Limits to Internet Freedoms

Being Heard in an Increasingly Authoritarian World

Michael Nekrasov
UC Santa Barbara
Santa Barbara, California 93106
mnekrasov@cs.ucsb.edu

Lisa Parks
MIT
Cambridge, Massachusetts 02139
lparks@mit.edu

Elizabeth Belding
UC Santa Barbara
Santa Barbara, California 93106
ebelding@cs.ucsb.edu

ABSTRACT

The Internet is a critical tool for communication and knowledge acquisition in societies across the globe. Unfortunately, its use has become a battlefield for governments, corporations, and individuals to censor speech and access to information. In this paper, we present research into the use of social media for free speech in Turkey, Mongolia, and Zambia as a basis for discussing the limits of Internet freedoms. We discuss the actors, adversaries, social and technological limits, as well as limitations of existing tools for the free exchange of ideas on-line. We conclude with a discussion of how design and development choices for technology can affect marginalized communities, as well as the ethical and technical considerations for developing tools and applications that support Internet freedoms.

CCS CONCEPTS

•Security and privacy →Social aspects of security and privacy; •Human-centered computing →*Social content sharing;*

KEYWORDS

Social Media, Internet Freedoms, Free Speech, Censorship, Anonymity, ICTD.

ACM Reference format:
Michael Nekrasov, Lisa Parks, and Elizabeth Belding. 2017. Limits to Internet Freedoms. In *Proceedings of LIMITS '17, June 22–24, 2017, Santa Barbara, CA, USA, ,* 10 pages.
DOI: http://dx.doi.org/10.1145/3080556.3080564

1 INTRODUCTION

The Internet is pervasive in societies across the globe. As of 2016, 3.5 billion people, roughly 47 percent of the world's population, are connected to the Internet [54]. A substantial part of Internet activity comprises users who learn, play, converse, and access content for work, entertainment, and intellectual growth. Users connect with one another and spread ideas on a massive scale. Out of the total Internet users, 1.8 billion use Facebook to communicate, and countless others use blogs, news, and social media platforms. The Internet is the dominant tool for humans to access and share information; as a result the Internet is central to free speech and dissemination in the world today. The United Nations has declared free speech and Internet access as basic human rights [10, 16]. Internet access is a core component of personal, political, and economic life across the globe. Given the continuing growth and reach of the Internet, one would hope that the freedom to access and speak on-line is a growing resource.

However, as we move into 2017, authoritarianism is on the rise globally with 94 countries under non-democratic regimes [40]. Even previously democratic nations, such as Turkey, are increasingly cracking down on free speech. The West, often the advocate and defender of democracy, is likewise not immune. Europe and the United States are both seeing a rise in authoritarian governments [47, 60]. The rise of authoritarianism brings with it limits on Internet usage. While the United States acted in defense of these freedoms world wide in 2010 [28], the current US administration campaigned, among other things, on "closing that Internet up in some way" [33] and is already taking steps to eliminate net neutrality [39]. Even as the Internet continues to expand, digital freedoms are a resource under threat.

The Internet plays a critical role to freedoms in the world, but it is increasingly turning into a battleground. On-line content, forums, blogs, and news are increasingly censured. Protections against reprisals offered by on-line anonymity are stripped. Individuals, corporations and governments catalog discussions posted on social media for future exploitation. Hate groups use existing freedoms to attack individuals. Terrorist cells use the Internet to recruit and plan attacks. While citizens across cultures, ideologies, and economic class use the Internet to bridge understanding, others use it to create social division.

This paper explores the growing limits to free speech based on research conducted in Lusaka, Zambia; Ulaanbaatar, Mongolia; and Istanbul, Turkey from 2014-2016. As part of our research we reached out to diverse sets of communities to investigate Internet Freedoms and in particular their relation to social media use. We use this research as the basis of discussion into the limits, actors, and concerns in this space. Over the course of our research, we formally interviewed 110 people and had informal conversations with dozens more individuals. While our work provides only a small window into the broad set of limits that individuals encounter in on-line access and speech, the diverse perspectives, cultures, and struggles serve as a platform of understanding the limits to Internet freedoms in a global context.

LIMITS '17, June 22–24, 2017, Santa Barbara, CA, USA

DOI: http://dx.doi.org/10.1145/3080556.3080564

2 LIMITS TO SPEECH AND ACCESS

During our research, we sought out a diverse set of individuals, with independent and sometimes conflicting agendas. To understand the barriers they encounter, it is helpful to explore the competing motivations, the adversaries, and the tools they use to silence speech and block access. Existing tools, areas of growth, and a discussion about some of the ethical considerations when designing free speech technology follows in subsequent sections.

2.1 Seeking the Voices

Before understanding the limits on digital free speech and access, we identify the groups facing these barriers. From our research across the three countries, we interviewed a multitude of groups that struggled to access and post content on-line. These groups include: political activists, the press, minority groups, watchdogs and NGOs, and unaffiliated citizens.

Political Activists:
Political activists are the most common targets of censorship. Ruling politicians silence and discredit political rivals both physically and digitally. In Turkey and Zambia the ruling parties exercise legal suppression of dissenting opinion, shut down websites and arrest opposition leaders. Voices speaking out against the current government are prime targets for censorship.

The Press:
Journalists shared similar stories. In Turkey, news organizations, like Zaman [58], are physically raided and journalists are arrested for publishing content that defies the government. In Zambia, radio stations and newspapers are likewise raided and, in multiple reported incidents, shut down for printing, streaming, and publishing physical and digital content. When press organizations are shut down, some reporters continue to work as citizen journalists, publishing news on blogs and social media platforms. Many face arrests, law suits, and censorship of their content. Even single tweets on topics such as governmental corruption, lead to arrest of journalists [57].

Minority Groups:
People face censorship for reasons other than speaking out against the government. Those investigating minority issues are especially vulnerable. Journalists reporting on Kurdish treatment in Turkey face arrests, confiscation of their devices, and bullying. LGBTQ activists in Mongolia struggle with language censure that prohibits posting impolite words, including sexual terminology, even when using medically appropriate language [11]. When soliciting information about safe sex, their material is labeled pornographic in nature and prohibited. In Zambia, we interviewed an HIV health center that faced issues of getting past the stigma of the disease. Minority groups often look to technology to overcome societal barriers and engage open discussion.

