JOURNAL OF COMMUNICATION

Journal of Communication ISSN 0021-9916

ORIGINAL ARTICLE

Social Media and the Activist Toolkit: User Agreements, Corporate Interests, and the Information Infrastructure of Modern Social Movements

William Lafi Youmans[1] & Jillian C. York[2]

1 Department of Communication Studies, University of Michigan, Ann Arbor, MI 48109-1285, USA
2 Electronic Frontier Foundation, San Francisco, CA, USA

The uprisings in Tunisia, Egypt, and elsewhere have been credited in part to the creative use of social media platforms such as Facebook and Twitter. Yet the information policies of the firms behind social media can inhibit activists and empower authoritarian regimes. Analysis of Facebook's response to Egypt's "We Are All Khaled Said" group, YouTube's policy exemption for videos coming from Syria, Moroccan loyalist response to the online presence of atheists, and the activities of the Syrian Electronic Army illustrate how prohibitions on anonymity, community policing practices, campaigns from regime loyalists, and counterinsurgency tactics work against democracy advocates. These problems arise from the design and governance challenges facing large-scale, revenue-seeking social media enterprises.

doi:10.1111/j.1460-2466.2012.01636.x

Social media platforms are utilized extensively by activists in a variety of political systems. Their role in the evolution of events during the "Arab Spring" has been widely discussed, but it is also important to recognize that social media are used to serve the political goals of reformers, revolutionaries, and authoritarian regimes alike. At the same time, Facebook, Google, Twitter, and the other firms must view social media in commercial terms as products and services with customers and users. In this article we examine four cases in which social media design and policies created tensions between the sociopolitical uses by activists and the commercial interests of the platform owners.

Information technologies have become indispensable to reformers, revolutionaries, and contemporary democracy movements. They serve as venues for the shared expression of dissent, dissemination of information, and collective action. In the

Corresponding author: William Youmans; e-mail: wyoumans@umich.edu

Middle East, they offered a sphere of public life in which Arab youth could reach beyond the control of older generations and build links with transnational networks of advocates who provide a partial counterbalance to state power (Aday & Livingston, 2008; Armbrust, 2007). Social media in the Middle East and elsewhere undermine the territorial, coercive, and social underpinnings of despotic governments by exposing and breaking the state's power to silence popular grievances and to criminalize opposition (Masoud, 2011).

Social media provide the tools for organized dissent yet can constrain collective action. The architecture of social media shapes its uses and limits at two levels. First, the application's programming code sets the range of usability. Thus, "Codes constitute cyberspaces; spaces enable and disable individuals and groups. The selections about code are therefore in part a selection about who, what, and most important, what ways of life will be enabled and disabled" (Lessig, 2006, p. 88). "Code is law," as Lessig (1999) famously declared, because it permits and forbids the uses set out by an application's sponsoring firms (Grimmelmann, 2004). Second, users' actions are enabled and constrained by company policies and user terms governing, among other things, intellectual property, community policing provisions, anonymity, and offensive and violent content. These are enforced through code, by actual programming design as well as by firms' adjudication and actions against violations.

Firms focus primarily on increasing users, improving usability, boosting revenue streams, avoiding negative public relations, seeking access to new markets, and protecting other larger classes of nonactivist users. These privatized goals of platform owners and developers can conflict with their use as tools for civil society and popular mobilization. Changes in architecture may thus adversely impact activists.

This article centers on specific developments—namely evolving policies, functionalities, and user guidelines—that affect the key social media activists employ. These architectural changes alter the communicative structure of social media sites, ultimately affecting who connects with whom. To complicate matters further, states are catching up on social media, using them to gather intelligence and spread proregime propaganda. While state powers have some leverage over the companies, their infiltration of the platforms is another threat to activists.

Social media and the activist toolkit

Debate regarding the influence of online activism in revolutions in the popular press pits advocates of the Internet's emancipatory promise (Shirky, 2008, 2011) against those who warn of negative consequences, including its use in state repression (Morozov, 2011) or encouraging "slacktivism," or superficial, minimal effort in support of causes (Gladwell, 2010). While the Arab Spring was labeled a "Facebook revolution" by some, others have pointed to core causes such as unemployment and state repression. Still others argue that by placing too much emphasis on the role of social media, popular commentaries both mystify its effects and ignore the deeper historical roots of rebellion in the pre-Internet era (Anderson, 2011; Aouragh

& Anderson, 2011). For their part, communication researchers have gravitated away from polarized perspectives, focusing instead on the more specific ways social media are used and what the effects of those may be (e.g., Bennett, 2003; Howard, 2010).

The Arab Awakening, as some call it, presents a particularly interesting set of cases for examining theoretic perspectives on the relationship between social media and collective action (e.g., Bimber, Flanagin, & Stohl, 2005; Flanagin, Stohl, & Bimber, 2006; Segerberg & Bennett, 2011). Much of the initial research and analysis finds that social media played an important role in the collective actions that resulted in the overthrow of the governments of Egypt and Tunisia's revolutions (Iskander, 2011; Kavanaugh, Yang, Sheetz, Li, & Fox, 2011; Khamis & Vaughn, 2011; Wilson & Dunn, 2011). According to Lynch (2011), social media contributed to collective action in four ways: (a) by making it easier for disaffected citizens to act publicly in coordination; (b) by creating information cascades that bolstered protesters' perceptions of the likelihood of success; (c) by raising the costs of repression by the ruling regimes; and (d) by dramatically increasing publicity through diffusion of information to regional and global publics. No one social media platform served all of these functions all of the time, but instead platforms provided a variety of affordances that were important at different times, sometimes providing forums for early critiques of the regimes and later helping to form public opinion and provide logistical assistance to those organizing protests. (Aouragh & Anderson, 2011; Howard & Hussain, 2011).

