access

SOCIAL MEDIA IN TIMES OF CRISIS

October 2011

INTRODUCTION

The events of this past year have illustrated the increasingly pivotal role that social networks play in enabling citizens to freely, fully, and safely participate in society. Revolutionary movements in the Middle East and North Africa were fuelled by active participation on social media. People affected by natural disasters in Japan and Australia used social media to report damage, call for help, and communicate with loved ones. While governments throughout the world were up in arms about Mubarak coercing Vodafone and others to shut down networks, it only took a few days of rioting in select cities in the UK for Prime Minister David Cameron to consider similar actions. These events have shown us not only that social media is critical to the facilitation to a number of rights, including freedom of expression and access to information -- as outlined in the Report of the UN Special Rapporteur on freedom of expression, Frank La Rue --but also the fragility of their existence and lack of adequate protections of our fundamental rights.

In this context, it has become clear that we cannot always rely on yesterday's understanding of technology to protect our rights tomorrow. It is for this reason we have put together this paper, which outlines the myriad uses of social networks, particularly during times of crisis. As policy makers in the public and private sectors grapple to understand the implications that social media has for public policy and corporate social responsibility, it is crucial that these actors recognize the importance of devising coherent strategies which respect and promote human rights.

Key Stats:

- 1.96 billion people have access to the internet. There are 5.3 billion mobile lines in the world,[1] up from 2006, when there were 1.2 billion landlines globally.[2]
- 350 million people access Facebook through a mobile device.[3] 50% of mobile Internet traffic in the UK is on Facebook.[4]
- Access to mobile networks is now available to 90% of the world's population and 80% of the population living in rural areas.[5]

THE VALUE OF SOCIAL MEDIA

The following is a brief overview of some ways in which access to social media enriches civic participation, safety, and well-being.

MORE EFFECTIVE AND TARGETED DISASTER RESPONSE

During a time of crisis, individuals look to social media as a means to communicate with one another — sending photos of damage, checking the status of friends and family, or passing along news and updates about the disaster's effects. But people also look to social media channels for information from government agencies and companies. People may not have ready access to televisions or radios but are increasingly using mobile networks, effectively making access to the internet

1 Mobithinking, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats

2 International Telecommunications Union data

3 Facebook Official Statistics, https://www.facebook.com/press/info.php?statistics

4 "Facebook leads rise in mobile web use", Guardian UK, http://www.guardian.co.uk/media/pda/2010/feb/08/facebook-rise-mobile-web-use

5 https://www.accessnow.org/page/-/docs/ITU%20FactsFigures2010.pdf

and social networks faster, more convenient and often more reliable than traditional forms of media. And it's not only a one-way transmission, as organizations and open source software, such as CrisisCommons.org and Ushahidi, have been used during natural disasters to give people the ability to easily report incidences of damage, injury or safety hazards to a centralized location where they are addressed and then swiftly responded to.

People turn to social media in times of crisis. And, according to a recent study by the American Red Cross, 80 percent of US citizens expect national emergency response organizations to both observe social media during disasters and respond quickly to help.[6]

PROMOTING TRANSPARENCY AND MORE ROBUST DEMOCRACIES

Social media has proven to be one of the greatest enablers of grassroots-inspired democratic activity, namely by providing more channels for individuals to exercise their rights and participate meaningfully in civic activities. Election monitoring, for example, has proven to be valuable in bolstering the credibility of elections in democracies or countries in the process of democratization. Ushahidi is designed to assist in the democratization of information, increasing transparency and lowering the barriers for individuals to share their stories. Ushahidi has also been used, amongst other things, to assist in the election monitoring process in Kenya, Tanzania, Sudan, Egypt, Liberia, India, Mexico, and elsewhere.[7]

ENABLING GREATER ACCESS TO INFORMATION AS IT HAPPENS

In times of crisis, the Internet and social media offer an information lifeline to the world. Twitter, Facebook, and YouTube played a key role in telling the story about the Arab Spring to billions of people around the world in real-time. While the Mubarak regime severely restricted press access, and eventually employed the infamous internet "kill switch," protesters on the ground uploaded videos and stories that propagated through the internet to a global audience. Al Jazeera, the network that delivered arguably the best coverage of the Arab Spring, broadcasts for free over the internet to markets in Europe and the Americas where most cable and satellite operators have yet to offer the channel to subscribers..