Watchdogs and NGOs:
Watchdogs and NGOs also conveyed difficulty in reporting factual information. In Mongolia, groups are sued for libel when reporting on corporate environmental damage, and free press watchdogs face opposition when reporting on government crackdown on media. In Zambia, NGOs overseeing water projects are opposed by people unwilling to report corruption due to pressure from corporations and local governments. As these groups rely on accurate information to function, censorship and external interference inhibits their success.

Unaffiliated Citizens:
Unaffiliated citizens are also not exempt. In Turkey, we interviewed a gay man who was arrested and fined over a tweet [18]. Due to laws against insulting the government of Turkey, a single tweet is enough to warrant arrest. This discourages people from speaking out in the first place. Even if individuals do not find themselves in violation of the law, they can become collateral in large-scale censorship efforts. In times of social conflict, governments, like Turkey, shut down access to websites for all citizens [13]. Aside from government pressure, people living in Mongolia, Zambia, and Turkey looking for information such as LGBT issues face on-line bullying and social stigma.

2.2 Assessing the Adversaries

There are groups whose goals motivate them to restrict Internet freedoms. Agents imposing these limits are adversaries of free speech and access. They include: government, corporations, and communities.

The Government:
The most dominant adversary is usually the government. Governments all over the world litigate and enforce censorship of content [12, 23, 41–43]. Governments may do so to proscribe social norms, to stifle minority opinions, to ensure "safety", or out of political self-interest - suppressing news that would make the government look bad. Of the three countries in which we conducted research, the government of Turkey most directly imposed limits on free speech. Many times in the past several years, the Turkish government used technology to censor voices and cut off access to social media, including Twitter, Facebook, WhatsApp, and YouTube [13]. Turkey also aggressively enforced laws by policing content posted on-line, tapping phone conversations, and arresting political dissidents. In Mongolia, our interviews identified governmental focus on filtering speech, and banning and blocking sites based on content. In Zambia, our interviews suggested a government that acted through arrests and law suits to silence opposition.

Corporations:
Corporations are another critical adversary to on-line speech and access. They bring lawsuits against journalists and individuals under libel laws, using these suits as a deterrent from reporting on issues of corruption and environmental damage. In particular, on-line social networks play a large role in imposing limits on speech. By tracking users and gathering personal information, large social media sites like Facebook and Twitter provide tools for others to reveal identities of users. Reporting tools that can be used to flag posts as improper can also be used by other adversaries to silence speech. Additionally, by isolating users in content bubbles of like-minded users and suggested posts, users are shielded from dissenting ideas and opinions. Even if speech makes it onto social media, the echo chamber effect [24] can prevent it from ever being viewed or heard.

Communities:
The last and often most influential adversary limiting free speech is a person's community. Individuals that post views on controversial issues can be targeted by cyber bullies. Journalists reporting on sensitive topics, such as on Kurdish issues in Turkey, face constant barrage of hateful posts. In Zambia, it is difficult to voice an opinion in an on-line forum. A user's ethnicity, gender, and past posting record stereotypes the user. Resulting responses from the on-line community frequently target the physical characteristics or past political affiliation, over the content of discussion. Even in the confines of one's household, people encounter limits to their on-line freedoms. During a security training for a gender-based violence center in Mongolia, we heard stories of how husbands and partners break into email and social media accounts of their wives. The goal is to monitor communication and content access, and the result can be domestic violence.

Even when adversaries do not specifically target an individual they can force self-censorship. The same adversary that limits on-line communication can restrict physical media and create a conversational stigma. With an adversary in every corner, Internet freedoms are severely limited. When people are afraid to ask questions, or do an Internet search for fear of reprisal, they are cut off from resources that could improve their physical and mental well-being.

2.3 Techniques to Limit Freedoms

Adversaries place limits on Internet freedoms through legal action, technology, threat and violence, and control of infrastructure. These techniques allow adversaries to censor content, track users, and log communications.

2.3.1 Legal Action. Governments pass laws criminalizing discussion of certain topics. Even if no further action is taken, those laws serve as a deterrent for voicing opposing view points. Some laws, such as those banning insult of government officials in Turkey, are far reaching and suffice as cause for prosecuting individuals perceived as political threats. For anything ranging from public criticism to satirical tweets, celebrities, newspapers, activists, and unaffiliated citizens face criminal charges [19, 44].

Sometimes these lawsuits border on the absurd, such as when Dr. Bilgin Ciftci, a Turkish physician, went to court over a meme he created, comparing Erdogan, president of Turkey, to Gollum, a fictional character from Tolkien's *Lord of the Rings*. [53]. The doctor lost his job and is facing 2 years in prison. The outcome of his court case hinges on testimony from a panel of experts expounding on the moral character of Gollum in order to determine whether the meme was insulting the public official. Such wide enforcement makes even mundane opposition to the government dangerous for an individual.

In countries with strong libel laws, like Mongolia, politicians and corporations sue against unflattering reporting by alleging wrongful defamation of character. Using expensive legal teams, these libel plaintiffs are able to silence opposing viewpoints, intimidating those who may not have the monetary resources from fighting a legal challenge. Threats of libel suits also act as a deterrent.

Unlike voiced speech, which needs to be recorded to be saved, on-line content is tracked and archived. Even passing thoughts, formulated into late night tweets, that are later deleted, become a matter of record and can be called into evidence at a later date. When every word written can be used against them at a later date, individuals self-censor themselves when posting on-line.

2.3.2 Technology. In addition to retroactive enforcement of laws, adversaries use technologies for proactive censorship of content. Governments, such as Turkey, can enact broad DNS and IP bans that block entire sections of the web, targeting news and dissenting opinions [50]. As regimes become more restrictive they may block specific types of network streams, such as VPNs and TOR connections as was seen in Turkey last December [17]. Other governments, like those in China, employ comprehensive filtering of websites by topics and keywords [61]. Mongolia takes a more direct approach by mandating website hosts to install a program to filter content, including comments for slander and rude language, based on an extensive banned word list [14]. This makes access to local content on topics, such as sex, difficult.

When access is allowed, governments actively work to identify users. Internet service providers and mobile providers are often forced to register IPs and SIMs to real names. This allows arrests and intimidation, even on un-named accounts on-line. Some tracking is harder to detect. For example, some governments and individuals have deployed IMSI catchers, which are fake cellular towers that intercept calls and texts. IMSI catchers can log communication and register a phone's presence at a location, such as a protest [30]. While, in some cases, it is possible to bypass the tracking and censorship technologies with the use of proxy servers and VPNs, this brings other limitations that will be discussed in a section 3.

