NEW AMERICA

December 2018

Perspectives and Policies on the Digital Safety of Vulnerable Communities

Dillon Roseen & Spandana Singh

Last edited on December 06, 2018 at 12:12 p.m. EST

Acknowledgments

We'd like to thank all of the digital security and safety experts, activists, and advocacy groups that engaged with us during the production of this report. We'd particularly like to thank reproductive justice activist Renee Bracey Sherman, Neil Melhuish of Netsafe, the Association of Progressive Communications, and Lisa Gutermuth at the Ranking Digital Rights team at New America for their support in refining the recommendations in this report. While these individuals supported the production of this report, they primarily served as peer reviewers. The opinions in this report are not necessarily theirs. We would also like to thank the Millennial Public Policy Fellowship program at New America for its support of our work in this area.

About the Author(s)

Dillon Roseen was a Millennial Public Policy Fellow in New America’s Cybersecurity Initiative. Roseen, from Peachtree City, Ga., was a Fulbright Scholar in Amsterdam where he conducted research on the intersection of law, politics, and international security.

Spandana Singh is a policy program associate in New America's Open Technology Institute.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation’s highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Millennials Initiative

The Millennials Initiative at New America will examine the challenges facing this generation of young adults (born between 1980 and 2000) as they aspire to assemble the basic building blocks of success—getting an education, finding a job, managing finances, buying a home, raising a family, and engaging socially and politically in a community.

Contents

Introduction

The proliferation and adoption of technology has had a profound impact on the digital security of communities across the globe. But, not all of these effects have been positive.

In 2017, over one half of American businesses reported experiencing a cyberattack in the preceding year.[1] A Pew Research Center study also found that a majority of Americans (64 percent) have personally experienced a major data breach, through avenues such as credit card fraud, compromised Social Security numbers, and hacked email and social media accounts.[2]

Addressing the growing repertoire of threats to digital security, which can be defined as the safety of an individual's digital identity, online data, and well-being related to hardware and software, is not an easy task. This is especially true given that the current definition of security against digital threats is generally limited to topics of cyber warfare, hacking information systems, financial and economic crimes, and internet governance. As the number of digital threats and attacks against individuals and communities increase, reciprocal response frameworks and tools need to be established and expanded. In order for this to be successful, the definition and scope of digital security efforts need to be broadened to include threats and protections related to digital safety, such as online abuse, at the individual and community level.

Digital safety is increasingly becoming a concern for online users. A 2017 Pew Research Center study found that 41 percent of adult internet users have personally experienced harassment online.[3] These negative online experiences particularly impact minority and marginalized communities. Factors such as race, ethnicity, sexual orientation, age, and religious preferences routinely play a role in these cases. For example, three out of four women around the world and 67 percent of young adults in the United States have been subject to some form of online abuse or harassment.[4] In addition, one in four African Americans and one in 10 Hispanic Americans were targeted with harassment on account of their race or ethnicity, compared to only 3 percent of white Americans.[5]

In this report, we focus on threats to digital safety, such as instances of online abuse and harassment that impact vulnerable and marginalized communities. Typically, disruptions and threats to an individual's digital security, especially their digital safety, have profound impacts on that individual's willingness to utilize technology. In addition, when thinking about the collective impact that silencing individual voices has in a democratic society, the effects become particularly worrisome. In a world that is no longer distinctly separated into the physical and virtual spheres, it is entirely possible that the targeting and threatening of vulnerable and minority communities online can mirror the silencing and marginalization of these groups in the physical world. In effect, several core pillars of democratic society—speech, expression, equity, privacy, and freedom from harm—are threatened by such attacks.

The definition and scope of digital security efforts need to be broadened to include threats and protections related to digital safety, such as online abuse.

In the United States, debates on how to effectively protect vulnerable communities online from abuse and harassment often creates tension with the need to safeguard free speech rights provided by the First Amendment, especially since hateful speech is protected speech. On a global level, these debates create tensions with the need to safeguard free expression rights provided by frameworks such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. This report outlines approaches for how individuals and communities, the private sector and the public sector can augment their digital safety while avoiding impinging on the civil right to free speech or the human right to free expression.

