CITIZENS AS ACTORS

Bruce Etling

The Internet has not led to radical new forms of direct democracy, as some predicted in the early days of the Web, but it is hard to look at the major protests and political changes that have swept across the globe recently and not see myriad ways in which the Internet has empowered citizens. Online tools continue to aid citizens in efforts to check government and corporate power and to highlight cases of corruption and abuse of power. The networked public sphere has continued to mature into a political force, marked by important victories such as the thwarting of the Stop Online Piracy Act (SOPA), Protect-IP Act (PIPA), and Anti-Counterfeiting Trade Agreement (ACTA). The Internet and social media have also enabled new forms of citizen dissent, the ethics of which are still under debate, including leaks of national security information by well-placed individuals in security bureaucracies and the emergence of "hacktivism" tactics as new forms of civil disobedience. In the most advanced of Western democracies, the Internet has created additional pathways for constituents to be heard by their representatives and made it easier for citizens to participate, through mechanisms such as e-voting in Switzerland. Still, the greatest changes to the citizen-government relationship appear to be those created at the grass roots by citizens, instead of those initiated from the top-down by governments.

> ***Without the Internet, the opposition to the AKP's popular but strong-handed rule may never have made it into the streets in such a spectacular fashion.***
>
> —ZEYNEP TUFEKCI
> "I was wrong about this Internet thing": Social Media and the Gezi Park Protests

The Internet and Protests

Citizens have increasingly used the Internet and social media to mobilize and coordinate protests. In the past few years alone, the world has seen a number of mass protests, including those connected to the Arab Spring in the Middle East and North Africa, those sparked by election falsification in Russia, disputes over public park space in Turkey, protests over an increase in public transportation fares in Brazil, the Indignados movement in Spain, and the global Occupy movement. A common undercurrent in many of these protests is citizen pushback against corruption, entrenched political elites, and economic inequality. These protests were not caused by the Internet, but online tools and social media platforms have played important information-sharing, coordination, mobilization, and community-building roles when economic, political, demographic, and other structural factors have aligned to create conditions conducive for protests and political change.

The most spectacular and far-reaching examples of Internet-enabled protests remain those associated with the Arab Spring, which led to the fall of entrenched dictators in Tunisia, Libya, Yemen, and Egypt. Those events also undercut many arguments put forward by skeptics that online talk is cheap, that online activism is not real activism, that the Internet is more useful for dictators, and that the region was immune to the gradual but continuing expansion of democracy. For example, research in Egypt shows that social media, in particular Facebook, provided new sources of information that the regime was not able to counter, and that social media use greatly increased the likelihood that

individuals would attend protests on the first day, when success is typically least assured and the risk of attendance the greatest. The Internet was also critical in shaping how citizens made decisions about the logistics of protests and their likelihood of success.[1] Researchers have also found evidence that social media played a central role in shaping political debates in the region, especially among the young, urban, and well-educated; that spikes in online revolutionary discussion often preceded major offline protest events; and that social media helped spread democratic ideas across international borders.[2] However, as events in the region since 2011 have shown, while the Internet may be especially useful for protests and issue-specific campaigns, social media have yet to provide an equivalent level of support to citizens in building democracy and creating new political institutions.

A significant benefit of the Internet is that it massively reduces the costs of mobilization and coordination of collective action. Event pages on social networking sites such as Facebook, Twitter, and similar local variants provide protest leaders with easy and low-cost ways to spread the word about protests and mobilize core constituencies and for protest participants to signal their intention to participate. Protesters can then also use social media sites, including video and photo sharing sites, to show the wider public their power in numbers, share popular signs and humorous memes, develop a group identity, and expose the reaction of the state, including government-sanctioned violence.

These tools are also used to provide alternative framings of the protest movement and protest activities. For example, while many have questioned the political impact of the Occupy movement, it is clear that the movement was able to push the frame of the "99%" into mainstream public discourse. The ability to put alternative framings and agendas into the public sphere is especially important in countries such as Russia, China, and Iran, where there is strong influence over or complete control of mainstream media outlets, including both print and broadcast. These tools also offer new ways for protesters to participate in movements and contribute to campaigns through, for example, creating, posting, and remixing user-generated video. More generally, online tools have also made easier identifying affinity groups and connecting divergent groups and parts of society that might have vastly different political platforms, but come together at times of political discontent and mass protests. Examples include nationalists and liberals in Russia united behind a common protest banner and Islamists, leftists, and youth movements in Egypt in the anti-Mubarak protests in 2011. Finally, the Internet and social media have created a public space for experimentation and learning at a local, national, and international level. This enables the diffusion of protest ideas and also allows movement leaders in one place to see what is working and what is not, and then adjust strategy, tactics, framings, and organizational efforts for greater success given local conditions.

In many cases, offline protest events are still critical for these movements and issue campaigns; the success of exclusively online action is still quite rare. However, in defeating the SOPA/PIPA legislation, online actions were probably much more important than the small, offline protests held in cities across the United States. The mix of offline and online organization also varies depending on the individual movement. For example, in Brazil's recent protests, offline organizational efforts by the Free Fare movement seem to have been important to organization of the initial protests, and helped to lay a foundation of dissent before just a small increase in transportation fares ignited large-scale protests. Those protests grew larger than anything seen before by organizers thanks at least in part to social media, and video evidence of police brutality also helped pull more Brazilians to the side of the protesters. It is worth highlighting that the Internet has been especially helpful for protests and

issue-specific campaigns, but in many instances has not led online protest leaders to run for office, create political parties, or otherwise participate in mainstream politics (although there have been exceptions, including in Russia, Tunisia, and the Tea Party in the United States).

While the media and many scholars tend to emphasize more positive examples of social media empowering democratic social movements and civil society, the Internet does not pick favorites. Those that society has intentionally marginalized from the political process—including extremists, nationalists. and nativists—can just as easily use the Internet. Still, those with ideas that are on the margins and have little support to begin with rarely gain mass followings solely because of a larger potential audience on the Internet. It may be easier for such individuals to find each other than it was in the past, but this does not mean their ideas have become more popular.