Our approach begins by noting that social media technologies, as well as their governance and management, and thus, their uses by both activists and regimes, are still evolving. Programmed orders of functionality, or code, embody the governing architecture of social media applications to a degree not recognized in the behavioral research on new media (Mansell, 2006). The main social media platforms are institutions that shape interactions within activists' collective action spaces. Changes in platform architecture may introduce new or expand previous constraints for activist users, thus affecting the risks and effectiveness of their efforts.

This focus contributes to the concern with the impact of the political economy of media corporations on content production and circulation (Dahlberg, 2005; Mansell, 2004), as well as the power of states to influence media. It accepts power, ownership, and control as important factors shaping social media development and use governance. Although we accept the disruptive potential of social media, our goal is to highlight the mismatch between the commercial logic of platforms such as Facebook and the needs of activists using social media as public information infrastructure. The fundamental problem is that social media governance, both in terms of code-as-law and the rule of policies and user terms, is driven by necessary commercial considerations, namely monetization. Companies must appeal to broad classes of users and advertisers, which both can help activists and lead to policy changes that constrain them. Social media operators are not inherently antiactivist by agenda or driven by ideological impetuses. As the platforms were not designed to cater to activist users, changes in rules and architectures can have negative, unintended consequences for activists.

Interpretive case analysis

We present analyses of four cases in which social media architecture, policies, and user terms obstructed or complicated activist uses. Rather than seeking generalizations or tests of theories of user behavior, our focus is on the practices of specific institutions. Interpretive case study analysis is particularistic and emphasizes both thorough description and drawing fresh insights (George & Bennett, 2005; Yin, 2003).

The cases were selected according to the following criteria: They involved one of the primary social media platforms (Google, Facebook, Twitter, or Yahoo! and their subsidiaries); credible and verifiable documentation was available; and interference with activist purposes was apparent. The case study approach was useful because it allowed us to weave several sources of evidence together. These included: (a) document analysis of their user terms and policy guidelines; (b) documented changes to their technical infrastructures; (c) official and unofficial statements by social media spokespeople and heads; (d) advocacy platforms of nongovernmental organizations; and (e) personal correspondence with activists.

As profit-seeking entities, the companies that develop and control social media platforms must retain and gain users, develop new revenue streams, and avoid liabilities and bad publicity. When state power also comes to bear on them, the utility of social media to activists could decline. Four case studies demonstrate how prohibitions on anonymity and certain content types, and the use of community policing of offensive material and greater infiltration by government agents can lessen social media's utility. States and the private sector are allied against online anonymity because it impairs governance and monetization. And yet, anonymity, as well as the overarching concern of privacy, is of central importance for activists and dissident journalists using social media.

Case study 1—"We Are All Khaled Said": Banning anonymous users

The now-famous "We Are All Khaled Said" Facebook page was created by a pseudonymous user' "ElShaheed" ("the martyr") in June, 2010. It became a central platform for debate and helped mobilize many during the Egyptian uprising. "ElShaheed" is now known to have been a former Google executive, Wael Ghonim. One reason for using a pseudonym was his personal security. In the first week after the protests broke out, Ghonim told *Newsweek* "I'm taking as much measures as I can to remain anonymous. But of course I'm scared" (Giglio, 2011). Other benefits of a pseudonym, according to Ghonim, included avoiding the factionalism of Egyptian oppositional politics. Ghonim administered the account until November 2010, when—just before Egyptian parliamentary elections—Facebook deactivated Ghonim's pseudonymous account and the page. A Facebook spokeswoman said it "was removed because of a violation of our terms and not because of contact from any government" (Coker, Malas, & Champion, 2011). Facebook officially prohibits the use of pseudonyms in accounts. The page was relaunched eventually. An Egyptian activist suggested social media platforms should "allow anonymous accounts, even if

it means putting a small symbol stating that it is one'' (Egyptian activist 3, personal communication, 6 August 2011). Privacy on social networks is about controlling who precisely gets access to one's personal account. As one activist said, ''The main concern is about my privacy and safety of information I provide, and how far will the website fight for users privacy'' (Egyptian activist 1, personal communication, 14 July 2011). Yet, many users show lax attitudes toward protecting theirs' (Debatin, Lovejoy, Horn, & Hughes, 2009). People share text updates, photographs, videos, and other content within their networks, but often lack awareness of precisely with whom their information circulates or who else can gain access to their accounts, which for activists can risk personal security (Faris, Roberst, Heacock, Zuckerman, & Gasser, 2011). This can be reduced by education in online literacy, but other privacy risks are built into social media governance and can come to the fore during moments of policy changes.

Both Facebook and Google have been subject to controversies around privacy. In 2007, Facebook launched the *Beacon* service, which morphed user content into advertisements shared with users' friends without consent (Brodkin, 2009). Facebook was slow to implement privacy settings to begin with and even then privacy options did not always function correctly (Debatin et al., 2009). Google settled a class-action lawsuit brought by 31 million users of Google's *Buzz* social networking service, after the service publicly exposed users' e-mail contacts without permission (Grimmelmann, 2010). This particularly angered journalists, activists, lawyers, and others whose networks were highly sensitive information. Citizen journalists were especially vulnerable since they lacked the (albeit limited) protection of institutional affiliation. Even without professional credentials, they played a role as information-gatherers during the Arab uprisings (Khamis & Vaughn, 2011) and likely will in future revolutions when traditional media are heavily manipulated or have scant access.