Scope of Report

This report focuses on three vulnerable and/or minority groups: youth, women, and ethnic and racial minorities, with the aim of comparing and contrasting the digital safety risks and threats these communities face. While other communities, particularly religious minorities, the elderly, and the LGBTQ community also face significant threats to their digital safety, the scope of this report is narrowed for several reasons. First, based on a preliminary research sprint of each of the aforementioned communities, more longitudinal and geographically relevant information was available on the three selected groups.[6] Second, it was more effective to build on existing research than construct a new research agenda in a more nascent area of this field, especially considering limited time and resources. However, given the intersectional nature of many digital safety threats, some case studies engage multiple dimensions of identity and the challenges facing members of intersecting communities. In addition, although digital safety is a broad concept that engages the three selected communities in numerous ways, the scope of this report has been narrowed to focus on digital safety threats related to online abuse and harassment. This category of digital safety threats was selected based on the availability of research and the experiences of those interviewed for this report.

Further, this report focuses primarily on the domestic environment in the United States, across federal, state, and local levels. Some international examples are included as a resource for further research. Similarly, findings from the preliminary research sprint that relate to other vulnerable communities have been included to highlight some of the challenges that fall outside of the formal scope of this report.

The research in this report was conducted over a period of eight months (from November 2017 to June 2018) using a range of methods, including reviewing existing cybersecurity, digital security, and digital safety literature, conducting interviews with 30 cybersecurity, digital security, and digital safety experts representing some of the leading organizations in the field—including consultations with internal experts at New America—and attending over a dozen workshops, conference events, and trainings on digital security, digital safety, and human rights in the digital age. The aim of this research was to identify the organizations, programs, best practices, platforms, and policies that are being effectively deployed to support vulnerable communities in the digital space, while also identifying gaps in these existing support structures. In the future, these findings can be used to identify ways to more effectively deconstruct silos between advocacy groups, and increase meaningful collaboration across communities, which can aid in filling unmet needs.

The Digital Safety Landscape

As new technologies are developed and adopted, in addition to the positive benefits they may provide, they also augment the power of existing forms of abuse and exploitation. This augmentation results in the emergence and enhancement of a range of digital safety threats, including an expansion of potential consequences. The digital safety threats and subsequent consequences associated with cases of online abuse can be seen in Appendix 1 and 2, respectively. Digital safety threats, particularly the category of threats this report focuses on, disproportionately impact vulnerable communities and are often motivated by an animus towards an individual's race, class, age, nationality, ethnicity, religion, and sexual orientation. In addition, digital safety threats and attacks often vary based on geographical and community contexts. For example, the devices and platforms used to perpetrate attacks in a small, rural environment are often different than those used in a large, urban city.

This section provides an overview of the digital safety landscape of the three selected communities. Each discussion analyzes the types of threats each community faces and outlines some of the programs that exist to support them. This section also includes case studies which are based on real events that we learned about during the course of researching and producing this report. Names and identifying details have been changed to protect the identity of our interviewees.

Youth

Case Study: Azariah

Names and identifying details have been changed to protect the identity of our interviewees.

Azariah is 13 years old and attends a small, rural middle school. After many serious discussions with their doctors, Azariah recently took one of their first steps in the long process of transitioning to their preferred gender identity. Despite strong support from their family, Azariah was understandably nervous about how other classmates and people in the community might react to the transition. Unfortunately, their worst fears were realized just a few months after beginning puberty blockers.

On their way to school, Azariah received a text with a link to a social media group. The members of the group were other students in Azariah's class, including supposed friends, who were making fun of Azariah for transitioning. There were transphobic slurs, pictures of Azariah photoshopped on other people's bodies, and comments that vaguely alluded to hurting Azariah. The group had been active for weeks. Mortified, Azariah immediately went home and shared everything with their parents.

Around that time, Azariah's phone began buzzing incessantly. A flood of hateful text messages from other students in Azariah's class popped up one after another, causing Azariah to have a panic attack. Remembering the advice of Azariah's doctors and therapists, Azariah's parents immediately took Azariah to the hospital to make sure the episode wasn't a side effect of the new medication. In fact, the medication was not the problem, concluded the doctor. It was strictly a result of the trauma that resulted from such an intense and coordinated bullying effort. Later that day, Azariah was released to go home but under the doctor's instructions not to send Azariah back to school until the parents were sure that it would be a safe environment.