An Accountability and Fact-Checking Platform

Citizens living in a range of international settings and under various regime types continue to use the Internet as a check on corruption, mismanagement, and abuse of power by governments, corporations, and political and economic elites. China has provided a number of examples where netizens have been able to highlight corruption and malfeasance, abuse by local officials, and cover-ups of scandals that the government-controlled media would not cover. Examples include the tainted powdered milk formula scandal in 2008, the infamous Wenzhou high-speed train crash, and numerous examples of land disputes and ecological disasters. As a check on corporations, we also see cases where workers are increasingly expressing their demands for better pay and working conditions to international customers and national leaders, such as multiple strikes by employees of technology producer Foxconn.

> ***This past year has shown an especially significant rise in the prominence of primary source material originating from members of the general public. In numerous significant instances, individuals have engaged with primary source material to supplement mediated news content or highlight under-reported issues.***
>
> —JEFF HERMES AND ANDY SELLARS
> The Role of Citizens in Gathering, Publishing, and Consuming Primary Source News Content

Online communities are able to bring issues to the forefront of the public debate that would not occur otherwise, especially where political or economic elites have control over national media. Citizen journalism platforms, including Canada-based NowPublic, Global Voices internationally, and Ridus in Russia, among others, play an important role in surfacing and publicizing cases of corruption and abuse of local leaders. At least in China, the central government seems willing to let local leaders take the fall when this type of corruption and abuse become publicized, perhaps to let off steam in an otherwise tightly controlled political space, even if structural changes at the national level still seem far off.

The Networked Public Sphere and Issue-Specific Campaigns

The rise of social networking and digital communication technologies has facilitated the creation of the networked public sphere, broadly defined as an online public space where citizens can come together to debate and decide what issues are most salient as well as determine how to act on them. While critics argue that online organization and protests are not equivalent to those undertaken by previous generations of social movements, the networked public sphere has had some important recent victories that undermine this skepticism. The starkest examples are online efforts that killed Internet-related legislation that was pushed by the music and recording industries. In the United States, online efforts averted passage of the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). Soon after, the international trade agreement ACTA lost support in the face of similar civil society opposition. Individuals can play outsized roles in the networked public sphere: one example is the Houston blogger who started an online campaign to ban the use of 'pink slime' (which food writer Michael Pollan describes as a kind of industrial-strength hamburger filler made from a mix of slaughterhouse scraps and treated with ammonia) in the hamburger served in the federal school lunch program. Within days of the online petition, the USDA allowed schools to drop the product, and major supermarkets stopped carrying it. Recently though, it still seems that collectives—informal and formal civil society groups and social movements—have more effectively leveraged the Internet in support of issue-specific campaigns.

> ***Users of a number of online platforms, such as Reddit and various online gaming communities, successfully pushed technology companies to reverse their support for SOPA and PIPA.***
>
> —BRUCE ETLING
> The Defeat of SOPA, PIPA, and ACTA: The Networked Public Sphere Comes of Age

New Forms of Civil Disobedience

Networked technologies have also enabled new forms of civil disobedience. Two forms of digital disobedience have been on the rise recently: DDoS attacks that take down websites (and other "hactivist" tactics such as defacing opponents' websites) and leaks of national security information. The ethics and legitimacy of these tactics, to say nothing of the outcomes, continue to be fiercely debated. Even if consensus never emerges, it seems very likely that these news forms of civil disobedience will continue for the foreseeable future and that they will continue to be highly disruptive to traditional legal and political institutions. Leaks certainly occurred before the Internet, but the leak by Bradley (now

> ***As familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, what about tactics like street marches, picket lines, sit-ins, and occupations? Where is the space online for civil disobedience?***
>
> —MOLLY SAUTER
> The Future of Civil Disobedience

Chelsea) Manning of US diplomatic cables was unmatched in its scale and by Manning's choice to distribute the cables through the Internet via the Wikileaks website, instead of primarily through a traditional print publication.

> ***Website defacement activities during the Arab Spring have emerged as a common form of disruptive protest by rival groups.***
>
> —HELMI NOMAN
> Antagonism Uploaded: Website Defacements During the Arab Spring

The use of DDoS attacks by activists is controversial within digital activist communities. Some argue that DDoS attacks are also legitimate forms of civil disobedience. Others view such activity as akin to digital vandalism. These types of attacks have taken place for decades, in support of a range of different causes, from the Zapatista movement in Mexico to more recent DDoS attacks both in support of and against Wikileaks. DDoS attacks are also frequently used by proxies of the Russian, Chinese, and Syrian governments to attack domestic and international opponents of those regimes. In the case of the Russian election protests, DDoS attacks were also used by the Russian branch of Anonymous to take the website of the pro-Putin youth group Nashi offline. Hackers also released internal Nashi emails that purportedly proved that the group pays journalists and online communities for positive coverage of itself and the Russian government.

The long-term political impacts of these new forms of civil disobedience remain unclear. The Manning case does not seem to have led to any major changes in US foreign policy or to drastic shifts in US public opinion against the wars in Iraq and Afghanistan, and Manning has since been sentenced to 35 years in prison. The US State Department cables Manning leaked to Wikileaks appear to have had a larger impact in other countries. For example, the leaked cables appear to have played a role to the Arab spring protests after they were used by activists to attest to the corruption and excesses of the rulers at the time. The evolving Snowden case, however, has led to a national and global conversation about US government surveillance practices, the role of private companies in these practices, and user privacy. The efficacy of DDoS attacks is not entirely clear either, since most sites come back online fairly quickly. DDoS and other hacker attacks seem most useful in raising awareness and gaining attention for social movements, a critical issue for all activists who, even in the new media ecosystem, still struggle to gain attention among the many new voices and sources of information available in the broader media ecology.