2.3.3 Infrastructure. Some limits to on-line speech manifest in a block to on-line access itself. Areas that are rural, underdeveloped, or war-torn, may lack the infrastructure to access the Internet in a meaningful way. This lack of infrastructure can be a byproduct of economic disincentives, difficulty due to physical obstacles, such as terrain, weather, and distance, or in some cases deliberate neglect. In Mongolia, towns we visited on the railway lack Internet access due to the tough terrain, expensive upkeep due to weather, inaccessibility, and lack of economic prospects for telecommunications providers. The lack of incentive is typical of rural communities, including those in Zambia and other parts of the world. As mentioned, sometimes infrastructure neglect is deliberate as it is a way of suppressing a particular community. In the case of the Za'atari refugee camp, Internet access was deliberately not provided in order to discourage refugees from encroaching on the labor market of Amman through on-line work [51].

Even when existing infrastructure is present, access to it can be rescinded. Governments may block Internet and mobile access for a region in response to events, such as protests. During such times, all citizens, not just members of the protest, lose access to news, communication, as well as access to digital financial transactions. This has been the case, among others, in Turkey, Egypt, and Syria [15, 27, 52]. Even when there is no deliberate block, protests or natural disasters can overload mobile networks and disrupt Internet access intermittently [29].

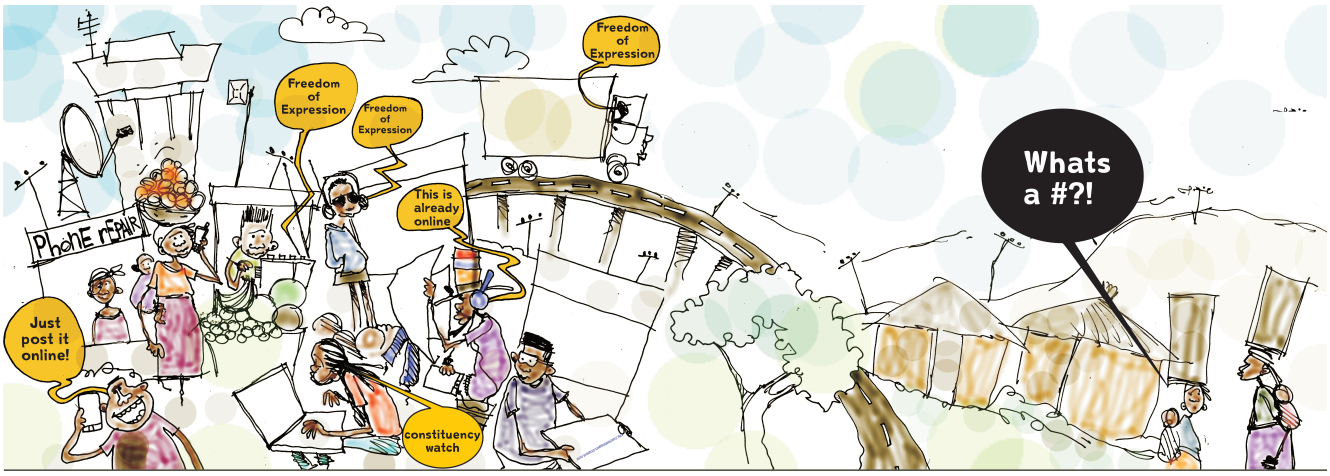

Figure 1: Political Cartoon by Kiss Brian Abraham commenting on the use of technology for freedom of expression in Zambia.

When infrastructure is present and functional, the cost, speed, and quality of Internet connectivity may restrict usage to a particular socio-economic class. Additionally, upload and download bandwidth and costs are not always symmetrical for users. Internet service providers regularly provide plans that allow downloads at a disproportionately faster rate than uploads. While users may have the capacity to consume content, their ability to voice their own ideas and culture might be limited due to upload caps. Projects that claim to provide free access, such as Facebook's Internet.org [21], may limit which websites are freely available to subscribers. Limiting access to infrastructure can be profitable to companies aiming to control consumer choice but detrimental to user freedoms.

While infrastructure limits to Internet access is comprehensibly studied by ICT4D literature, it is important to emphasize how lack of Internet access can be used to suppress the voice of a particular group or minority on-line. Connecting communities to the Internet amplifies their voice both globally and domestically. Hindering connectivity intentionally or through neglect censors a community and muffles their voice. The drawing shown in figure 1, by Kiss Brian Abraham, reminds viewers that while freedom of expression through technology is an active part of Zambian cities, those in rural Zambia lack the infrastructure to participate.

2.3.4 Threats and Violence. The enforcement of laws sometimes results in physical altercations. Before going through due process in court, police may make a show of violence when apprehending suspects. A manager was beaten by police at Komboni Radio in Zambia, which offers both radio broadcast in Lusaka and on-line streaming, and the radio station was temporarily shut down [20]. Government shows of force during arrest act as a deterrent for others thinking of speaking out. Even when no probable cause exists for arrest, police and government agents may use force to intimidate journalists or, in some cases, seize belongings. The search and seizure of devices is a major barrier to journalists reporting in areas with no Internet access [48]. Reporters who rely on their phones and laptops to store and ferry footage from conflict zones and are especially vulnerable to seizure as a means of censorship.

Aside from government agents, violence or the threat of violence is a powerful de-motivator on-line. Individuals who post on-line expose themselves to cyber-bullying. Bullies attack users personally using identifying information to tailor attacks. In an attack known as doxing, bullies find and release personal contact information, such as phone, email, or address, thereby inviting escalation against an individual [37, 56]. When personal information is known, attacks can escalate from threats to acts of violence. Associates and family members are likewise potential targets. Not only is this a technique for silencing the target, but acts it as a deterrent for others.

When on-line users post or search for content, they open themselves to targeted acts of hate. For example, searching or posting on LGBT topics can lead others to label individuals as non-heteronormative. These labels can impact job availability, interpersonal behavior, and trigger threats both from society at-large and at home [35]. At the gender-based violence center in Mongolia, we heard stories that husbands assault their wives based on search history or social media posts. When inquiry leads to such grave consequences, individuals are unlikely to take the risk and engage on-line.