THE POWER OF CROWDSOURCING

Social media and social networks have made crowdsourcing possible by giving anyone with an internet connection the ability to participate in any variety of projects. Wikipedia is a prime example of a successful crowd-sourced initiative, where over 90,000 people have individually contributed to write 17 million articles.[8] Facebook translated its entire platform into 70 languages using the help of over 300,000 volunteers.[9] Fixmystreet.com is a website that empowers people living in a city to be the eyes and ears of the municipality to spot things that need fixing like potholes, broken streetlights, or other hazards. This improves overall delivery of service and creates a stronger connection between citizens and their government.

6 http://www.redcross.org/portal/site/en/menuitem.94aae335470e233f6cf911df43181aa0/?vgnextoid=7a82d1efe68f1310VgnVCM10000089f0870aRCRD

7 http://blog.ushahidi.com/index.php/category/elections/

8 Wikipedia.org

9 Facebook official stats, https://www.facebook.com/press/info.php?statistics

CHALLENGES

> "States should take all necessary steps to foster the independence of these new media and to ensure access."
>
> — The UN Human Rights Committee[10]

The purpose of this section is to identify and briefly explain some of the main challenges surrounding the use of social media, with an eye to encouraging ICT companies to devise strategies that incorporate human rights protections, and governments to take a step back and examine the potentially adverse effects of extreme measures — such as shutting down networks — particularly during times of crisis.

ANONYMITY: THE DOUBLE-EDGED SWORD

> "If we believe privacy is a social good, something necessary for democracy, liberty and human dignity, then we can't rely on market forces to maintain it."
>
> — Bruce Schneier, Security Expert[11]

In general, it can be said that social networking sites, such as Facebook, have a strong preference for users to create accounts in their real names. There are, however, at least two sides to this issue. On the one hand, it is important that people are identifiable, or at least connected to a persistent identity over time, which can be a pseudonym. On the other hand, as Facebook is credited for the revolutions sweeping the Middle East and elsewhere, its policies do not allow users to participate anonymously, or pseudonymously, (meaning their names must be attached to their real life identity), which puts those living under repressive regimes in direct danger.

It is also important to remember that social networks, which mine and harvest user data, find that this information is much more valuable to advertisers when it can be connected to real names. From an advertiser's perspective, the more granular and detailed information that is available about a "real person," the better, yet, the same data that is useful to an advertiser is also valuable to governments, both democracies and dictatorships alike, interested in tracking political dissidents.

Proponents of "real name" policies online have argued that "in a world of asynchronous threats, it is too dangerous for there not to be some way to identify you."[12] However, as social networking platforms become the window through which individuals participate on the web, for example, by being required to post comments or "like" articles or websites through their Facebook or G+ profile — the "real name" culture has a potential to chill free speech through self-censorship. If everything you do and say is connected to your real name, would you be comfortable expressing yourself on matters that your employer, or future employer would potentially take issue with? The issue then, cannot be framed only in regard to "cybercriminals," but must take into account the implications for all users of the internet.

eBay is an example of pseudonyms working. People buy things everyday on eBay from others all over the world, who they have never met, and who don't use their real names, instead relying on the trust rankings of others in order to have confidence in online transactions and interactions.

10 http://www.ohchr.org/EN/NewsEvents/Pages/FreedomExpressionandnewmedia.aspx

11 http://www.schneier.com/blog/archives/2010/04/privacy_and_con.html

12 http://techonomy.typepad.com/blog/2010/08/google-privacy-and-the-new-explosion-of-data.html

PRIVACY: ONE WARRANT, ONE USER

> "If police and private companies develop a habit of handing over information about people who are rioting, that will set a precedent that could be carried over to political activities."
>
> — Jim Killock, Open Rights Group [13]

Users enjoy significantly fewer protections online than they do offline, and it is incumbent upon national governments to ensure that especially in times of crisis, the rights we have fought so hard for offline are protected on the web as well. For example, the same rights that have traditionally existed for mail sent through the postal system must be extended to e-mail.