Allowing anonymity in social action is arguably essential for the protection of basic rights such as liberty, dignity, and privacy, yet both states and the private sector push for real identity requirements (Kerr, Steeves, & Lucock, 2009, pp. 439–440). In the United States, various social media firms have attempted to limit anonymity despite its support in American jurisprudence and political history (Wallace, 1999). Many bloggers and activist social media users particularly seek anonymity as a mean of protection from retaliation (Viégas, 2005).

At the same time, online anonymity has been used by some as a cover for harassment, fraud, and illegal activity. For example, a blogger known as ''the Gay Girl in Damascus'' became a media source on protests in Syria and was later found to be a middle-aged American man living in Scotland (Addley, 2011). Anonymity can also encourage ''trolling,'' the uncivil use of discussion forums to provoke, degrade, and distract others. Facebook designers argued publicly for curbing online anonymity as a way to prevent these types of abuses (Zhuo, 2010). Facebook's terms of service therefore limit users to one profile and require that ''users provide their real names and information.''

The commercial interest is that real identities are easier to monetize. They are needed for online commerce as well as for generating the valuable consumer data that Facebook collects. CEO, Eric Schmidt, claimed that Google's Real Name policy was important for providing users access to a wide array of products and services. With real names, he said, "we could you know bill them, you know we could have credit cards and so forth and so on" (Pfanner, 2011).

Another emerging issue is how social media platforms attempt to police content in congruence with their stated community standards. Facebook's "Statement of Rights and Responsibilities" (revised April 26, 2011) states that users will "not bully, intimidate, or harass any user" or "post content that is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence." Not all social media is so prohibitive. Twitter's Terms of Service only warn users they "may be exposed to Content that might be offensive, harmful, inaccurate, or otherwise inappropriate."

Case study 2—YouTube videos from Syria: Banning offensive content

YouTube has been cited as a vital platform in the Arab Spring uprisings, particularly in Syria, where the absence of professional journalists has created a need for citizen video (Amos, 2011). Many videos from Syria were extremely graphic, capturing the regime's use of violence to quell protests. YouTube took down a popular video showing the battered body of a young boy, Hamza Ali al-Khateeb, who was reportedly tortured and killed by authorities in Jiza. Those trying to view the video found a message saying, "This video has been removed as a violation of YouTube's policy on shocking and disgusting content" (Melber, 2011). The video was restored, but only after a journalist of *The Nation* brought it to the attention of YouTube staffers.

YouTube includes a warning against graphic images in the terms of service, but sets specific standards through "Community Guidelines." During the Arab Spring, there was a shift in policy enforcement at YouTube. In May 2011, while addressing the platform's policies in light of video from Libya, YouTube Manager of News, Olivia Ma, said that, although such violence violates their community guidelines and terms of service, making it subject to removal, "we have a clause in our community guidelines that makes an exception for videos that are educational, documentary, or scientific in nature . . . So, we will actually adjust our policies in real time to adapt to situations" (Plesser, 2011). This was done on a case-by-case basis, and the Arab uprisings were granted exemption.

For activists, documenting and circulating video and images that demonstrate regime violence can help recruit new members to collective action efforts. For instance, in 2007, Egyptian antitorture activist, Wael Abbas, posted on YouTube a video of two police officers sodomizing an Egyptian bus driver. Although the video brought about a public outcry and the conviction of the officers, YouTube removed the video and deactivated Abbas's account. They restored it eventually. Even when videos are restored, however, the impact on behalf of activists may be diminished by

the loss of viewers and because the video may be overtaken by more recent events. Furthermore, content standards can be difficult to adjudicate. When sectarian divisions overlap with power differences, as in Bahrain and Syria, antiregime rhetoric may include language derogatory of entire groups, such as Sunni Muslims in Bahrain or Alawites in Syria. These can easily be construed as incitement, promoting terrorism or hatred.

Most platforms utilize community policing mechanisms, in which account holders may report others for terms of service violations, including offensive content or unwanted contact (''spam''). Given the enormous amount of data, this crowd-sourced monitoring of community standards lowers the costs of policy enforcement significantly. Some platforms additionally employ automated content controls to remove or prevent the posting of certain words, phrases, or links. Although these strategies can be very effective, for example, at combating overzealous e-marketers, they can also harm activist users. During the Arab Spring for example, state agents and regime supporters used such flagging to report and have removed content generated by activists. This reflected a longstanding problem by which certain, offended communities exploit these functions to censor views they oppose.

Case study 3—The antiatheist Facebook campaign: Community policing abuse

Campaigns for the specific purpose of getting certain content or accounts taken down have emerged. They exploit reporting mechanisms and pressure firms directly. An Arabic-language group called ''Together to close all atheist profiles on Facebook'' began identifying Arab Facebook users known to be atheists and calling on group members to report those users for violating the site's identification policy (York, 2010). Although there is no proven link with the activities of those using that group page, it is worth noting that Kacem El Ghazzali, a Moroccan blogger who is identified as an atheist, had his account removed. Other atheists' accounts were blocked, as well. A group page calling for the separation of religion and state in the Arab world was also taken down, though it was reinstated within a few days. Community policing practices can easily be turned against dissidents with unpopular positions or members of minority identity groups.

There are, however, some safeguards in place to protect against orchestrated abuse. YouTube staffers have stated, for example, that the reports of users who frequently create erroneous reports will be negatively ''weighted'' so as to ensure fair enforcement of their rules. Other social networking platforms may have similar mechanisms and be cognizant of orchestrated and selective reporting. Importantly, however, no social media site has yet posted explicit policies against malicious reporting and the process for appealing actions taken remain unclear and weak. Yet orchestrated manipulation of reporting mechanisms continues to have grave consequences for activists, especially when attacks are timed so as to disrupt planned events crucial to the activists–such as demonstrations. Governments such as Tunisia

reportedly pushed loyalists to engage in reporting campaigns (''Les 'ennemis de la Tunisie'. . . ,'' 2010). Government agents in Sudan posted pornography to protest pages and then reported them to Facebook (Boswell, 2011).