The [panic attack] was strictly a result of the trauma that resulted from such an intense and coordinated bullying effort.

At home the next few days, Azariah continued to be hounded by texts, posts, and even phone calls from tormentors. Even though Azariah's parents shut off the internet and banned cell phones, the damage was done. Unbeknownst to Azariah's parents, Azariah began harming themselves and considering suicide, an all-too-common response in teens who have been bullied in this way. The problem is especially pronounced for LGBTQ youth like Azariah.

Through all of this, Azariah's parents continually sought recourse through the school system and local law enforcement. This required them to document all of the instances of hateful speech hurled at their child, an emotionally traumatizing experience on its own. Exacerbating this painful experience, they received little support from school and law enforcement officials. After first calling the school, they were redirected to the police who said that, since most of the students were underage, there was little action they could take. As Azariah's parents continued searching for help, they discovered the school's bullying policy. The terms clearly covered the situation, but Azariah's parents still had to fight for the school to recognize what was happening by sending a lengthy letter with dozens of pages of evidence to support their claim. Only then did the school take steps to create the safe environment guaranteed under the bullying policy. At that point, still not fully convinced that Azariah would be safe back at school, Azariah's father decided to switch to the night shift at work so that he could stay home and homeschool Azariah during the day.

The Digital Safety Landscape for Youth

Nearly a third of youth between the ages of 11 and 19 have been victims of online abuse.[7] New technologies augment existing forms of abuse and exploitation, leading to increased levels of sexual abuse and harassment, increased profitability for criminal enterprises, reduced risk of detection, increased harm to victims, and provision of social affirmation for offenders (See Appendix 1).[8] Moreover, new forms of abuse and exploitation are made possible through new technologies, including made-to-order child sexual abuse material and broadcasting of live sex abuse.[9] For LGBTQ youth, digital safety threats, particularly those related to online abuse and harassment, are even more pronounced. Over half of LGBTQ youth have experienced online harassment (55.2 percent) compared to the 10-33 percent of youth overall who reported similar abuse.[10] In addition, LGBTQ youth were four times more likely to report sexual harassment online (32 percent) than their non-LGBTQ peers (8 percent), with rural LGBTQ youth reporting substantially higher rates of online victimization than suburban or urban peers.[11]

Below are some examples of groups working to combat instances of online abuse and harassment against youth and provide digital security training, education, and support to youth in the United States and around the world. These organizations were selected based on their accessibility, public engagement with digital security, efforts to counter online abuse against youth, and recognition within communities working to support youth. However, this is in no way an exhaustive list.

- **Cyberbullying Research Center**: Contributes useful research on cyberbullying policy and legislative efforts.

- **Netsafe**: A non-profit organization based in New Zealand focused on internet safety and security through education, response, and advisory roles. Netsafe holds a statutory role under New Zealand's Harmful Digital Communications Act 2015, and receives funding from the New Zealand Ministries of Justice and Education.

- **NetSmartz**: Sponsored by the U.S. Justice Department, an educational program offering adaptable, free, downloadable training and education resources for children and parents on digital risks

- **Stop Bullying.gov**: A U.S. Department of Health and Human Services initiative that provides information on cyberbullying prevention efforts, reporting mechanisms, and a repository of legal/statutory resources

- **The Trevor Project:** A U.S.-based organization focused on provision of crisis intervention and suicide prevention services to LGBTQ youth under the age of 25.

Nearly a third of youth between the ages of 11 and 19 have been victims of online abuse.

Women

Case Study: Rabia

Names and identifying details have been changed to protect the identity of our interviewees.

Rabia is a young, aspiring journalist. She recently landed the editorial internship of her dreams and was over the moon about publishing her first independent article online. She wrote about a topic very near and dear to her heart—gender equality in the workplace. Shortly after the article was published and shared on social media, Rabia's phone began blowing up. She proceeded to check her notifications and was shocked to find that she had become the target of a coordinated group of online trolls who berated her for her "silly feminist perspectives" and singled her out for her Middle Eastern heritage and her religion—Islam. By the end of the day, Rabia's social media feeds and inboxes were overflowing with hateful content, including death threats. But, the abuse did not stop there.