Under the guise of national security, governments today frequently engage in mass surveillance of everyone who was in a particular area at a given time (e.g., a protest in Cairo's Tahrir Square). Yet, if we consider the offline analogue to this, intercepting the postal mail of everyone who lives in a particular neighborhood during a certain period of time, this action seems blatantly excessive and an abuse of power.

In the case of the UK riots, executives from Twitter, Facebook, and Research in Motion (makers of BlackBerry) met with British Home Secretary Theresa May, to facilitate cooperation with a view to identify rioters and help the government "anyway they can."14 While this closed-door meeting did not result in network shutdowns, it is unclear as to what level of access to user data and through which process these social networks granted the UK authorities. If these instances — which bypass the rule of law and undermine our fundamental right to privacy and the right to communicate freely — become the norm, what guarantees are there that these data would not be misused regardless of circumstance?

Beware of copycats. Actions taken by liberal, democratic governments to curtail network access, and by extension free speech, are quickly used to justify similar or even more heavy-handed tactics in other countries. Since RIM agreed to cooperate with the British police during the riots, including handing over data about a number of its users, other governments were quick to press RIM into similar secret "cooperative" agreements, including India, Kuwait, South Africa, Indonesia, the United Arab Emirates, and Russia.[15]

NETWORK ACCESS: PROTECTING CITIZENS

> "It's an absolutely horrible idea to suspend [social networks] during important times."
>
> — Alexander Macgillivray, General Counsel for Twitter [16]

The Arab Spring has caused an awakening in that region and around the world about both the power of social networks to greatly enhance and facilitate civic mobilization, and also the way governments can use ICT for nefarious ends. Individuals are just beginning to recognize the vast power governments and private actors have over our personal data, our ability to access information and to suppress free speech. While the Egyptian shut down of the internet was not unprecedented — for example, Nepal (2005) and Burma (2007) have also revoked connectivity during times of political turmoil — it was

13 http://www.thedailybeast.com/articles/2011/08/12/london-riots-police-use-social-media-to-track-rioters.html

14 http://www.guardian.co.uk/media/2011/sep/15/social-media-civil-unrest

15 http://en.rsf.org/blackberry-gives-way-to-pressure-11-10-2011,41159.html

16 http://www.guardian.co.uk/media/2011/sep/15/social-media-civil-unrest

of a greater complexity and scope than ever seen before. What differentiates Egypt from these previous cases is that the government did not have control of the internet from a central location; rather, ISPs were ordered by the government to shut down their networks. This highlights the need for major telecoms operators to anticipate and prepare for future instances in order to protect their users.

It's not only network shutdowns. While there are only a couple of cases of complete internet blackouts, blocking is pervasive throughout much of the world. Of particular concern is the trend of "just in time" blocking, a phenomenon in which access to information is denied — through throttling or filtering access to specific sites — during important political moments when the content may have the greatest potential impact such as elections, protests, or anniversaries of social unrest. This kind of blocking is also harder to detect and rarely provokes international response.

EXPORTING SURVEILLANCE TECHNOLOGY: "WEST CENSORING EAST"

"What we need is a recognition that our reliance on surveillance technology domestically — even if it is checked by the legal system — is inadvertently undermining freedom in places where the legal system provides little if any protection"

— Evgeny Morozov, author of "the Net Delusion [17]

Currently regulation surrounding the issue of the exportation of dangerous, so-called "dual-use" technologies — tools that can be used for both peaceful and military aims — is grey, as governments attempt grapple with how best to mitigate the proliferation of these products. To maintain a consistent position on human rights, particularly in regard to the democratizing potential of ICT, it is imperative that policy makers in both the public and private sectors look carefully at how these technologies can be used to empower repressive regimes, infringe on the rights of users, and undermine democracy and the rule of law.

The European Parliament has taken a proactive step to control the exports of dual use technologies, recently adopting a resolution that would prohibit their export to select countries (such as India, China, Turkey, and Russia) where they may be used "in connection with a violation of human rights, democratic principles or freedom of speech."[18] Access hopes this will be followed by more concrete regulation and that other countries will soon emulate this approach.