> ***The technical underpinnings of our digital interactions are so complex that the average Internet user doesn't have the know-how to build their own tools to browse the web, much less to interact securely and privately online. Instead, consumers rely on "free" platforms built by software companies to communicate and browse the Internet.***
>
> —ASHKAN SOLTANI
> The Privacy Puzzle: Little or No Choice

Despite the success of citizens in pushing back against governments and corporations, large institutions continue to dominate the Internet space. This makes it difficult for individuals to act autonomously and securely

online, especially for activists who may work at cross-purposes to both corporate and government interests. Platforms and software exist that can help citizens counter this trend, such as anonymizers and tools for encryption and secure email and speech. Unfortunately, these tools have not yet gained wide adoption beyond the most tech-savvy of users, but that may change as a result of revelations about the reach of NSA and other government surveillance programs. The renewed interest in these tools was demonstrated recently by the tremendous increase in subscribers to Lavabit's secure email service, whose owner ultimately closed the company instead of betraying his promise to provide secure email to his customers. But this example also points to a weakness of these tools, as they are often run by small companies or groups of users that do not have the legal and lobbying clout to push back against governments.

> ***On June 30, 2013 prompted by revelations of surveillance programs in the US and UK, former Union of International Associations Assistant Secretary-General Anthony Judge published a detailed proposal titled "Circumventing Invasive Internet Surveillance with Carrier Pigeons."***
>
> —REX TROUMBLEY
> Flying Past Firewalls: Pigeons as Circumvention Tools?

Conclusion

Digitally mediated collective action by individuals and groups is constantly evolving as activists continue to experiment, learn, and adapt from one another and from the reaction of states, corporations, and other power holders to their efforts. Recognizing the importance of online, grassroots support, corporate and state actors are increasingly trying to harness the power of the Web as well. It is unclear if governments and corporations will be able to create "astroturf" online communities that have the authenticity and legitimacy of emergent protest movements, but it may be enough to sow fear, uncertainty, and doubt through well-financed misinformation campaigns. It is also unclear how widely the lessons of single-issue campaigns such as SOPA/PIPA can be applied, or if new forms of digital disobedience will ever be accepted by majorities as legitimate political acts. The power dynamic between governments, corporations, and citizens has not been totally overturned, but digitally empowered civil society actors continue to disrupt that status quo in ways that was hard to imagine even just a few years ago, and on a global scale that has surprised even the most optimistic among us.

Notes

1. Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square," Journal of Communication, 62 (2012) 363-379.
2. Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hussain, Will Mari and Marwa Mazaid, "Opening Closed Regimes: What was the Role of Social Media During the Arab Spring?", Project on Information Technology & Political Islam: http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.

"I WAS WRONG ABOUT THIS INTERNET THING": SOCIAL MEDIA AND THE GEZI PARK PROTESTS

Zeynep Tufekci

"I was wrong about this Internet thing."

I heard this sentiment again and again during my interviews at Gezi Park, Istanbul, during the height of the protests in June 2013. The protests were sparked by top-down plans to raze a small park in the city's historic Taksim square in the Beyoğlu district, an area known for its concentration of artists, nightlife, and theaters, and to replace it with a shopping mall and a hotel fashioned as a replica of the Ottoman Barracks that had once stood where the park was.

This growing realization of the Internet's power came from middle-aged people who had previously chided youth for their attachment to screens, phones, and social media. Yet when Turkey's heavily self-censored corporate media—owned by large conglomerates that vie for lucrative construction, energy, and urban renewal contracts from the government and that use their mass media outlets as a means to curry favor with the powerful ruling party, the AKP—broadcast penguin documentaries and cooking shows while ignoring the multi-day clashes between protesters and the police at the center of the most populous city in the country, it was social media that got the news out to the bewildered, angry residents of Istanbul.

At least 50 percent of the population of Turkey is online, most through broadband connectivity. Mobile devices are ubiquitous as well—the number of cell phone subscriptions cover about 90 percent of the population. Twitter has become the medium of choice for the protesters, who favor it for its lightweight applications on mobile devices, short texts, and ability to get news with pictures out quickly to large numbers of people. With estimates as high as 39 percent of Turkey's Internet users adopting the platform, and daily "trending topics" wars between supporters of AKP and Gezi protesters, it was not a huge surprise when the Prime Minister Erdogan singled out the platform and called it a "menace to society. The biggest lies are all there."[1]

Many protesters were convinced that without Twitter's ability to spread news quickly and widely, they could not have organized such large-scale action. Many had wrestled with the problem of false reports on Twitter, targeted by Erdogan as an indication of platform's untrustworthiness, and had undergone a crash course on social media literacy. "I have learned which accounts to trust and how to verify information," many told me. Others went a step further: "If I hear of clashes, I personally try to get there and take a picture to provide proof," a protester told me, while showing a wound in his leg from being hit with a tear gas canister while on a mission to verify and report.

Despite AKP officials' blatant dislike of social media as source of dissent, the Internet was not unplugged either in the Gezi Park or in the country, nor were any of the platforms shut down. Instead, the AKP seems to have decided on a strategy of engaging in a public relations blitz on social media by hiring "6,000 social media experts" itself,[2] increasing its efforts to force social media companies to open offices in Turkey so that the government can acquire user IP's in response to court rulings (currently Facebook and Google have offices in Turkey, but Twitter does not), and relying on its total dominance of mass media. In fact, polls showed that majority of AKP supporters believed that the

protests were "organized by foreign sources," a claim repeated multiple times by the prime minister and other AKP officials on mass media. AKP officials have also announced that they will pass new laws to "regulate misinformation" on social media—sending a clear signal that Turkey's Internet users will come under close scrutiny.

However, Turkey's electoral system, designed by generals in the 1980 coup, makes it very hard for new parties to break into the parliamentary system. This barrier, coupled with the incompetence of legacy opposition parties—which cannot be replaced, thanks to the said electoral system—and the AKP's own powerful electoral machinery, makes it unlikely that a social media-organized opposition will mount an effective electoral challenge in the 2014 elections.

Without the Internet, the opposition to the AKP's popular but strong-handed rule may never have made it into the streets in such a spectacular fashion. It remains to be seen if they can find their way into the voting booth in the face of corrupt mass media, a skewed electoral system, and a smart, powerful, and dominant ruling party that is ready to both beat them and join them online.

Notes

1. Will Oremus, "Turkish Prime Minister Blames Twitter for Unrest, Calls It 'the Worst Menace to Society,'" Slate, June 3, 2013, http://www.slate.com/blogs/future_tense/2013/06/03/turkey_protests_prime_minister_erdogan_blames_twitter_calls_social_media.html.
2. Ayla Albayrak and Joe Parkinson, "Turkey's Government Forms 6,000-Member Social Media Team," Wall Street Journal, September 16, 2013, http://online.wsj.com/article/SB10001424127887323527004579079151479634742.html.