Automated social media protocols for discouraging ''spammers'' often work against the interests of activists. For example, Tunisian activist Rafik Dammak found his account disabled in mid-2010, with a message explaining, ''We will not be able to reactivate [your account] for any reason, nor will we provide further explanation of your violation or the systems we have in place. This decision is absolutely final.'' Dammak suspected he was reported by regime loyalists, but a Facebook official said Dammak had sent too many friend requests that were rejected, and ignored warnings about spam (MacKinnon, 2010). In another case, Ahmed Maher, an administrator of the Facebook group for the Egyptian April 6 group, found that his account had been disabled because of his high volume of correspondence (Wolman, 2008). In both cases, the automated systems were thwarting attempts to reach as many people as possible, the very thing that activists want social media to do for them.

In attempting to stifle communications amongst activists, governments have essentially three tactics from which to choose: censorship, surveillance, and propaganda (Morozov, 2011). While the first generation of content controls was covert, a new generation is making Internet censorship the global norm (Deibert, Palfrey, Rohozinski, & Zittrain, 2008). Furthermore, while first-generation controls denied access through basic means, next-generation techniques are more sophisticated.

The ability of a government to shut down Web sites, or indeed, the Internet during a protest is one tool available to states (Howard & Hussain, 2011). Indeed, following Egypt's footsteps, both Libya and, briefly, Syria attempted to cut off Internet access (Cowie, 2011a, 2011b). In the case of Libya, this tactic was largely ineffectual due to the country's low Internet access. Syria's leader Bashar al-Assad, perhaps recognizing the failed approaches of the Tunisian and Egyptian regimes, chose to *unblock* Facebook, Blogspot, and YouTube, which were blocked since 2007, in order to increase surveillance. This move was shrewd, showing how a government can use social media to repress.

During the Arab protests, each government approached social media differently, in attempting to quell protests. In Tunisia, where access to various digital communication tools had been cut off for years (Deibert et al., 2008), activists succeeded in utilizing digital tools to organize and disseminate information about protests, using proxies to circumvent censorship. Facebook was never blocked there. Egypt's Mubarak took a different approach, first blocking popular tools Facebook and Twitter, then shutting down access to the Internet (Perez, 2011; Richtel, 2011). Mubarak's ploy seemed to have the opposite effect than what was intended, possibly resulting in more citizens taking to the streets. In the end, the week-long Internet blackout did not end protests. As with Iran, crowd-sourced regime supporters in Bahrain gathered information on online dissenters (Bahraini activist, personal communication by phone, 6 August 2011). Regimes have adapted activists' digital tools to combat protests through counter mobilization and to enhance surveillance and prosecution

abilities. In 2010, following the previous summer's protests in Iran, the government asked citizens to identify the faces of protesters in images posted online (Athanasiadis, 2010). Sudan also used protesters' Facebook pages to gather intelligence, spread disinformation, and disrupt demonstrations (Boswell, 2011). Repressive regimes are demonstrating learning curves when it comes to limiting the usefulness of social media for activists. Just as in Bahrain and Egypt, Syrian authorities arrested Facebook users and forced them to turn over sign-in information. They have also reportedly used Facebook accounts featuring photographs of attractive women in attempts to entrap activists (Wood, 2011).

Case study 4—The Syrian Electronic Army: Authoritarian social media use

The "Syrian Electronic Army" is a hacker group whose aim has been to bring down, deface, or otherwise target sites that host antiregime content. The group denies affiliation with the regime of Bashar al-Assad, claiming on its Facebook page that its founders are ordinary Syrians fighting against "fabrications and distortions of events in Syria." The Army's targets have included Oprah Winfrey, journalist Nicholas Kristof, and President Barack Obama, among others (Noman, 2011). The group posted dissidents' contact information, threats against critics, and proregime messages such as "I love Bashar" on social network sites (Karam, 2011). It has also conducted denial of service (DoS) attacks aimed at bringing down the Web sites of news organizations, and defaced many others with proregime images and texts. The Army's actions led President al-Assad to thank them in a speech, hailing them as a "real army in virtual reality" (al-Assad, 2011).

The responses to these actions by social media platform managers has been mixed. Facebook, for instance, removed a number of pages belonging to the Syrian Electronic Army, but allowed many others to remain. When the Army attempted to drown out opposition messages on Twitter by using automated accounts to bombard users with photographs of Syrian landscapes using the hashtag #Syria, the company responded by removing the account's tweets from hashtag search results, but did not remove them from their profile pages.

These examples illustrate how the social media tools that facilitate protest can also be used by repressive regimes and their supporters to dampen and disrupt opposition. But activists in the Arab Spring have also adapted to the state's infiltration of social media in several ways. In Bahrain, for example, activists have used closed direct messaging and chats instead of public walls and profiles on Facebook and Twitter to communicate (Bahraini activist, personal communication by phone, 6 August 2011). Similarly, Syrian activists have developed strategies to prevent detection, advising other users to erase contacts with "any name that sounds Islamic," as well as to remove content that refers to revolution (Sayed, 2011). Activists in Egypt coordinated contingency plans to have others delete their accounts in the case they go missing.