There are many techniques that adversaries use to limit Internet freedoms, as we explored in this section. The barriers go beyond technological, extending into the legal, social, and economic. Aspects of these techniques can be countered by tools that, among others, circumvent censorship, anonymize users, and obfuscate communication.

3 LIMITATIONS OF EXISTING TOOLS

While aspects of the techniques to limit speech can be circumvented by large libraries of existing tools, these tools have limitations. In our research we sought to assess the successes and shortcomings of these tools to understand the capabilities individuals have to overcome limits. We found existing tools are often a poor fit for marginalized communities and fail to overcome limits in effective communication. To tackle imposed or naturally occurring barriers to on-line speech, users need tools from multiple technological facets.

3.1 Censorship Circumvention

As explored earlier, one of the direct ways that adversaries limit access to particular content is through the censure of websites. To overcome these blocks, users use circumvention tools. A common tactic is tunneling content through unblocked devices, such as proxy servers, that sit outside the control of a censoring adversary. Users funnel their normally blocked request via this proxy. The proxy relays requests and mirrors the responses from the desired website. While this technique is popular in regions where governments or corporations block content, it comes with some security drawbacks. Proxies are able to read requests made by the user and modify the results. Free proxy services allow user access in exchange for injecting advertisements into web pages. Users lose the ability to trust responses as the third party advertisers can modify web pages. The proxies are able to intercept user requests and can monitor any unencrypted user materials, such as passwords. Un-encrypted requests and responses can still be intercepted by Internet service providers as well as intermediate network routers. Adversaries monitoring the network can link these activities to a particular IP address.

Similar to proxies, Virtual Private Networks (VPNs) are used to relay network traffic from a device through an intermediary. This can allow users to access censored content. While proxy servers are typically used on an application basis, VPNs can be used to project network traffic through a remote server. Unlike proxies, the requests sent through VPNs are encrypted along with all other traffic while en-route to the VPN server. Once at the VPN server, unencrypted requests and responses can still be read and modified. Due to the added computation cost of encrypting and decrypting communication, VPNs are rarely free, and the encryption adds a processing cost to the user's device, which narrows the accessibility to certain socio-economic classes.

Many of the individuals we encountered in our research had heard of proxies and VPNs. In Turkey, where active IP and DNS filtering is common, many of the users, even those less technically proficient, had used proxies or VPNs as a tool for bypassing censorship blocks. Few, however, knew about the benefit to anonymity these approaches provided.

3.2 Anonymity

In addition to blocking content, adversaries track users for legal prosecution or as an intimidation tactic. Tracking identities in turn promotes self-censorship by the user. By providing a means of censorship-circumvention, proxies allow possible anonymity between requester and the desired website. However, if requests and responses are not encrypted, outside parties, such as governments and corporations, can still track users. Worse, proxies themselves may keep logs of interactions and share them with adversaries, either willingly or through subpoena. Proxies may keep lists of requested IPs, linked to users, which can serve as a hit-list for an adversary.

VPNs are only marginally better than proxies for anonymity. While all traffic to VPN servers is encrypted, the IPs of both the requesting device and VPN are visible on the network. If both the requester and the VPN is within a part of the network monitored by an adversary, traffic analysis can link the IPs to the final destination. While VPNs are employed by businesses, the act of using a VPN can still raise suspicion by an adversary policing censorship circumvention. If the VPN server is compromised or legally vulnerable to subpoena by an adversary, it may still be possible to get full access records. Corporations, such as Netflix [34], limiting certain groups of users from accessing content can also block VPN use.

Another popular approach to proxies, which provides better anonymity, is Tor. Tor is a network of proxies that relay encrypted data. Anyone can volunteer to become a relay of this network by running freely available software. Users connect to the network and funnel TCP streams through an entry node in the Tor network. The stream is relayed across multiple Tor relays. For a given stream, each Tor relay only knows the IPs of its two neighbors. Intermediate relays do not know the IP of the original requester nor of the destination. The packets in the stream are encrypted multiple times, like layers in an onion, with ephemeral keys of the intermediate nodes [31]. This type of system makes traffic analysis, linking the requester and intended destination, difficult. However, if enough Tor nodes are compromised, then traffic analysis is possible [46]. Even if adversaries are unable to de-anonymize traffic, downloading or using Tor is visible on the network and can flag an individual as a person of interest. In our research, we found that many technically proficient users knew about Tor, but that new users found the concept confusing and suffered language barriers when attempting to install and use it themselves.

Most social media platforms force users to reveal real identity. For example, Facebook, imposes a real name policy as part of the terms of service [9, 32], while Twitter requires a phone number to create an account. Additionally, social media platforms log access, including the IP of each request. Corporations can sell this data to other adversaries. Other websites can reuse tracking cookies left by social media to identify users. Governments can requisition these user records [2]. Using a service, such as a proxy server, VPN, or TOR can mask the accessing IP. However, if the account is ever accessed by a device with an IP tied to the user, that single interaction suffices to de-anonymize the entire account. As mentioned, in addition to monitoring censorship infractions, governments and corporations may go after users deemed offensive or dangerous by tying words or site visits to identity.

Revealing personal identities exposes users to threats from governments and corporations as well as bullying and violence from on-line and real world communities, including family members. When users know they are tracked, they self-censor posts and queries, which limits both speech and access to vital information. Even when adversaries lack the ability to identify users on IP, they can de-anonymize users based on the content they post. While using social media, users frequently post identifying information. An account using a fake name that posts a personal photo can instantly identify the individual. Less obvious details can still allow adversaries to guess identities, for example naming a school, age, and town of birth might be enough to uniquely identify an individual. As users generate content they expose identifying information. A dedicated attacker can correlate this information and call out the identity of the user. Doxing the user by an adversary exposes them to the threats mentioned in previous sections.

Use of anonymity tools, such as proxies, coupled with meticulous discipline can help protect users from adversaries. Unfortunately,

self-censoring all identifying information limits the content an individual is able to post and access. It is difficult to have frank conversations about personal issues, with the worry that every word can be used to reveal identity and expose the user to danger.

3.3 Reputation

While anonymity can help individuals access information and post without retribution, anonymous communication has drawbacks. Personal investment brings with it accountability, and while those seeking genuine discourse can use anonymity to be heard, others can use anonymity as a tool to attack. Without the reputation of the individual, anonymous accounts can have difficulty fighting for credibility. This is especially difficult for journalists and media outlets whose credibility is tied to reputation. During interviews in Turkey, we repeatedly heard that journalists were unwilling to use anonymity tools as it would strip them of credibility and prevent them from doing their job.