THE ROLE OF CITIZENS IN GATHERING, PUBLISHING, AND CONSUMING PRIMARY SOURCE NEWS CONTENT

Jeff Hermes and Andy Sellars

For over a decade, scholars have noted the increased role that those outside the institutional press play in informing the public. This past year, however, has shown an especially significant rise in the prominence of primary source material originating from members of the general public. In numerous significant instances, individuals have engaged with primary source material to supplement mediated news content or highlight under-reported issues. This engagement has involved both the gathering of primary source material to share with others and the collective analysis of such material by loosely-connected networks of experts, analysts, and commentators.

Over the past year, several major news stories were broken by concerned citizens and activists gathering and disclosing direct evidence of government and political activity, including the videos shot by citizens of Damascus documenting the use of chemical weapons in the Syrian civil war; the "47 percent video" recorded by a member of the catering staff at an event held for presidential candidate Mitt Romney; the PRISM slide deck and other NSA materials disclosed by Edward Snowden to The Guardian; and the "lady in red" photo of Ceyda Sungur, which served as a unifying moment for anti-government protests in Turkey. This year has also brought unexpected collaboration between citizen media and law enforcement, including during the investigation into the Boston Marathon bombing, where the FBI actively solicited terabytes of eyewitness photographs and video to help identify the bombers.

In the United States, courts have begun to recognize a constitutional right of citizens to engage in this form of direct documentation, at least when directed at the actions of the government. Following the 2011 decision of a federal appeals court in Glik v. Cunniffe, a second federal appellate court recognized a First Amendment right for citizens to record the police in ACLU v. Alvarez. Marking a rare intervention in the behavior of state law enforcement, the Department of Justice's Civil Rights Division also stepped in to support the rights of citizens to record the police in a case pending in federal court in Maryland, Sharp v. Baltimore Police Department.

Private organizations, including MuckRock, Open Corporates, OpenGov, and MapLight, continue to provide resources to facilitate access to public records and government data and publish relevant documents. Judicial attention to transparency with electronic government records has increased concurrently, punctuated in the United States by cases addressing GIS mapping data and access to government document metadata. Meanwhile, a number of organizations, including Public.Resource.Org, SCOTUSblog, and the Oyez Project, have obtained funding, favorable judicial rulings, or other support for efforts to mirror general government data on their own websites.

While the creation and surfacing of primary source material by citizens has been seriously questioned only when the source breaches a duty of confidentiality over the information disclosed, such as the disclosures of Edward Snowden, significantly more criticism has been voiced as citizens move from documentation roles into analysis roles. This complexity was best highlighted during the events surrounding the Boston Marathon bombing. While public documentation of the incident was critical to the law enforcement investigation, the public's desire for information at a rate faster than the

government (or traditional news sources) would provide it led many citizens to try to parse primary source material directly. The results of these efforts were mostly negative; attempts to locate the bombers using online platforms like Reddit (on early iterations of /r/findbostonbombers) and to gather more information on the day of the Tsarnaev manhunt by listening to police scanners led to misidentifications and confusion – although similar criticisms were appropriately leveled against institutional news outlets for similar behavior. The increasing social recognition of traditional media ethics around verification of information posted on these sites has led to a richer and more expedient dissemination of information than traditionally thought possible through institutional media outlets.

The increased role of citizens in surfacing and analyzing documents has helped break news stories and improve public understanding of issues, but not all government activity with respect to primary source material has favored publication. Even in the United States, a nation that prides itself in transparency and free speech, the government has aggressively punished some of these disclosures. This has included a notorious criminal prosecution against activist Aaron Swartz for gathering thousands of academic articles for an undisclosed future use, which received significant attention and scrutiny following Swartz's suicide. The Department of Justice also obtained a conviction against Andrew Aurenheimer for accessing an unprotected AT&T website, escalating the charges from a misdemeanor to a felony based on Aurenheimer's disclosure of the data he obtained from the AT&T website to news website Gawker as evidence of AT&T's security vulnerability. (This case is now on appeal.) In August 2013, the United States also sentenced Chelsea Manning to 35 years in military prison, following her disclosure of thousands of documents to the organization Wikileaks. The position reflected in the pending federal shield bill—that citizen media and organizations dedicated to surfacing primary source material are not "journalists" worthy of protection—further underscores the continuing reluctance of the government to recognize the critical role that primary source material plays in informing the public.

THE DEFEAT OF SOPA, PIPA, AND ACTA: THE NETWORKED PUBLIC SPHERE COMES OF AGE

Bruce Etling

Arguably the most striking example of the rise of the networked public sphere as a political force is the reversal of support for the Stop Online Privacy Act (SOPA) and the Protect IP Act (PIPA) in the United States, and the international trade agreement ACTA, which lost support after the successful defeat of SOPA and PIPA.[1]

A number of successful tactics were used to support the movement, which culminated in January 2012 when millions of citizens contacted Congress to voice opposition to the legislation. Specialized tech media news outlets such as Tech Dirt, which exist primarily as web native media, as well as groups dedicated to digital freedoms, including Public Knowledge, the Center for Democracy and Technology, and the Electronic Frontier Foundation, played a critical role in sounding the alarm early and pushing the issue into the mainstream public sphere. Major online platforms and their communities of users, in particular Wikipedia, blacked out their websites and simultaneously pointed US voters to contact information for their elected representatives in Congress. Critically, the technology industry was also opposed to the legislation, although opposition was not universal. Google in particular, with its huge online user base and lobbying power, was also a major player in coming out against the legislation, placing a banner on its site in opposition to the legislation and connecting users to their Congressional representatives.

Users of a number of online platforms, such as Reddit and various online gaming communities, successfully pushed technology companies to reverse their support for SOPA and PIPA. A superb example is the Reddit community's boycott of web-hosting company Go Daddy, where a single user mobilized the community to begin moving their websites to other domains. The boycott quickly led Go Daddy to withdraw its support for the legislation. The online community was also able to draw on and promote expert commentary and analysis by Internet engineering pioneers to rebut the claims made by the content industry. Bloggers also used the space to take down the specific claim that the cost of piracy in the US is $58 billion, a number bloggers showed was vastly overblown and based on faulty assumptions.

