/dont-shoot-the-instant-messenger-david-camerons-social-media-shutdown-plan-wont-stop-uk-riots-2854 (criticizing Prime Minister Cameron's proposal to limit social media during times of social unrest).

[137] *See* Jim Killock, *Prime Minister's Attack on Social Media Unwarranted*, OPEN RIGHTS GROUP (Aug. 11, 2011), http://www.openrightsgroup.org/blog/2011/david-cameron (criticizing a statement by Prime Minister David Cameron and discussing problems with the UK potentially imposing limitations on the Internet).

[138] Evgeny Morozov, *Repressing the Internet, Western-Style*, WALL ST. J. (Aug. 13, 2011), http://online.wsj.com/article/SB10001424053111903918104576502214236127064.html.

[139] *Id*.

[140] *See* Dunn, *supra* note 11, at 19–20.

[141] *Id* at 20.

[142] *Id* at 21

[143] *Id*.

could be.[144] Most importantly, the government-placed limitations on the ability to communicate openly ultimately proved ineffective as Mubarak was eventually forced to resign.[145]

VI. A PREVENTATIVE RESPONSE

¶54 In light of the wave of social and political unrest that have occurred across the world, the United States must take a preventative approach. This requires the federal government to take action before any social uprisings occur so that it is well-equipped to contain them in the future.

A. Private-Public Partnership

¶55 In the aftermath of the London riots, the British government retreated from its initial position considering shutting down social media to stop individuals who are plotting violence on the platforms.[146] Instead, the Home Office had a "constructive" meeting with representatives of Facebook, Twitter, and BlackBerry where they discussed "how law enforcement and the networks can build on the existing relationships and cooperation to crack down on the networks being used for criminal behaviour."[147] The UK Home Office took a step in the right direction by acknowledging the importance of a private-public partnership to respond to national crises where social media is used to promote criminal behavior.

¶56 As seen in Egypt, activists' technological knowledge regarding the use of "circumvention and anonymity technology" will inevitably outpace the government.[148] Therefore, it is imperative to partner law enforcement agencies with social media companies to explore the different measures that each could take to help prevent or contain impending disorder.

¶57 The Google-NSA alliance is a good example of a productive private-public partnership. On February 4, 2010, Google and the National Security Agency (NSA) partnered to assist Google and its users to better defend against future cyberattacks.[149] This alliance allows the NSA to use its expertise—analyzing "cyber-'signatures'" in previous attacks to defend against future intrusions—to help Google evaluate its hardware and software vulnerabilities.[150] Google, in turn, shares details regarding the malicious code used to attack its system, without violating Google's policies or laws that protect the privacy of online communications.[151] The rationale behind this public-private partnership was rooted in understanding that the critical infrastructure of the United

---

[144] *See* Costa, *supra* note 123.

[145] *See* Dunn, *supra* note 11, at 21–22.

[146] *See Social Media Talks About Rioting 'Constructive,'* BBC NEWS (Aug. 25, 2011, 11:31 AM), http://www.bbc.co.uk/news/uk-14657456.

[147] *'Constructive' Social Media Meeting*, HOME OFFICE (Aug. 25, 2011), http://www.homeoffice.gov.uk/media-centre/news/constructive-meeting.

[148] *See* Dunn, *supra* note 11, at 16.

[149] Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, WASH. POST (Feb. 4, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

[150] *Id*.

[151] *Id*.

States is best protected through a collaborative relationship between the public and private sectors.[152]

¶58 Similarly, prior to any civil unrest, the federal government must reach out to social media companies to form a collaborative partnership. The government, for its part, should use its expertise in pushing for freedom in communication by defending United States-based social media companies like Facebook and Twitter so that they are not subject to oppressive governments who restrict social media in times of social unrest. On the other hand, social media companies like Facebook should do their part by being more active in reporting pages or groups that are inciting disorder, while Twitter should enhance its efforts to prevent postings of violence-related tweets.[153]