Nevertheless, over time, even anonymous accounts can earn credibility. Groups that share factual information on anonymous social media pages or blogs can build a reputation of credibility, tied to an assumed identity. In Turkey, an anonymous Twitter account, going by Fuat Avni, delivered information ostensibly from within the Turkish government. By repeatedly posting credible information, the account gained millions of followers and became the target of a government investigation [22].

Unfortunately, anonymous groups suffer from a variety of problems. When accounts are blocked or removed, the credibility chain is disrupted. Reestablished groups must provide evidence of continuity or risk forfeiting established reputation. Infiltrators joining the group or seizing the account can tarnish reputation as readers struggle to determine what information is factual and what is planted. Loosely formed groups that span accounts can have unclear affiliations. While the hacker group "Anonymous", for example, has some degree of reputation, almost any anonymous account can claim membership, muddying the message and reputation of the group. Cryptographic signatures can validate assumed identities, but are difficult to use in the social media context.

Additionally, there is a difference between anonymity of a group and that of an individual. A media organization may wish to retain its identity and reputation in on-line communication while protecting individuals in that organization from prosecution. The Zambia Watchdog used this approach, combining public and anonymous sources under a single identity to publish critiques of the government and expose corruption [48].

3.4 Broad Reach

When individuals and groups manage to make it on-line, their voices are only heard if they are able to reach a breadth of people. There are many tools that enable secure end-to-end encrypted communications for email, messaging, and content sharing. These tools are somewhat effective at disseminating information in a group securely but do little to communicate with broader audiences. Individuals and groups we interviewed were primarily interested in social media due to the ability to reach a large audience. Tools with narrow audiences limit viability in many of the use cases. Speaking to an empty room does little to share ideas.

Table 1: Number of languages in which tools are available.

Tool	Languages
Privacy Badger (Chrome) [5]	10
Confide (iOS and Android) [1]	15
Tor Browser [8]	16
Orbot (Android Tor App) [4]	25
Signal (iOS and Android) [6]	36
HTTPS Everywhere (Chrome) [3]	48

3.5 Crowding Out

When a post makes it to social media, overcoming the many barriers, it can still be silenced. Governments and corporations increasingly deploy bots, automated programs behaving like users, to crowd out dissenting voices [36, 45]. In comment sections on social media platforms and news sites, automated posts can overwhelm real discussion. On sites using ranking algorithms, bots can downvote posts, forcing them into obscurity. Some governments, such as Russia, go further and employ real people in "troll" farms [26, 59] to control the direction of discussion and suppress opposing viewpoints.

Even mechanisms enacted to protect users are frequently exploited. Reporting functionality, present on much of social media, allows users to flag posts as harassment or indecent. This is helpful in preventing cyber-bullying. Unfortunately, adversaries use bots or trolls to falsely report posts, generating mass complaints towards a user. Russia has been aggressive in silencing opposing views from popular accounts by falsely flagging content as containing violence or pornography, resulting in temporary and permanent account bans [55]. These attacks exploit automated moderation algorithms of platforms, such as Facebook, to temporarily or permanently ban accounts, thereby silencing dissenting voices.

3.6 Technical Literacy and Language

While a wide library of tools, including those discussed, exist to overcome limits to Internet freedoms, there is often a capacities mismatch between the developers and users. One of the most direct issues is language. Many security tools and corresponding instructions are only available in a small set of languages. When discussing security in Turkey, we attempted to introduce users to Tor. We found that Orbot, an Android application for Tor, was not available in Turkish. This was a barrier to usage as all instructions and user interfaces required explanation and translation. No application we examined had a Mongolian translation. While Zambia uses English as its official language, the 73 Zambian native languages were also absent. For a quick overview of language availability for a sampling of tools please refer to Table 1. Lack of instructions in a native language limits the ability to understand and use tools effectively.

Security tools are frequently used by those in computing fields who already have some level of technical literacy. Proper use of tools requires an understanding of the threat, purpose of the tool, and its limitations. In our interviews we found variation in technical expertise. While some were proficient and, in many cases, using tools for on-line interactions, many others were far less technically

literate. Many did not understand the mechanisms behind tracking or censorship, when they were vulnerable, or how to protect themselves. Those working in journalism, in highly dangerous conditions may have the interest but lack the resources to get the necessary training to overcome limits. Learning to use tools in a non-native language compounds the issue.

Individuals working with technology are not always literate in the vulnerabilities of their on-line activities. Users often do not worry about security and anonymity until they become targets themselves. When training undergraduates in computer science at Mongolian National University, the group showed little initial interest in learning about security tools. When we showed them a live demo of intercepting complete web pages running over HTTP on an unsecured wireless access point, the level of interest in protecting their identity and communication increased dramatically. Simply making users aware what aspects of their on-line activity is visible and to whom is a powerful first step to raising interest and overcoming future limits.

Even if an ideal tool existed to overcome each technical limitation, language and digital literacy would still hinder adoption. Access to language and technical experience may be tied to particular groups of individuals based on access to education and socio-economic status. The design and translation of tools can determine who is able to overcome the limits and speak, and who remains silent.

4 DISCUSSION

The capacity to speak and be heard is a powerful force with both societal and ethical implications. The decisions behind design, implementation, and deployment of technologies that overcome these limits can have the power to define which groups and ideas promulgate on the Internet. Empowering Internet speech is vital as it shines light on injustices, empowers minorities, breaks cycles of poverty, and assists individuals to succeed. However, the same tools empowering free speech can also be used for hate speech, planning acts of violence, destabilizing governments and societies, or even reinforcing socio-economic divides by favoring particular groups of individuals. The authors of the tools play a crucial role in deciding who these tools empower.

4.1 Impact of Design

For a tool to overcome a limit, it has to be used. As discussed in previous sections, even existing tools are not suitable for users who may lack the knowledge, experience, or income to use them. From our research, we observed that proficiency in English and technical literacy tend to favor those who are wealthier and live in large cities.