These tactics may not be applicable against all types of legislation; they also appear to be less effective in countries with less democratic forms of government. For example, although the international agreement ACTA was stalled after the SOPA/PIPA reversal in the United States, the online community in Russia was not able to stop the passage of recent Internet legislation that now allows deep-packet inspection and gives the Russian government the ability to take down websites. This occurred even though opponents to the legislation adopted many of the same successful tactics used against SOPA/PIPA, including a blackout of Russian Wikipedia, support from Russian technology companies and their leaders, and active opposition from the Russian online community. Further, even in the United States, this type of online action cannot necessarily overcome a well-funded lobbying and advertising campaign by major industry players, as seen with the reversal of public opinion against Proposition 37, a GMO labeling initiative in California. That initiative saw opinion swing from solidly opposed (by nearly 3 to 1), to eventual passage by 3 percent at the polls thanks to a multi-million dollar adver-

tising blitz by the chemical industry (most prominently Monsanto), major processed food companies, and grocers. Money and corporate influence have not been eliminated from the political process, but there have been some important victories when the legislation concerns the Internet and in places where governments are responsive to citizen demands and public opinion. Still, it may also be the case that SOPA and PIPA are a harbinger of future online civil society action, as the tools and tactics used in this case gain adoption by civil society more broadly.

Notes

1. For a detailed analysis of this case see: Yochai Benkler, Hal Roberts, Rob Faris, Alicia Solow-Niederman, and Bruce Etling, "Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate," July 25, 2013, http://cyber.law.harvard.edu/publications/2013/social_mobilization_and_the_networked_public_sphere.

THE FUTURE OF CIVIL DISOBEDIENCE

Molly Sauter

This article previously appeared in a different version on the Io9 website.

The Internet is a central zone for political organizing. When there is a message to get out or a group to build, most people will turn to the Internet and the tools and networks on it. Online, people sign petitions, investigate stories and rumors, amplify links and videos, donate money, and show their support for causes in a variety of ways. But as familiar and widely accepted activist tools—petitions, fundraisers, mass letter-writing, call-in campaigns and others—find equivalent practices in the online space, what about tactics like street marches, picket lines, sit-ins, and occupations? Where is the space online for civil disobedience?

The affordances of networked technologies mean our opportunities for effective political activism have increased exponentially. Where activists once put their physical bodies on the line to fight for a cause, they can now engage in digitally based acts of civil disobedience from their keyboards. Digitally based civil disobedience is developing along three major lines: Disruption, Information Distribution, and Infrastructure. Each works to empower the public, and each has its own particular challenges and benefits.

Disruptive tactics like distributed denial of service actions and website defacements have a fairly long history in Internet terms. Activists groups like the Electronic Disturbance Theater, the Strano Network, pro-Palestinian groups, and others used DDOS and website defacements in their campaigns as early as the mid-1990s. These tactics disrupt the normal flow of information, directing attention to a cause and message. Disruptive tactics are popularly focused: they aim to deliver a message to as many people as possible, by either exposing them to disruption and dissent, recruiting them to take part, or both. To be effective, this type of civil disobedience needs to attract the attention of the public, typically through the mainstream media. If the media doesn't recognize or cover the actions as acts of protest, then the activist message falls flat. (If an activist defaces a corporate website, and no one sees it, does it have political impact? Probably not.)

Information Distribution-based tactics are built around the acquisition and release of information that someone doesn't want someone else to have. In the past three years, we've seen whistleblowing, information exfiltration, doxxing (releasing personal information, such as addresses and social security numbers, about others online), and crowdsourced vigilante investigations become the tactics of choice for groups such as Wikileaks and Anonymous and those they inspire. These tactics, in one way or another, move information from a state of low visibility to one of high visibility. Crowdsourced vigilante investigations and "human flesh search"-style manhunts try to bring public attention to injustices in cases where traditional law enforcement avenues seem to have failed. Anonymous has been developing this tactic in the US and Canada with Steubenville, #JusticeforReteah, and other operations. "Human flesh search" message boards are already popular in China, giving netizens the chance to bring formerly untouchable corrupt officials to justice. The FindtheBostonBombers subreddit was a homegrown example of this kind of crowdsourced vigilante investigation. The goal of this class of tactics is to empower people to take action by adding to the information landscape. Whistleblowers and leakers rely on the cooperation of the mainstream media to publicize, contextualize, and analyze

the information they release. This may become easier as more news organization recognize open paths for whistleblowers and leakers. Wikileaks' five media partners for the Cablegate documents, the New Yorker's Strongbox program, and the Guardian's extensive work with NSA whistleblower Edward Snowden are all examples of how cooperation between whistleblowers and news organizations is growing.

Infrastructure-based activism involves the creation of alternate systems to replace those that have been compromised by state or corporate information-gathering schemes. Tor, Diaspora, and identi.ca are examples, as are the guerrilla VPNs and network connections that often spring up—generally provided by activists in other countries—to serve embattled areas. Similar to living off the grid, these projects provide people with options beyond the default. Open source or FLOSS software and Creative Commons follow the same generative ideology: when the system stops working, create a new system. The challenge is to bring these new systems into widespread use without allowing them to be compromised, either in terms of ideology or of security for users. However, these new systems often have to fight network effects as they struggle to attract users away from dominant systems: Diaspora faced this issue with Facebook. Without being able to disrupt dominant systems, user migration is often slow and piecemeal, lacking the impact activists hope for.

Disruption, Information Distribution, and Infrastructure tactics and strategies are often practiced by separate groups working independently on different issues. Sometimes these groups' interests will overlap, as when Anonymous launched the disruptive Operation Payback in support of Wikileaks during Cablegate, but there is little inter-group organization. As the practice of civil disobedience develops online, those who favor different styles of activism but who are united in a common cause should organize themselves into affinity-based coalitions, building alliances for more effective activism. Effective digitally based civil disobedience needs a diverse, integrated repertoire of contention from which to draw. A disruptive action targeting Facebook could drive users toward alternate, more open, social networking services. A leak detailing government intelligence abuses could spur disruptive protests, consumer flight to uncompromised services, or further leaks.