Government pressure can also be directed at the social media companies themselves. Most major social media platforms are based in the United States and

are therefore subject to U.S. laws. Although laws regulate the export of a wide variety of materials and products, including certain technologies such as cryptographic software, to repressive regimes, there is little legal guidance or protection for social media companies.

As a consequence, social media companies regularly receive government requests to provide user data, or to remove content. Companies typically comply rather than face penalties when this occurs as a result of a valid legal request. If a request for data or content removal occurs outside of the home jurisdiction, the company may refuse to submit the request. However, because refusing such requests may result in being banned or blocked, states can exert leverage over social media even when they lack legal grounds for doing so. Business considerations may trump civic considerations. In some cases companies receiving illegal or extralegal requests have chosen to disclose the requests to the public. Google, for instance, makes information about requests for content removal and user data public in its Transparency Report. The majority of companies do not, however. Of the companies providing social network services, only Google and Twitter publicly report such government requests. Companies face perhaps their biggest challenge when they have employees and capital in a given country. They are more easily coerced into compliance with laws that contradict global standards and principles of free expression or privacy.

There is growing documentation of the risks to individuals when social media companies cooperate with repressive regimes. In 2005, for example, Chinese journalist Shi Tao was convicted of leaking state secrets and sentenced to 10 years imprisonment. Key evidence cited by the prosecution in his trial included information about Shi's Yahoo! account, provided to the Chinese State Security Bureau by the company itself (MacKinnon, 2007). And in 2008, following the arrest of Moroccan engineer Fouad Mourtada for creating a fake Facebook profile of a member of the country's royal family, civil liberties groups claimed that Facebook may have handed over the user's information to the Moroccan government (Vara, 2008).

Beyond these dramatic cases, the state's power over social media will eventually be seen in the form of content restrictions. Google, for example, chose to launch its localized Google.cn search engine in 2006, shortly after opening their first office in China. Chinese content regulations prohibited certain types of "sensitive content" including information on the 1989 Tiananmen Square Massacre, the banned Falun Gong, and prodemocracy movements (Deibert et al., 2008). The photo-sharing site Flickr, owned by Yahoo!, restricts content to users in certain countries. Microsoft's Bing search engine restricts search results for users in various countries, including the entirety of the Arab world (Noman, 2010).

Conclusion: Agency against the social media constraints on collective action

Social media firms will continue to limit anonymity, prohibit certain content, and depend on community policing, while at the same time governments undoubtedly will seek to increase their leverage against firms and pursue strategies of infiltration

and surveillance. There are at least six strategies that activists might use to maintain or even enhance social media as tools for collective action.

First, activists can exert their power as consumers by jumping to new social media platforms en masse. Over time, this line of reasoning goes, the market provides applications with the security and functionality that activists require. The downside of this approach is that platforms optimized for activists may be so niche that it is more difficult to broadcast their concerns widely and mobilize networks of casual sympathizers.

Second, activists can try to use the law by applying extant legal doctrine to create new remedies against social media companies that put users at extra risk. Consumer safety provisions in American law, such as product liability law, would seem to have some parallels, even if there are important differences. Legal scholars like Grimmelmann (2010, p. 827) do not argue for a direct application of laws governing manufacturer liability for harms stemming from the products' uses, but instead advocate greater dialogue between "two bodies of law that have a common history and more in common than scholars and lawyers sometimes realize."

Third, activists can appeal directly to the governments in the United States and other countries that claim to be committed to an open Internet and democratization. U.S. Secretary of State Hillary Clinton (2010) has expressed Internet freedom as an aim of American foreign policy; she called for companies to "take a proactive role in challenging foreign governments' demands for censorship and surveillance." Exhortation is unlikely to be enough. To be effective, this approach will require the development of a regulatory apparatus in the United States and elsewhere.

Fourth, activists can work to advance industry self-regulation. One such effort is the Global Network Initiative in which a diverse group of experts and stakeholders have negotiated a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector. Although it has produced extensive statements of principle and implementation guidelines, the initiative has only attracted three ICT companies after 4 years of effort (Kopytoff, 2011).

Fifth, they can pressure large social media companies via long-term, iterative, incremental advocacy. In the words of one Egyptian activist, this approach advocates a "system in which the power shifts toward the users rather than the powerful private companies running the network" (Egyptian activist 2, personal communication, 14 July 2011). MacKinnon (2011) argued that achieving a "citizen-centric" Internet will demand a broad and sustained movement.

Finally, activists can embrace the development of what Zittrain (2009) calls "civic technologies." These technologies are not constrained by government or commercial gatekeepers, but instead are untethered platforms for the generation of further innovations. Civic technologies depend on an open architecture that is free to accept whatever structures and content users wish to build. Civic technologies such as Wikipedia are not only open to activists, but have themselves become sites of political contestation.

Although social media firms made some exceptions for reformers during the Arab Spring, their policies and the architecture of their products will increasingly

complicate collective action efforts. Nonetheless, pressures by users have and will continue to force adjustments in design and policy. Social media researchers must consider the tensions between activists, governments, and firms' commercial interests. This interplay not only has obvious civic and political consequences, but also creates a rich context for the re-examination of social media and collective action.

Acknowledgment

Funding was provided by the University of Michigan's Department of Communication Studies.

References

Aday, S., & Livingston, S. (2008). Taking the state out of state-media relations theory: How transnational advocacy networks are rewriting (some of) the rules about what we think we know about news and politics. *Media, War, and Conflict*, **1**(1), 99–107. doi: 10.1177/1750635207087630

Addley, E. (2011, June 13). Syrian lesbian blogger is revealed conclusively to be a married man. *The Guardian* (UK). Retrieved from http://www.guardian.co.uk/world/2011/jun/13/syrian-lesbian-blogger-tom-macmaster

Amos, D. (2011, August 3). Syrian uprising expands despite absence of leaders. Npr.org. Retrieved from http://www.npr.org/2011/08/03/138936844/syrian-uprising-expands-despite-absence-of-leaders

Anderson, L. (2011). Demystifying the Arab spring: Parsing the differences between Tunisia, Egypt and Libya. *Foreign Affairs*, **90**(3), 2–7.