4.1.1 Language. When developing tools that enable Internet freedoms, the choice of languages to support has consequences. Every country in the world has users that speak major languages such as Mandarin, Spanish, and English, but many countries only have partial adoption [7]. Picking a language can alienate portions of the population for which the language is non-dominant. Language expectation may bias toward a particular socio-economic class [25]. People who engage in international business or higher education may be more likely to speak a major language. Even without creating new tools, translating existing tools to new languages can reduce the adaptation barrier for currently restricted minorities. Selectively distributing tools can amplify a subset of voices over others. Neglecting to translate a tool that provides freedoms for some, effectively limits freedoms of others.

4.1.2 Technical Literacy. Alongside language is the expectation of technical literacy. Tools that are hard to use and setup, or those with poorly explained limitations can alienate and even endanger groups. While information technology professionals may have the technical understanding to use or learn to use existing tools, the same is not true for users from all domains. From our experiences, journalists and civil rights advocates, especially those who have little funding for I.T. support, face difficulties setting up and using existing tools. Worse still, groups with poor backgrounds in cybersecurity may not understand the threat model that a particular tool is designed to counter, leading to a false feeling of security.

Even if a tool is available in a language the user understands, without comprehension of the full security context and without an intuitive design, the user may not be able to use it effectively. Like language, the design and usability of a tool can segregate populations. Ensuring that an application is clear to a novice extends the application's reach and ability to empower. Conversely, ignoring the design and ease of use of a tool can disproportionately favor those with the education and experience to use it, or those with the economic advantage to hire someone who can.

4.1.3 Device and Platform. Choosing a platform or operating system for a security tool limits the user demographic that a tool empowers. Requiring a Twitter account, for example, may alienate users who would otherwise be interested in the security tool, but who lack interest in starting a Twitter account. When applied on a global scale, alienated demographics could comprise the majority of entire countries. In our research we found a high usage of Twitter in Turkey, but when talking to activists in Mongolia and Zambia, we found nearly all favored Facebook.

Likewise, the choice of operating system can segregate populations of users. This is especially true for mobile applications that have experienced rapid growth and change. Selecting iOS over Android can alter the types of groups who are able to use a mobile application. The version of operating system can further subdivide groups. In Istanbul, we found newer Android phones running the latest operating system were quite common; however, when working in Zambia we found phones running operating systems as old as Android 1.6. Android applications not targeting such old versions would not run. Adding backwards compatibility to applications can increase development time, complexity, and complicate usability testing. On the other hand, restricting operating system type or version limits the tools to those who can afford newer devices.

It is important to note that while mobile-broadband usage in the developing world is limited, it is the primary method for Internet access. As of 2016, 41% of the population in the developing world had mobile-broadband subscriptions compared to 8% with fixed-broadband subscriptions [54]. Throughout much of the developing world, mobile devices are the primary means of accessing the Internet. Technologies that are not accessible via mobile, segregate users for whom this is the only method of access.

Ownership of a suitable device, like a smart phone, is still a limit. While most of the people we talked to in the capital cities owned smart phones, in rural communities this is not the case. In Zambia, for example, a 2015 study found only 51% of the population actively used mobile devices and only 13.5% of those devices were smartphones [38]. While it is impossible to tailor a software tool for communities with no hardware, these groups should still factor in ethical considerations. As societies become reliant on technology for protecting freedoms, those without the proper hardware may fall further behind.

4.1.4 Connectivity and Power. Lacking access to power and Internet connectivity can be a limit to speech. Between no access and reliable access is a gray zone in which much of the world resides [49]. In tool design, connectivity and power are commonly treated as binary, either present or absent. In reality, Internet access can be unreliable, expensive, or incredibly slow. Power is similarly unreliable. In rural areas, blackouts may be frequent and brown outs, when voltage drops bellow operating norms, may be common. Applications built on the assumption of low latency, high bandwidth, and continuous power may be unusable for these communities. Like other design choices, the network and power requirements of tools selects the demographic that they empower. Developers can overcome some of these restrictions through techniques such as caching data, bundling server requests, and minimizing local computation. Optimization of tools for resource poor environments takes development time and adds complexity. Failure to design and test for situations of limited resources favors those in richer conditions.

4.2 Security

While technologies can overcome limits on speech and access, they can present a danger to their users. Even if empowering users is not the priority to tool developers, user safety should be. If a tool is poorly explained, users may not realize that they are not protected against specific threats. For some, speech can put them in danger, leading to incarceration, economic hardship, violence, or even death. While tools typically try to grow a user base, advertising to users without adequately preparing them can do more harm than good. Even experienced users may grow complacent from a feeling of security and make mistakes that expose them to threats.

Like other tools, software focusing on Internet freedoms occasionally have bugs or oversights that create vulnerabilities. For low-risk individuals, a vulnerability may pose little threat. For high-risk individuals, who are under scrutiny by adversaries with high levels of network control, a single vulnerability can suffice to identify users or provide evidence for incarceration. Tool designers are responsible for the integrity of their tools. Like other concerns, keeping tools up-to-date and informing users of potential problems may be harder in particular communities. Users lacking affordable Internet access may not keep their applications updated. Similarly, users who side-load applications due to blocking of larger repositories may never receive application updates. These users might be exposed to vulnerabilities for which their software was never patched. Alternate delivery systems, as well as resource-aware update sizes can help protect these users.

4.3 Ethical Concerns

4.3.1 Misuse for Harm. Some worry that agents seeking to do harm will misuse tools intended for Internet freedoms. Encryption tools enabling human rights activists to talk without fear can be used by terrorist groups to coordinate attacks. Tools allowing circumvention of censorship for tasks such as gaining knowledge about safe-sex practices can be used to access bomb-making instructions. Further, free speech entails the possibility of hate speech. Anonymity tools can protect the identity of activists, but also of cyber-bullies. When working on these technologies, there is an ethical concern that in the course of empowering communities, they would cause collateral harm.

One possible justification goes as follows. While marginalized groups are silenced, those seeking to cause harm, like terrorists, have the funding and expertise to build comparable tools for themselves or enlist others to do it for them. Even if researchers did not build these particular tools, bad actors would still have the capabilities to do harm. If developers stopped building encrypted communication applications that keep individuals safe from oppression, terrorists could still build the same type of application for themselves.

Anyone suspicious of this justification might instead suggest that concerns of freedom, especially of vulnerable populations, typically trumps concerns of safety. Fear of wrongdoers intentionally corrupting tools for malice should not come in the way of protecting the oppressed or empowering the marginalized. Designing tools that are resilient to misuse is not always possible. Sometimes it is possible, however, to mitigate the potential harm.