As digital activism develops, civil disobedience will continue to a be vital tool for expressing dissent. The tactics and strategies of Disruption, Information Distribution, and Infrastructure provide many avenues for activists for activists to work together in concerted, effective campaigns. The Internet offers the unique opportunity to organize across geography, allowing for the creation of robust global affinity groups. To be the most effective, digital activists need to work together across the lines of tactics and strategy. The future of digital civil disobedience lies in inter-group, cross-border cooperation that combines the tactics and strategies of Disruption, Information Distribution, and Infrastructure-based activism.

ANTAGONISM UPLOADED: WEBSITE DEFACEMENTS DURING THE ARAB SPRING

Helmi Noman

The popular uprisings in the Middle East and North Africa (MENA) in 2011 polarized citizens in the region. People on both sides of the conflict took up their causes online, hacking and defacing websites, comment spamming on opponent Facebook pages, and using phishing URLs to gain access to targets' online accounts. Website defacement activities during the Arab Spring have emerged as a common form of disruptive protest by rival groups—a way not only to sabotage opponents' online presences but also to disrupt the flow of information and spread opposing messages during conflict.

Website defacements are not a new tactic in the region: these types of attacks took place earlier in the context of the Israeli-Palestinian conflict, in the antagonistic relationship between Morocco and Algeria over Western Sahara, and in the religiously motivated defacement of websites between Sunni and Shiite hacker groups. These activities were rare and limited in scope, but during the MENA uprisings, information operations conducted by politically motivated groups emerged online in a newly organized and intensive way.

One of the most widely active and visible of these groups is the Syrian Electronic Army (SEA). The SEA was organized in May 2011 and tends to target groups and individuals that the Syrian regime has singled out for supporting regime change.[1] The SEA has defaced the websites of public figures such as political cartoonist and outspoken critic of the regime Ali Ferzat, Syrian composer Malek Jendali, and Syrian singer Asalah Nasri, all of whom have been harassed by Syrian security forces or the Syrian Ministry of Information. The SEA has also defaced independent news and opinion websites such as Transparent Sham and Hadatha for Syria. As the conflict in Syria came under closer international scrutiny in mid-2013, the SEA began to focus more on compromising the Twitter accounts and websites of high profile international media organizations, choosing targets such as the New York Times based on their perceived biased coverage of the events in Syria.

Anti-government groups took a similar course of action: in February 2012, anti-regime hackers defaced Syria's pro-regime Addounia TV website by replacing the content of the front page with a defacement message that included links to YouTube clips of the regime's forces cracking down on protesters. Earlier in the same month, the TV's mobile news service was compromised, with the perpetrators sending "news alerts" supporting the uprisings.[2]

In Yemen, a pro-revolution group called the Union of Yemeni Hackers targeted government-controlled media websites to protest their reporting on the uprising in March 2011. The group defaced the websites of two state TV channels, Yemen TV and Sheba TV, with messages criticizing their "distortion of the facts."

In Egypt, Mubarak supporters exchanged attacks with pro-revolution websites and groups. One group known as Sons of Mubarak compromised several Facebook pages, including one run by the Muslim Brotherhood's political organization, the Freedom and Justice Party. The group left a message on the compromised page that read, "Sons of Mubarak will punish the revolution supporters" and vowed to attack websites that refer to Mubarak as a "deposed president" and websites that produce content

that "distort the history of Mubarak." In July 2013, the website of Tamarod (an opposition group dedicated to forcing President Mohamed Morsi to call early elections) was defaced by supporters of the Muslim Brotherhood. The defacement contained a message linking to a live stream of pro-Morsi demonstrations in Cairo.

A number of other defacements have taken place in the region outside of the context of large-scale revolutionary movements. During the September 2013 protests in Sudan over fuel price increases, during which as many as 200 protesters were killed, a Sudanese government website was defaced. The defacement message criticized the governmental religious establishment's stance that "disobeying the state head or president" via street protests was haram (forbidden by God). The message asked, "Isn't killing protesters haram?" In the same month, the website of the Prime Minister of Jordan was defaced with a message protesting the increasing cost of living in the country. In October 2013, the website of an online campaign supporting the right of women to drive in Saudi Arabia was defaced with a message that claimed to reveal the name and address of the person behind the site. A later defacement message on the same site vowed to persecute those who support the campaign.

Hacking and defacing activities are not limited to internal targets. In 2011, Syrian-Turkish relations deteriorated after Syria accused Turkey of interfering in its internal affairs and supporting rebel activities; in response, Turkey accused the Syrian regime of killing civilian protesters. Syrian and Turkish hackers responded by defacing several government websites in both countries. The SEA has also defaced websites in Libya, Israel, and the United Kingdom, as well as websites outside of the region, in an attempt to disseminate Syrian regime's version of the conflict. These targets include the websites of Harvard University, Purdue University, and the Lineberger Comprehensive Cancer Center at the University of North Carolina, as well as celebrity fan sites such as johnny-depp.org, ben-affleck.us, and bradpittweb.com.

Pro-revolution hackers in Syria have also attacked targets both inside and outside the region, including the site of an Iraqi oil company (mociraq.com), where they replaced the front page with a message reading, "The Iraqi regime, backed by the Iranian regime, is supporting the Syrian regime in oppressing Syrian people." The hackers replaced the website's banners with pro-revolution insignia, along with a photo of a child who—according to protesters—was killed by Syrian security forces during one of the demonstrations. They have also targeted the websites of the Russian Embassies in India and Singapore in protest of Russia's veto of a UN Security Council resolution to condemn the Syrian government.