¶59 In addition, once civil disorder has broken out, Facebook, Twitter, and other similar social media companies should be open to working closely with law enforcement to track riots and obtain real-time data that could help contain the violence, although they should not be required to go so far as giving the government privileged access to their networks.[154] At the same time, it is also very important to educate the public to effectively report civil disorder brewing on social networks.[155]

B. Recognizing the Value of Social Media

¶60 Before hastily reacting to social unrest by restricting social media access, it is important for the United States to first recognize and appreciate the value of social media during times of crisis. During the London riots, much was made of social media's power to incite disruption on such a wide-scale;[156] yet, its ability to bring order was equally important—at the height of the rioting and looting, law enforcement used social media such as Twitter to update citizens with accurate information and to dispel rumors.[157] In addition, even while the riots continued overnight, the very tools that police claimed rioters used to help organize violence were being used to organize hundreds of volunteers to clean up the damage.[158] The public also took to social media platforms including Facebook, Tumblr and Flickr to post photos and videos of suspected looters to help law enforcement identify the culprits.[159] Thus, for London, the information the police gathered by keeping social media running during the riots played a substantial role in eventually containing the riots.

---

[152] *See* Stephanie A. DeVos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 173, 215 (2011).

[153] *See* Dan Sabbagh, *UK Riots: The Questions Social Media Giants Need to Answer*, GUARDIAN (Aug. 24, 2011, 8:11 AM), http://www.guardian.co.uk/media/2011/aug/24/uk-riots-social-media.

[154] *See id*.

[155] *See England Riots*, *supra* note 19.

[156] See *supra* Part III.

[157] *See* Kelly Fiveash, *Keep Calm and Carry On Networking, Says UK.gov*, REGISTER (Aug. 25, 2011, 3:58 PM), http://www.theregister.co.uk/2011/08/25/twitter_blackberry_facebook_home_office.

[158] Jill Lawless, *Tottenham Riots: Social Networks Help Organizing Cleanup*, HUFFINGTON POST (Aug. 9, 2011, 1:43 PM), http://www.huffingtonpost.com/2011/08/09/tottenham-riots-social-networks_n_922273.html.

[159] Parmy Olson, *Londoners Use Facebook, Tumblr, Flickr To 'Catch Rioters,'* FORBES (Aug. 9, 2011, 8:34 AM), http://www.forbes.com/sites/parmyolson/2011/08/09/londoners-use-facebook-tumblr-flickr-to-catch-rioters/.

¶61 Recognizing social media's positive role during times of social unrest is important because the United States can now shift policy efforts from shutting down social media to finding more effective ways of using the platforms.[160] Harnessing social media's potential will enable law enforcement to respond more quickly and provide the public with vital information regarding safety and emergency services.[161]

C. Enhance Law Enforcement's Capabilities to Anticipate and Quickly Respond to Violent Disorder

¶62 It is equally important to ensure that law enforcement officers are equipped with the necessary technological resources not only to respond to the threats but also to extract valuable information from social networks. After the London riots, the Metropolitan police acknowledged that they "'needed to do more'" to understand how to effectively use social media, admitting that they were "'slightly behind'" when it came to Twitter and Facebook.[162] Richard Allan, Facebook's director of public policy in Europe, stated that the London police "'need to create new mechanisms to catch up with social media.'"[163]

¶63 Recently, the United States took steps in the right direction as the Department of Homeland Security announced that it is currently developing guidelines on gathering information for law enforcement purposes from social media sites such as Twitter and Facebook.[164] Undersecretary Caryn Wagner assured that the protocols are "being developed under strict laws meant to prevent spying on U.S. citizens and protect privacy, including rules dictating the length of time the information can be stored and differences between domestic and international surveillance."[165] In this newly emerging issue, the challenge lies not only in developing guidelines for collecting the information but also in ensuring that the information is analyzed to provide meaningful intelligence.[166]

¶64 The New York Police Department (NYPD) has recognized the importance of enhancing law enforcement's capability to effectively use social media to respond to criminal activities.[167] They have formed a new unit specifically to monitor social media sites like Twitter and Facebook for information regarding planned crimes so as to anticipate such criminal activity.[168] In addition, the new unit will look for postings, photos, and videos of crimes that have already been committed to prevent perpetrators from repeating their criminal activities.[169] The NYPD unit intends to educate its officers

---

[160] *See* Bruns, *supra* note 136.