Aouragh, M., & Anderson, A. (2011). The Egyptian experience: Sense and nonsense of the Internet revolution. *International Journal of Communication*, **5**, 1344–1358.

Armbrust, W. (2007). New media and old agendas: The Internet in the Middle East and Middle Eastern Studies. *International Journal of Middle East Studies*, **39**(4), 531–533. doi: 10.1017/S0020743807071048

al-Assad, B. (2011, June 21). Speech of H.E. President Bashar al-Assad at Damascus University on the situation in Syria. Damascus, Syria. Retrieved from http://www.sana.sy/eng/337/2011/06/21/353686.htm

Athanasiadis, I. (2010, January 4). Iran uses Internet as tool against protesters. *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/World/2010/0104/Iran-uses-Internet-as-tool-against-protesters

Bennett, W. L. (2003). New media power: The Internet and global activism. In Couldry, N. & J. Curran (Eds.), *Contesting media power* (pp. 17–38). Oxford, England: Rowman and Littlefield.

Bimber, B., Flanagin, A., & Stohl, C. (2005). Reconceptualizing collective action in the contemporary media environment. *Communication Theory*, **15**(4), 365–388. doi: 10.1093/ct/15.4.365

Boswell, A. (2011, April 6). How Sudan used the Internet to crush protest movement. *McClatchy Newspapers*. Retrieved from http://www.mcclatchydc.com/2011/04/06/111637/sudans-government-crushed-protests.html

Brodkin, J. (2009, December, 8). Facebook halts Beacon, gives $9.5M to settle lawsuit. *PCWorld*. Retrieved from http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_95m_to_settle_lawsuit.html

Clinton, H. (2010, January, 21). Remarks on Internet freedom. Washington, DC. Retrieved from http://www.state.gov/secretary/rm/2010/01/135519.htm

Coker, M., Malas, N., & Champion, M. (2011, February, 7). Google executive emerges as key figure in revolt. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052748703989504576127621712695188.html

Cowie, J. (2011a). Libyan Disconnect. [blog]. Retrieved from http://www.renesys.com/blog/2011/02/libyan-disconnect-1.shtml

Cowie, J. (2011b). Tracing the Syrian blackout. [blog]. Retrieved from http://www.renesys.com/blog/2011/06/tracing-the-syrian-blackout.shtml

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, **15**, 83–108. doi: 10.1111/j.1083-6101.2009.01494.x

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering.* Cambridge, MA: MIT Press.

Faris, R., Roberst, H., Heacock, R., Zuckerman, E., & Gasser, U. (2011, 2 August) Online security in the Middle East and North Africa: A survey of perceptions, knowledge, and practice. Berkman Center for Internet & Society at Harvard University. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/OnlineSecurityinthe MiddleEastandNorthAfrica_August2011.pdf

Flanagin, A. J., Stohl, C., & Bimber, B. (2006). Modeling the structure of collective action. *Communication Monographs*, **73**, 29–54. doi: 10.1080/03637750600557099

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences.* Cambridge, MA: MIT Press.

Giglio, M. (2011, 30 January). The mysterious 'anonymous' behind Egypt's revolt. *Newsweek*. Retrieved from http://www.newsweek.com/2011/01/30/el-shaheed-the-mysterious-anonymous-behind-egypt-s-revolt.html

Gladwell, M. (2010, 4 October). Small change. *The New Yorker*. Retrieved from http://www.newyorker.com/reporting/2010/10/04/101004fa_fact_gladwell

Grimmelmann, J. (2004). Regulation by software. *Yale Law Journal*, **114**, 1719–1775.

Grimmelmann, J. (2010). Privacy as product safety. *Widener Law Journal*, **19**, 793–827.

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

Howard, P. N., & Hussain, M. M. (2011). Digital media and the Arab Spring. *Journal of Democracy*, **22**(3), 35–48. doi: 10.1080/10714421.2011.597254

Iskander, E. (2011). Connecting the national and the virtual: Can Facebook activism remain relevant after Egypt's January 25 uprising? *International Journal of Communication*, **5**, 1225–1237.

Jepperson, R. (1991). Institutions, institutional effects, and institutionalism. In W. W. Powell & P. J. DiMaggio (Eds.), *The new institutionalism in organizational analysis* (pp. 143–163). Chicago, IL: The University of Chicago.

Karam, Z. (2011, September 27). *Syria wages cyber warfare as websites hacked.* Associated Press. Retrieved from http://www.google.com/hostednews/ap/article/ALeqM5h_ALtePegit5Y7joOwz51xnk-dSA?docId=876d93bf5fa04fe7a132c428ca97bb92

Kavanaugh, A., Yang, S., Sheetz, S., Li, L. T., & Fox, E. A. (2011). Between a rock and a cell phone: Social media use during mass protests in Iran, Tunisia and Egypt. *ACM Transactions on Computer-Human Interaction*. doi: 10.1145/0000000.0000000

Kerr, I., Steeves, V., & Lucock, C. (2009). *Lessons from the identity trail: Anonymity, privacy and identity in a networked society.* Oxford, England: Oxford University Press.