Ethics and appropriateness

Many hacker forums set their own broad ethical guidelines, which are primarily based on political and religious considerations rather than national legal frameworks. These guidelines often argue that the incumbent regimes and their laws are part of the problem, and therefore can be legitimately ignored.[3] Sometimes the discourse on what constitutes an appropriate act of hacking focuses on the "Islamicity" of the act, with hackers invoking Islamic legal code to determine which websites are permissible targets. Aside from Fatwa-backed near-consensus on the permissibility of defacing and even destroying websites perceived to be anti-Islamic,[4] hackers generally interpret for themselves

which targets are acceptable. Political, religious, and sectarian divides remain the main governing references used by the hackers, with hacking justified according to political grievances. Interestingly, forums where the hacking of certain political or religious sites is tolerated have themselves become targets of sabotage by rival political hackers, leading such forums to limit participation to trusted and invited members only.[5]

Identifying those behind the attacks

The groups behind the information operations described above appear to be grassroots, civilian efforts, many of which disband quickly and or go through long periods of inactivity. Linking these operations to formal entities is challenging, as most of these groups leave few digital traces. Most groups use Facebook or hacker forums to publicize their activities, claim responsibility for attacks, and recruit followers. The SEA, which has its own website, is an exception.

The SEA's domain name and web hosting subscriber can both be traced to the Syrian Computer Society (SCS), which was founded by President Bashar al-Assad in 1989 and is currently run by his brother. This information suggests the SEA enjoys at least tacit support of the Syrian regime.[6] Investigating other information operations is more challenging, though some clues exist. For example, a YouTube video exists that shows a group of young people who claim to be the Libyan Electronic Army being lectured to by an officer of the Libyan military, who tells the group that their electronic activities come second in importance only to the military itself.[7]

Verifying attribution for attacks can also be problematic, particularly as some websites show more than one defacement message claimed by different groups at the same time. For example, the website of Egypt's Social Justice Party, defaced in August 2013, showed two claims of responsibility on two different pages: one from the Yemeni Electronic Army, and another from a Moroccan group.

Final remarks

Arab Spring fallouts are likely to fuel more defacement campaigns, the scope of which is likely to increase as related social and religious contentions increasingly manifest themselves online. At the same time, the continued growth in both the quantity and quality of Arabic hacker forums is likely to produce more computerized activism and to increase the level of sophistication and potential damage of that activism. Though signs of government complicity in the current defacement campaigns are limited, it is possible that government agencies will exploit to their advantage non-state hacker groups as a proxy to hide state information operations behind anonymous grassroots activism, and to crowdsource antagonism against state opponents.

Notes

1. Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," Infowar Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/.
2. SANA (Syrian State News Agency), http://www.sana.sy/eng/21/2012/02/06/398571.htm.

3. See, for example, the ethical code on the popular hacker forum Al-Jyyosh, http://www.aljyyosh.com/vb/showthread.php?t=32358 (note: forum is password protected).

4. The author discusses this issue in his book chapter, "In the Name of God: Faith-Based Internet Censorship in Majority Muslim Countries," *Routledge Handbook of Media Law* (New York: Routledge, 2013). An earlier version is available from the OpenNet Initiative at https://opennet.net/sites/opennet.net/files/ONI_NameofGod_1_08_2011.pdf.

5. The hacker forum Al-Jyyosh limited its membership to trusted, invited users after an increase in the circulation of malware by adversaries.

6. Helmi Noman, "The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army," Infowar Monitor, May 30, 2011, http://www.infowar-monitor.net/2011/05/7349/.

7. See http://www.youtube.com/watch?v=Rh8W_CEQqTw.

THE PRIVACY PUZZLE: LITTLE OR NO CHOICE

Ashkan Soltani

The policies and common practices guiding online advertising put Internet users in a tough spot when deciding how to protect their privacy. The technical underpinnings of our digital interactions are so complex that the average Internet user doesn't have the know-how to build their own tools to browse the web, much less to interact securely and privately online. Instead, consumers rely on "free" platforms built by software companies to communicate and browse the Internet. In exchange for free services, consumers often allow these companies to track their activities and target advertising. Meaningful regulatory structure protecting users from online tracking abuses is also lacking; in fact, we even lack a clear sense of what it would mean to take advantage of a user of a free service. Currently, users must choose between accepting the options provided by these platforms and trying to independently navigate a complicated web of privacy tools and techniques. This decision is complicated by the fact that some of the do-it-yourself privacy protection measures available to consumers might put them at risk of violating arcane laws. The current policy landscape governing online tracking is woefully out of date and sometimes protects companies at the expense of consumer choice. As a result of the inconsistencies in this environment, users face a difficult puzzle when they attempt to protect their privacy.

The business model financing technology companies determines the privacy choices users are given. In the case of most platforms (browsers, social networks, phones, etc.) the model is built on monetizing consumers' data to deliver advertisements. As such, the defaults are typically set to encourage users to share information as broadly as possible to enable better targeting and measurement. While most of these companies offer users a selection of privacy settings, these are also designed with the company's bottom line in mind. This is a predictable outcome of the powerful incentive to maximize the value of user data by running complicated data mining algorithms that rely on large datasets. A selection of privacy settings can make users feel like they are in control, but these options are limited. This, combined with our knowledge that consumers rarely adjust the default settings, means that a few companies have implicit control over a majority of individual users' privacy settings.

There is no guarantee that companies will respect a user's stated preference to not be tracked, and users often lack the tools to confirm whether or not their preferences are recognized. Additionally, the companies responsible for much of this tracking are increasingly successful at circumventing blocking tools. Even if they may not undermine their own privacy setting options, they are not particularly inclined to adhere to preferences that are expressed through other vendors' software. My research has documented numerous cases of companies repeatedly circumventing the privacy settings developed by other companies that users utilize to protect their privacy. It is important to note that this kind of circumvention can violate regulations, and the Federal Trade Commission (FTC) has successfully held companies accountable for circumventing settings. So if a user (or researcher) notices a violation of this nature, there is an opportunity to rectify the situation. However, again, this depends on users being able to observe the infraction, which is far from guaranteed.