4.3.2 Suppressing Speech of Others. Even when tools make it to intended audiences they can still be abused. When interviewing marginalized groups about the types of capabilities they would like to have on-line, some desired tools to silence or attack those that speak negatively against them. If the point of access and speech is an exchange of ideas, not all communities, even those silenced themselves, are initially interested in allowing others to talk. Developers can be mindful of this ethical concern, and focus on technologies that empower speech without suppressing the speech of others.

4.3.3 Interfering with Other Nations. Another ethical concern is the right to interfere in other societies and cultures. Often technologies are developed in first-world nations, but the technologies can be used anywhere. This may explicitly or implicitly bias development and usage towards groups similar to the developers. To empower speech, developers may target marginalized groups on foreign soil and not have personal stake in the ramification. Sovereign governments, sometimes put there by democratic vote, may actively impose the limits that technology aims to overcome. The counter argument is that free-speech and Internet access are human rights. Most democratic governments, as well as the United Nations [10, 16], recognize this. Just as we have duties to recognize and prevent other human rights violations, we have an ethical responsibility to support freedom of speech and access across national lines. The marginalized may not have the access or resources to help themselves.

5 CONCLUSIONS

The world is becoming increasingly authoritarian. The precious resource of Internet freedoms is actively and intentionally limited by governments, corporations and communities. If, as a society, we place value in the rights of individuals to seek information and share their concerns and experiences, then overcoming those limits is a growing challenge. While technology can help tear down these barriers, it sometimes leads to externalities in the form of undesirable consequences.

When developing technologies supporting Internet freedoms, the design of applications has profound ethical implications. There is a balance between satisfying a human right and exposing others to danger. Empowering the speech of one group could mean suppressing speech of another. Tool developers can mitigate these risks while broadening access.

Developers often build from personal experiences, targeting users of their country and background, but the impact of their decisions often reaches far beyond the confines of their society. Successful tools are not confined to a single country or demographic. The Internet, as well as the ecosystem of tools that use it, is global and pervasive. Factoring in the experiences of users across the world, such as language, technical knowledge, and resource availability, can have profound impacts on peoples lives.

While a large library of security tools exists, there are underserved areas. Problems, such as maintaining reputation while preserving anonymity, the crowding out of voices using bots and trolls, and communicating despite network interruption continue to be areas of growth. Even existing technologies are often limited in their use due to the technical knowledge gap and language requirements associated with using them. As the Internet continues to grow and mature and new applications as well as censorship tools become available, so too will the need for new technologies to counter them.