Khamis, S., & Vaughn, K. (2011). Cyberactivism in the Egyptian revolution: How civic engagement and citizen journalism. *Arab Media and Society*, **13**. Retrieved from http://www.arabmediasociety.com/?article=769

Kopytoff, V. G. (2011, March 7). Sites like Twitter absent from free speech pact. *The New York Times*, **B4.**

Lessig, L. (1999). *Code: And other laws of cyberspace.* London, England: Basic Books.

Lessig, L. (2006). *Code: And other laws of cyberspace. Version 2.0.* London, England: Basic Books.

Lynch, M. (2011). After Egypt: The limits and promise of online challenges to the authoritarian Arab state. *Perspectives on Politics*, **9**(2), 301–310. doi: 10.1017/S15375927 1100091

MacKinnon, R. (2007). Shi Tao, Yahoo!, and the lessons for corporate social responsibility (Working paper). Retrieved from http://rconversation.blogs.com/YahooShiTaoLessons.pdf

MacKinnon, R. (2010, May 29). More problems in Facebookistan. [blog]. Retrieved from http://rconversation.blogs.com/rconversation/2010/05/more-problems-in-facebookistan.html

MacKinnon, R. (2011, July). Let's take back the Internet! TEDGlobal, Edinburgh, Scotland. Retrieved from http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html

Mansell, R. (2006). Collective action, institutionalism and the Internet. *Journal of Economic Issues*, **40**(2), 297–305. doi: 10.1177/1461444804039910

Masoud, T. (2011). The Road to (and from) Liberation Square. *Journal of Democracy*, **22**(3), 20–34.

Melber, A. (2011, May 31). YouTube reinstates blocked video of child allegedly tortured in Syria. *The Nation*. Retrieved from http://www.thenation.com/blog/161050/youtube-reinstates-blocked-video-child-allegedly-tortured-syria

Morozov, E. (2011). *The net delusion: The dark side of Internet freedom.* New York, NY: Public Affairs.

Noman, H. (2010). Sex, social mores, and keyword filtering: Microsoft Bing in 'Arabian Countries'. *OpenNet Initiative Bulletin*. Retrieved from http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabian-countries

Noman, H. (2011). The emergence of open and organized pro-government cyber attacks in the Middle East: The case of the Syrian Electronic Army. *Information Warfare Monitor*. Retrieved from http://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army

Perez, J. C. (2011). Egypt's Internet block aims at social media. *Computerworld*, January 28. Retrieved from http://www.computerworld.com/s/article/9206980/Egypt_s_Internet_block_aims_at_social_media

Pfanner, E. (2011, September 4). Naming names on the Internet. *The New York Times*. Retrieved from http://www.nytimes.com/2011/09/05/technology/naming-names-on-the-Internet.html

Plesser, A. (2011, May 6). YouTube is managing graphic, violent videos from the Middle East with community help. *Business Insider*. Retrieved from http://articles.businessinsider.com/2011-05-06/entertainment/30063062_1_videos-youtube-beettv.

Sayed, H. (2011, August 6). Fear of arrest. [blog]. Retrieved from http://www.jadaliyya.com/pages/index/2328/fear-of-arrest

Segerberg, A., & Bennett, W. L. (2011). Social media and the organization of collective action: Using Twitter to explore the ecologies of two climate change protests. *The Communication Review*, **14**(3), 197–215. doi: 10.1080/10714421.2011.59725

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations.* New York, NY: Penguin.

Shirky, C. (2011). The political power of social media. *Foreign Affairs*, **90**(1), 28–41.

Vara, V. (2008, February 29). Facebook denies role in Morocco arrest. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB120424448908501345.html

Viégas, F. B. (2005). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated Communication*, **10**(3), article 12. doi:10.1111/j.1083-6101.2005.tb00260.x

Wallace, J. D. (1999). Nameless in cyberspace: Anonymity on the Internet. *Cato Institute Briefing Papers*, No. 54, December 8. Retrieved from http://www.cato.org/pubs/briefs/bp54.pdf

Wilson, C., & Dunn, A. (2011). Digital media in the Egyptian revolution: Descriptive analysis from the Tahrir data sets. *International Journal of Communication*, **5**, 1248–1272.

Wood, J. (2011). Underground in Beirut. *Boston Review.* August, 1. Retrieved from http://www.bostonreview.net/BR36.4/josh_wood_syrian_activist_arab_spring_lebanon_beirut.php

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

York, J. (2010). Policing content in the quasi-public sphere. *OpenNet Initiative Bulletin*. Retrieved from http://opennet.net/policing-content-quasi-public-sphere.

Zhuo, J. (2010, November, 30). Where anonymity breeds contempt. *The New York Times*, **A31**.

Zittrain, J. (2009, May 6). How to get what we all want. Cato Institute [blog]. Retrieved from http://www.cato-unbound.org/2009/05/06/jonathan-zittrain/how-to-get-what-we-all-want/

社会媒体和激进分子的工具包：现代社会运动的用户协议、企业利益和信息基础建设

William Lafi Youmans

密歇根大学

Jillian C. York

电子前沿基金会

【摘要：】

人们认为突尼斯，埃及以及其他地方的暴动部分是因为对社会化媒体平台，如 Facebook 和 Twitter 创造性的运用。然而，社交媒体背后的公司信息政策可以压制社会活动者和赋予独裁政权权利。本文通过分析 Facebook 对埃及“我们都是萨伊德”组织隐私问题的反应，YouTube 对来自叙利亚视频的反应，摩洛哥效忠者对阿拉伯无神论者出现在网络上的回应，以及叙利亚电子军队的活动，说明禁止匿名、社区监控行为、专制效忠者的运动，以及平叛策略是如何阻止民主人士的。大规模的、以商业为目的的社会传媒企业所面临的设计挑战是导致这些问题出现的原因。