Particularly ambitious users can try to work around the sanctioned choices, but there are pitfalls here as well. There are some tools and techniques to mask online movements that a consumer could

cobble together in order to make it more difficult to track their online behavior. However, some these could be interpreted as violating the law. In particular, the Computer Fraud and Abuse Act (CFAA) poses a problem for innovations in privacy protection. The crux of a CFAA violation hinges on whether or not an action allows a user to gain "access without authorization" or "exceed authorized access" to a computer. In some cases, commonplace behaviors like managing cookies, changing browser headers, using VPNs, and even protecting one's mobile phone from being identified could be construed as an attempt to exceed authorized access to content. For example, clearing cookies is a commonly prescribed method to protect privacy (by limiting the ability for advertisers to uniquely identify a given user); however, by periodically clearing cookies—or using a browser's private browsing mode—users can easily bypass publishers' paywalls (e.g., the ten-articles-a-month limit at the New York Times). Under an unsophisticated judge's review, this could be interpreted as exceeding authorized access and is therefore a potentially prosecutable violation of the CFAA. This means that, by attempting to protect his privacy from one company, a user might "exceed authorized access" elsewhere (clearing your cookies to prevent Google from developing a profile could violate the NYT paywall).

This combination of circumstances severely limits users' choices to limit online tracking and protect their privacy. Most users stick with the business-supporting defaults set by the company and even those who deviate are still choosing among options designed to support a business model based on monetizing tracking. The ambitious users who step outside these pre-approved choices have to invest a great deal of time investigating privacy-protecting strategies and, even when they succeed in protecting themselves, may find themselves on the wrong side of the law. All of these factors make it hard to envision a way for the average Internet user to find a reasonable and effective way to protect his privacy.

FLYING PAST FILTERS AND FIREWALLS: PIGEONS AS CIRCUMVENTION TOOLS?

Rex Troumbley

On June 30, 2013 prompted by revelations of surveillance programs in the US and UK, former Union of International Associations Assistant Secretary-General Anthony Judge published a detailed proposal titled "Circumventing Invasive Internet Surveillance with Carrier Pigeons."[1] In it Judge discusses the proven competence of carrier pigeons for delivering messages, their non-military and military messaging capacity, and Chinese experiments to create pigeon cyborgs.[2] Judge acknowledges that pigeon networks have their own vulnerability (such as disease, hawks, or being lured off course by sexy decoys), but argues that others have proven pigeons are effective at transmitting digital data.

Judge's proposal has its roots in a series of earlier Request for Comments (RFC) to the Internet Engineering Task Force, the ad hoc body charged with developing and promoting Internet standards. On April Fool's Day, 1990, David Waitzman submitted an RFC on the idea of using carrier pigeons or other birds for the transmission of electronic data.[3] Waitzman called his new communication standard "Internet Protocol over Avian Carriers" (IPoAC). Nine years later, Waitzman issued a second RFC suggesting improvements to his original protocol.[4] On April 1, 2011, Brian Carpenter and Robert Hinden issued their own RFC detailing how to use IPoAC with the latest revisions to the Internet Protocol IPv6.[5]

Though all three RFCs were issued as April Fools' Day jokes, in 2004, the IPoAC idea encouraged the Bergen Linux group to send nine pigeons, each carrying a single "ping," three miles. (They only received four "responses," meaning only four of the birds made it.)[6] A few years later, an IT company in South Africa raced pigeons carrying data cards against the transfer speeds of their local Internet Service Providers and easily won.[7] A similar test by an British ISP in 2010 sent a pigeon carrying a microSD card loaded with a five-minute video 75 miles in 90 minutes, beating the time it took to upload the same video to YouTube via a rural farm's Internet connection.[8]

Before the advent of the global Internet and fast data-transfer speeds, it was common to physically carry information between storage devices. "Sneakernets," or the networks of people walking around in sneakers carrying digital data, haven't gone away. After the 2011 raid of Osama Bin Laden's compound, it was discovered that Osama had been evading US intelligence organizations by using a courier to send drafts of emails stored on USB drives from a nearby Internet cafe.[9] In the Kingdom of Bhutan an offline network project distributes digital educational resources, such as Khan Academy videos and archived Wikipedia articles, to hundreds of schools with no or slow Internet access.[10] USB drives have also been used to evade Internet restrictions in North Korea and Cuba.[11]

As governments and corporations increasingly block or monitor Internet communications, and as data production continues to outpace bandwidth speed increases, sneakernets are helping move data around. Pigeon-nets may not be too far behind.

Notes

1. "Circumventing Invasive Internet Surveillance with Carrier Pigeons: Rewilding the endangered world wide web of avian migration pathways," June 30, 2013, http://www.laetusinpraesens.org/musings/pigeon.php.
2. Noah Shachtman, "Cyborg Pigeons Revealed!," *Wired*, February 27, 2007, http://www.wired.com/dangerroom/2007/02/cyborg_pigeons_/
3. David Waitzman, "A Standard for the Transmission of IP Datagrams on Avian Carriers," RFC 1149, April 1, 1990, http://www.ietf.org/rfc/rfc1149.txt.
4. David Waitzman, "IP over Avian Carriers with Quality of Service," RFC 2549, April 1, 1999, http://tools.ietf.org/rfc/rfc2549.txt.
5. Brian Carpenter and Robert Hinden, "Adaptation of RFC 1149 for IPv6," RFC 6214, April 1, 2011, http://tools.ietf.org/rfc/rfc6214.txt.
6. Bergen Linux Group, "The informal report from the RFC 1149 event," http://www.blug.linux.no/rfc1149/writeup.html.
7. Lisa Zyga, "Carrier Pigeon Faster Than Broadband Internet," *Phys.org*, September 11, 2009, http://phys.org/news171883994.html.
8. Nate Anderson, "What's faster than rural Internet uploads? Carrier pigeons," *Ars Technica*, September 16, 2010, http://arstechnica.com/tech-policy/2010/09/carrier-pigeons-beat-rural-internet-upload-speeds/.
9. Declan McCullagh, "How bin Laden evaded the NSA: Sneakernet," CNN, May 13, 2011, http://news.cnet.com/8301-31921_3-20062755-281.html.
10. Rigsum Sheran Collection, http://www.rigsum-it.com/research/projects/sherig/.
11. Reporters Without Borders, "North Korea: Frontiers of Censorship," October 2011, http://en.rsf.org/IMG/pdf/rsf_north-korea_2011.pdf; and Nick Farrell, "Cubans face off government with USB sticks," *Tech Eye*, March 12, 2013, http://news.techeye.net/security/cubans-face-off-government-with-usb-sticks.