REFERENCES

[1] Confide. https://getconfide.com/. (Accessed Feb. 2017).
[2] Government requests report. https://govtrequests.facebook.com/. (Accessed Feb. 2017).
[3] HTTPS everywhere. https://www.eff.org/https-everywhere. (Accessed Feb. 2017).
[4] Orbot: Tor for Android. https://guardianproject.info/apps/orbot/. (Accessed Feb. 2017).
[5] Privacy Badger. https://www.eff.org/privacybadger. (Accessed Feb. 2017).
[6] Signal. https://itunes.apple.com/us/app/signal-private-messenger/id874139669. (Accessed Feb. 2017).
[7] Summary by language size. https://www.ethnologue.com/statistics/size. (Accessed Feb. 2017).
[8] Tor browser. https://www.torproject.org/projects/torbrowser.html.en. (Accessed Feb. 2017).
[9] What names are allowed on Facebook? https://www.facebook.com/help/112146705538576. (Accessed Feb. 2017).
[10] Universal declaration of human rights. http://www.un.org/en/universal-declaration-human-rights/, Dec 1948.
[11] List of banned words on its websites and comments. http://www.shuum.mn/news/newsid/14091/catid/17n, Mar 2013.
[12] Ethiopia: Government blocking of websites during protests widespread, systematic and illegal. https://www.amnesty.org/en/latest/news/2016/12/ethiopia-government-blocking-of-websites-during-protests-widespread-systematic-and-illegal/, Dec 2016.
[13] Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey. https://turkeyblocks.org/2016/11/04/social-media-shutdown-turkey/, Nov 2016.
[14] Mongolia: Freedom of the press 2016. https://freedomhouse.org/report/freedom-press/2016/mongolia, 2016.
[15] New internet shutdown in Turkey's Southeast: 8% of country now offline amidst Diyarbakir unrest. https://turkeyblocks.org/2016/10/27/new-internet-shutdown-turkey-southeast-offline-diyarbakir-unrest/, Oct 2016.
[16] The promotion, protection and enjoyment of human rights on the internet. https://www.article19.org/data/files/Internet_Statement_Adopted.pdf, Jun 2016.
[17] Tor blocked in Turkey as government cracks down on VPN use. https://turkeyblocks.org/2016/12/18/tor-blocked-in-turkey-vpn-ban/, Dec 2016.
[18] Turkey: Provisional release of human rights lawyer Mr. Levent Piskin. https://www.fidh.org/en/issues/human-rights-defenders/turkey-provisional-release-of-human-rights-lawyer-mr-levent-piskin, Nov 2016.
[19] Whoever criticizes Erdogan finds themselves in court; Here are the court cases! https://lgbtinewsturkey.com/2015/05/08/whoever-criticizes-erdogan-finds-themselves-in-court-here-are-the-court-cases/, May 2016.
[20] Wina justifies beating of Komboni radio owner. https://www.tumfweko.com/2016/10/09/wina-justifies-beating-of-komboni-radio-owner/, Oct 2016.
[21] Free basics by Facebook. https://info.internet.org/en/story/free-basics-from-internet-org/, 2017.
[22] M. Akyol. Another Turkish witch hunt begins. https://www.usnews.com/news/articles/2014/12/16/another-turkish-witch-hunt-begins, Dec 2014.
[23] C. Arthur. Egypt blocks social media websites in attempted clampdown on unrest. https://www.theguardian.com/world/2011/jan/26/egypt-blocks-social-media-websites, Jan 2016.
[24] P. Barberá, J. T. Jost, J. Nagler, J. A. Tucker, and R. Bonneau. Tweeting from left to right: Is online political communication more than an echo chamber? *Psychological science*, 26(10):1531–1542, 2015.
[25] D. Casale and D. Posel. English language proficiency and earnings in a developing country: The case of South Africa. *The Journal of Socio-Economics*, 40(4):385–393, 2011.
[26] A. Chen. The Agency. https://www.nytimes.com/2015/06/07/magazine/the-agency.html, Jun 2015.
[27] M. Chulov. Syria shuts off internet access across the country. https://www.theguardian.com/world/2012/nov/29/syria-blocks-internet, Nov 2012.
[28] H. R. Clinton. Remarks on internet freedom. *The Newseum*, 21, 2010.
[29] J. Cowie, A. Popescu, and T. Underwood. Impact of hurricane Katrina on internet infrastructure. *Report, Renesys*, 2005.
[30] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl. IMSI-catch Me if You Can: IMSI-catcher-catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference*, ACSAC '14, pages 246–255, New York, NY, USA, 2014. ACM.
[31] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.
[32] E. Galperin. Changes to Facebook's "real names" policy still don't fix the problem. https://www.eff.org/deeplinks/2015/12/changes-facebooks-real-names-policy-still-dont-fix-problem, Dec 2015.
[33] D. Goldman. Donald Trump wants to 'close up' the internet. http://money.cnn.com/2015/12/08/technology/donald-trump-internet/, Dec 2015.
[34] J. Greenberg. For Netflix, discontent over blocked vpns is boiling. https://www.wired.com/2016/03/netflix-discontent-blocked-vpns-boiling/, Mar 2016.
[35] M. R. Hebl, J. B. Foster, L. M. Mannix, and J. F. Dovidio. Formal and interpersonal discrimination: A field study of bias toward homosexual applicants. *Personality and social psychology bulletin*, 28(6):815–825, 2002.
[36] A. Hess. On Twitter, a battle among political bots. https://www.nytimes.com/2016/12/14/arts/on-twitter-a-battle-among-political-bots.html, Dec 2016.
[37] S. Hinduja. Doxing and cyberbullying. http://cyberbullying.org/doxing-and-cyberbullying, September 2015.
[38] Z. Information and C. T. Authority. ICT survey report - households and individuals. https://www.zicta.zm/Views/Publications/2015ICTSURVEYREPORT.pdf, 2015.
[39] C. Kangfeb. Trump's F.C.C. pick quickly targets net neutrality rules. https://www.nytimes.com/2017/02/05/technology/trumps-fcc-quickly-targets-net-neutrality-rules.html, Feb 2017.
[40] G. Kasparov and T. Halvorssen. Why the rise of authoritarianism is a global catastrophe. https://www.washingtonpost.com/news/democracy-post/wp/2017/02/13/why-the-rise-of-authoritarianism-is-a-global-catastrophe, Feb 2017.
[41] S. Kelly, M. Earp, L. Reed, A. Shahbaz, and M. Truong. Privatizing censorship, eroding privacy. https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf, Oct 2015.
[42] T. B. Lee. Here's how Iran censors the Internet. https://www.washingtonpost.com/news/the-switch/wp/2013/08/15/heres-how-iran-censors-the-internet, Aug 2013.
[43] K. Lim and E. Danubrata. Singapore seen getting tough on dissent as cartoonist charged. http://www.reuters.com/article/us-singapore-dissent-idUSBRE96P0AF20130726, Jul 2013.
[44] M. Lowen. Is Gollum good or evil? Jail term in Turkey hinges on answer. http://www.bbc.com/news/world-europe-32302697, Apr 2015.
[45] C. Miller. Bots will set the political agenda in 2017. http://www.wired.co.uk/article/politics-governments-bots-twitter, Jan 2017.
[46] S. J. Murdoch and G. Danezis. Low-cost traffic analysis of tor. In *Security and Privacy, 2005 IEEE Symposium on*, pages 183–195. IEEE, 2005.
[47] P. Norris. It's not just trump. authoritarian populism is rising across the West. here's why. https://www.washingtonpost.com/news/monkey-cage/wp/2016/

03/11/its-not-just-trump-authoritarian-populism-is-rising-across-the-west-heres-why, Mar 2016.

[48] L. Parks and R. Mukherjee. From platform jumping to self-censorship: internet freedom, social media, and circumvention practices in Zambia. *Communication and Critical/Cultural Studies*, pages 1–17, 2017.

[49] V. Pejovic, D. L. Johnson, M. Zheleva, E. Belding, L. Parks, and G. van Stam. The bandwidth divide: Obstacles to efficient broadband adoption in rural Sub-Saharan Africa. *International Journal of Communication*, 6:25, 2012.

[50] A. Peterson. Turkey strengthens Twitter ban, institutes IP level block. https://www.washingtonpost.com/news/the-switch/wp/2014/03/22/turkey-strengthens-twitter-ban-institutes-ip-level-block, Mar 2014.

[51] M. Pizzi. Isolated in camp, syrians desperate to get online. http://america.aljazeera.com/articles/2015/7/16/internet-access-zaatari-camp.html, July 2015.

[52] M. Richtel. Egypt cuts off most internet and cellphone service. http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html, Jan 2011.

[53] K. Rogers. The problem with insulting Turkey's President Erdogan. https://www.nytimes.com/2015/12/05/world/europe/is-gollum-good-or-evil-jail-term-in-turkey-hinges-on-answer.html, Dec 2016.

[54] B. Sanou. Ict facts and figures 2016. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf, 2016.

[55] V. Shevchenko. Ukrainians petition Facebook against 'Russian trolls'. http://www.bbc.com/news/world-europe-32720965, May 2015.

[56] P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett. Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 49(4):376–385, 2008.

[57] A. Taylor. This single tweet got a Turkish journalist detained. https://www.washingtonpost.com/news/worldviews/wp/2014/12/30/this-single-tweet-got-a-turkish-journalist-detained, Dec 2014.

[58] S. Timur and T. Arango. Turkey seizes newspaper, Zaman, as press crackdown continues. https://www.nytimes.com/2016/03/05/world/middleeast/recep-tayyip-erdogan-government-seizes-zaman-newspaper.html, Mar 2016.

[59] S. Walker. Salutin' Putin: inside a Russian troll house. https://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house, Apr 2015.

[60] R. Williams. The rise of authoritarianism. https://www.psychologytoday.com/blog/wired-success/201603/the-rise-authoritarianism, Mar 2016.

[61] J. Zittrain and B. Edelman. Internet filtering in China. *IEEE Internet Computing*, 7(2):70–77, Mar 2003.