Les médias sociaux et le coffre à outils de l'activiste : les contrats d'utilisation, les intérêts commerciaux et l'infrastructure informationnelle des mouvements sociaux modernes

William Lafi Youmans

Jillian C. York

Les soulèvements en Tunisie, en Égypte et ailleurs ont en partie été attribués à l'utilisation créative des plateformes de médias sociaux comme Facebook et Twitter. Pourtant, les politiques informationnelles des entreprises qui sont derrière les médias sociaux peuvent entraver les actions des activistes et donner du pouvoir aux régimes autoritaires. Une analyse de la réaction de Facebook face aux inquiétudes quant à la confidentialité concernant le groupe égyptien « We Are All Khaled Said » (*Nous sommes tous Khaled Saïd*), de la réaction de YouTube aux vidéos en provenance de Syrie, de la réaction des loyalistes marocains à la présence en ligne d'arabes athées et des activités de l'Armée électronique syrienne illustre comment l'interdiction d'anonymat, les pratiques de surveillance d'une communauté, les campagnes de loyalistes autoritaires et les tactiques de contre-insurrection jouent en défaveur des partisans de la démocratie. Ces problèmes découlent des défis de conception auxquels font face les entreprises de médias sociaux à grande échelle et à but lucratif.

Mots clés : médias sociaux, contrats d'utilisation, sites de réseautage social, printemps arabe, action collective, confidentialité, mouvements sociaux

Soziale Medien und der Werkzeugkasten des Aktivisten: Zustimmung der Nutzer, Firmeninteressen und die Informationsinfrastruktur moderner sozialer Bewegungen

Die Aufstände in Tunesien, Ägypten und anderswo wurden zum Teil dem kreativen Umgang mit sozialen Medienplattformen wie Facebook und Twitter zugeschrieben. Allerdings kann die Informationspolitik der Firmen hinter den sozialen Medien Aktivisten beschränken und autoritäre Regierungen bemächtigen. Die Analyse der Reaktionen von Facebook auf Bedenken hinsichtlich der Privatsphäre seitens der ägyptischen „Wir sind alle Khaled Said“-Gruppe, YouTubes Antwort auf den Zustrom von Videos aus Syrien, die Antwort marokkanischer Loyalisten auf den Onlineauftritt atheistischer Araber und die Aktivitäten der syrischen elektronischen Armee zeigen, wie Verbote bezüglich der Anonymität, politische Praktiken auf Community-Ebene, Kampagnen von autoritativen Lokalisten und Widerstandstaktiken gegen die Befürworter der Demokratie arbeiten. Diese Probleme rühren von den designbezogenen Herausforderungen, die an große, profitorientierte soziale Medienunternehmen gestellt werden.

Schlüsselbegriffe: soziale Medien, Nutzerbestimmungen, soziale Netzwerkseiten, Arabischer Frühling, kollektives Handeln, Privatsphäre, soziale Bewegungen

소셜미디어와 행동주의자 도구들: 사용자 동의들, 기업적 관심들, 그리고 현대 사회적 운동의 정보 기반들

William Lafi Youmans

Jillian C. York

요약

튜니지아, 이집트, 그리고 여러 곳에서의 대중항쟁은 페이스북과 트위터 같은 소셜미디어 플랫폼의 창의적 사용에 부분적으로 기인하였다고 할 수 있다. 그러나 소셜미디어 회사들의 정보 정책들은 행동주의자들을 억제하였고 권위적 정권에 힘을 보태주었다. 이집트의 We Are All Khaled Said 그룹과 관련된 개인정보노출 우려에 대한 페이스 북의 대응, 시리아로부터 오는 비디오들에 대한 유튜브의 대응, 무신론 아랍인들의 온라인 노출에 대한 모로코의 반응, 그리고 시리안 군대의 반응들에 대한 분석은 어떻게 익명성의 금지들, 커뮤니티 경찰 실행들, 권위주의적 충성자들로부터의 캠페인, 그리고 반대중 봉기적 전략들이 민주주의 지지자들에 반해 이루어 지는가를 잘 보여주고 있다. 이러한 문제들은 수익을 추구하는 소셜미디어 기업들이 해당 소셜미디어의 디자인을 통해 통제하려 하기 때문에 나타나는 것이다.

Los Medios Sociales y el Juego de Herramientas del Activismo: Los Acuerdos de los Usuarios, los Intereses Corporativos, y la Infraestructura de la Información de los Movimientos Sociales Modernos

William Lafi Youmans
University of Michigan, Ann Arbor

Jillian C. York
Electronic Frontier Foundation

Resumen

Las revueltas en Túnez, Egipto, y en cualquier otro lugar han sido debido en parte al uso creativo de las plataformas de los medios sociales tales como Facebook y Twitter. Aún las políticas de información de las firmas detrás de los medios sociales pueden inhibir a los activistas y dar poder a los regímenes totalitarios. Un análisis de la respuesta de Facebook a las preocupaciones sobre la privacidad con el grupo de Egipto “Somos Todos Khaled Said”, la respuesta de YouTube al suministro de videos que venían de la respuesta leal de Siria y Marruecos a la presencia online de Árabes ateos, y las actividades de la Armada Electrónica de Siria ilustran cómo las prohibiciones sobre la anonimidad, las prácticas de las políticas comunitarias, las campañas de los autoritarios leales, y las tácticas de la contra insurgencia trabajaron en contra de los defensores de la democracia. Estos problemas emergen de los desafíos del diseño que enfrentan las compañías buscadoras de ingresos de los medios sociales de larga escala.