[161] *See id*.

[162] Josh Halliday, *Government Backs Down on Plan to Shut Twitter and Facebook in Crises*, GUARDIAN (Aug. 25, 2011, 5:14 PM), http://www.guardian.co.uk/media/2011/aug/25/government-plan-shut-twitter-facebook.

[163] Tim Bradshaw, *Social Media Play Down Role in Riots*, FIN. TIMES (Sept. 15, 2011, 3:08 PM), http://www.ft.com/intl/cms/s/0/e52ea3f8-df9c-11e0-845a-00144feabdc0.html#axzz1cuB2k4IB.

[164] P. Solomon Banda, *Homeland Security Reviews Social Media Guidelines*, YAHOO! NEWS (Nov. 1, 2011), http://news.yahoo.com/homeland-security-reviews-social-media-guidelines-031146066.html.

[165] *Id*.

[166] *See id*.

[167] *See* Forbes Mobiledia Staff, *NYPD to Scan Facebook, Twitter for Trouble*, YAHOO! NEWS (Aug. 11, 2011), http://news.yahoo.com/nypd-scan-facebook-twitter-trouble-190941500.html.

[168] *Id*.

[169] *See id*.

not only about Facebook and Twitter but also about BBM, the encryption of which makes it difficult for the police to anticipate criminal activity.[170]

¶65 Moreover, there may be opportunities to develop technology that employs social media to identify and help prevent dangerous incidents from occurring. During Nigeria's presidential election last April, Michael Best, a Georgia Tech Associate Professor, and his team of researchers designed an aggregator tool for a Nigerian group that sought to use social media to track the election process and identify any potential problems.[171] The social media aggregator tool received information from different social media sources and analyzed the data in real time using keywords.[172] Best's team used social media to measure public response to political events in real time to help improve the electoral process.[173] Thus, if violence erupted during or immediately after the Nigerian election, the time saved by having identified the situation in real time could significantly improve law enforcement's ability to respond promptly.[174]

¶66 One can imagine a similar aggregator tool that analyzes information from different social media platforms in real time to improve law enforcement's ability to respond to violent riots like those in London or in localized situations like flash robs. It would be particularly advantageous in an environment where the potential for violence or unrest is high.

VII. CONCLUSION

¶67 The advent of social media and its ability to fuel social unrest has empowered people around the world to successfully challenge their oppressive governments. However, as the very qualities of social media that promote unprecedented political progress—"its openness, its leveling effect, its reach and speed"—are used to further incite criminal civil disorder, it is critical for the government to employ strategies to quickly respond to such threats without compromising the United States' commitment to a policy of an open Internet.[175]

¶68 Similar to authoritarian governments that have impulsively responded to civil unrest with repressive policies of restricting Internet access, the United States may have the legal authority to take a repressive approach. However, such a response would be at the expense of civil liberties, severe economic consequences, and setting dangerous precedents. Moreover, it may ultimately prove ineffective.

¶69 Thus, the United States should employ a preventative strategy. Specifically, prior to any potential civil disorder, the government should seek to establish relationships with social media companies to form a collaborative partnership with each party offering expertise to benefit the other. It is also imperative that the United States analyze and appreciate the beneficial role that social media played in the recent civil unrest in the Middle East and London so that legislation can be drafted fully recognizing the

---

[170] *Id*.
[171] *Crowdsourcing Democracy Through Social Media*, SCIENCEDAILY (Oct. 11, 2011), http://www.sciencedaily.com/releases/2011/10/111011121412.htm.
[172] *Id*.
[173] *Id*.
[174] *See id*.
[175] Clinton, *supra* note 134.

importance of these communication services. Furthermore, the United States should increase law enforcement officers' ability to effectively use social media platforms to anticipate and promptly respond to violence. By taking action prior to the eruption of social unrest, the government will be well-equipped to anticipate, prevent, and control any potential or ongoing violent civil disorders while still preserving Internet freedom.