INCREASING INTERMEDIARY LIABILITY: CHILLING ONLINE FREE SPEECH

"A public debate is urgently needed in order to assess the scale of the policing measures being entrusted to internet intermediaries, the cost for the rule of law and for fundamental rights as well as the cost for effective investigation and prosecution of serious crimes in the digital environment."

— Joe McNamee, European Digital Rights [19]

17 http://www.nytimes.com/2011/09/02/opinion/political-repression-2-0.html?_r=2

18 http://www.europarl.europa.eu/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports

19 http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Governments, corporations, and increasingly individuals have identified online intermediaries as a convenient single point of content control, because courts are perceived to be too slow and ill equipped to deal with illegal content and activities on the internet. As such, in many jurisdictions governments have delegated the regulation of content to these internet intermediaries.

This regulatory framework forces online service providers (OSPs) in most countries to play judge, jury, and executioner in determining the legality of online content, while simultaneously having to minimize their liability in its propagation. This has a chilling effect on free speech online, as it is in the best interest of OSPs to block, filter, delete, or otherwise remove potentially lawful content in order to avoid costly legal disputes and/or the wrath of their regulators.

"Online intermediaries" are not always large ICT companies. Chiranuch Premchaiporn, Director of Prachatai, an independent online newspaper which reports on freedom of expression issues in Thailand, was charged and jailed for a comment left on her blog by an anonymous poster. She and countless others have been criminally prosecuted under the controversial lèse majesté laws in Thailand, where anyone who "defames, insults or threatens" the Royal Family may be imprisoned for up to fifteen years, even if they did not create or influence the allegedly defaming content. [20]

CONCLUSION & RECOMMENDATIONS

The loose and non-hierarchical organization of people online reflects the very architecture of the web itself, which is in turn reflected in the challenges to internet governance and regulation. The only plausible way forward that protects the rights of users and recognizes the responsibilities of all parties is to develop effective means of collaboration among governments, the private sector, and civil society groups. The following are eight recommendations which we hope will guide the public and private sectors in effectively preparing for, and regulating social media, particularly in times of crisis.

1. ENSURE ACCESS

ICT companies should resist all efforts to shut down services or block access to their products, especially during times of crisis, when open communications are critical. Access condemns any attempts to use, or even build, the technical capability or regulatory authority to cut off or disrupt internet access.

2. SECURE COMMUNICATIONS

Information communication technology companies must provide a basic level of privacy, for example, HTTPS, to their users by default, and resist any bans or curtailment of the use of encryption. Furthermore, social media platforms should ensure the possibility of pseudonyms.

3. WARRANT (TRULY) LAWFUL SURVEILLANCE

Blanket government surveillance of corporate networks should be rejected. All surveillance measures must be targeted, proportional, and based on the rule of law. This means the burden of proof should lie with law

20 http://www.frontlinedefenders.org/node/13727

enforcement authorities, who should formally, through court processes based on probable cause, request a warrant for each individual whose information they would like to access.

4. REGULATE THE EXPORT OF CENSORSHIP AND SURVEILLANCE TECHNOLOGIES

It is critical that actors in both the public and private sector end the sale and service of surveillance technology, such as Deep Packet Inspection (DPI), to countries that would likely use these tools for ignoble ends.

5. MINIMIZE INTERMEDIARY LIABILITY

All action taken against illicit activity on the internet must be aimed at those directly responsible for such activities, and not at the means of access and transport — namely online intermediaries — always upholding the fundamental principles of freedom, privacy, and the respect for human rights.

6. PRACTICE HUMAN RIGHTS BY DESIGN

ICT companies should implement human rights respecting policies and practices into their day-to-day operations, and engage in regular multistakeholder and cross-sector dialogue to discuss challenges faced by the sector and developments in best-practice.

7. RESIST GOVERNMENT REQUESTS FOR DATA

Social media providers should resist overboard requests from governments to reveal user information, disclose no more information about their users than is legally required, and inform the user so they can legally respond.

8. ENSURE TRANSPARENCY, ACCOUNTABILITY AND APPEALABILITY

It is crucial for private and public institutions making decisions on policies and protocols regarding social media to fully disclose all actions. Such steps need to be embedded in frameworks with independent (judicial) oversight and provide users affected with the ability to appeal regulatory case-decisions.