Soon after, Rabia's personal email account was hacked. She was locked out. If that weren't enough, a troll set up a website dedicated to sharing violent and graphic photoshopped images of her. Rabia spent the entire day trying to mitigate these online attacks, and as a result she didn't get any work done, much to the dismay of her supervisor. The next day, the trolls began distributing Rabia's personal information—her home address, her parent's home address, her cell phone number, and where she went to school—online. By the end of the day, the death threats against Rabia had expanded to include threats against her friends and family. At this point, she began to genuinely fear for the safety of herself and her loved ones.

By the end of the day, the death threats against Rabia had expanded to include threats against her friends and family.

After work, she went to the local police station to report the incident. The police officer who received her gave her a perplexed look when she explained she was concerned about her safety because a group of people online had sent her abusive messages. He advised that she ignore the trolls, as they were all grown men living in their mothers' basements, and told her to forget about it. Rabia pushed back, but the officer pressed her on why she had encouraged the trolls by responding to them, making her feel as if she had brought this on herself. Dejected, Rabia returned home. The hateful and abusive online targeting did not stop, however, and before going to bed, Rabia decided to completely shut down her social media accounts. When she returned to work the next day, she shied away from taking on any potentially controversial writing assignments as she did not want to further exacerbate the situation.

The Digital Safety Landscape for Women

Rabia's experience with online abuse is jarring. Unfortunately, she is not alone. According to a report by the United Nations Broadband Commission, three-fourths of women around the world have been exposed to some form of online abuse or harassment.[13] In addition, despite advances in gender equality around the world, women are still 50 percent less likely to be internet users, regardless of the geographic region and income group they belong to.[14] For many women, education and cost remain barriers to accessing and effectively navigating online spaces.[15]

The extensive list of digital safety threats women can face (see Appendix 1) often spark fear and mistrust among women and results in them leaving the digital sphere altogether. In addition, this hostile environment also poses significant threats to the freedom of speech and expression of female users. According to a World Wide Web Foundation report, women are 52 percent less likely than men to express controversial views online, fearing consequences.[16] Rabia's story demonstrates this chilling effect.

Below are some examples of groups working to combat instances of online abuse and harassment against women and provide digital security training, education, and support to women in the United States and around the world. These organizations were selected based on their accessibility, public engagement with digital security, efforts to counter online abuse against women, and recognition within communities working to support women. However, this is in no way an exhaustive list.

- **Association of Progressive Communications (APC)**: APC is an international organization that operates the Take Back the Tech program, an initiative that combats violence against women (VAW) by providing female users with workshops on online safety, media monitoring on rape reporting, online and offline solidarity and support, among other things.

- **Crash Override Network**: A grassroots crisis helpline, advocacy group and resource center that offers free confidential support and advice on self-protection to those who are experiencing abuse online. The organization receives approximately 6,000 users every month and although it does not have an explicit focus on working with women, it is commonly used by female users.

- **National Network to End Domestic Violence (NNEDV)**: NNEDV operates a Safety Net project which engages communities, agencies and technology companies on the risks to safety, privacy and accessibility that technology poses to victims. Their work includes trainings for victims and victim advocates as well as for law enforcement.

- Public impact litigation firms such as **C.A. Goldberg, PLLC**, which fights for victims of sexual assault, blackmail and stalking, online and offline.

- **TrollBusters**: A "rescue service for women journalists, bloggers and publishers" that sends supportive images and messaging to a victim's social media feed, thus creating counter-narratives and providing a protective layer. TrollBusters also documents and monitors attacks for victims so they do not have to watch the abuse unfold.

Racial and Ethnic Minorities

Case Study: Chris

Names and identifying details have been changed to protect the identity of our interviewees.

Chris is an activist who works primarily with communities of color. As the midterm elections approached, Chris took to the internet to encourage his network to vote and share his thoughts on pressing issues such as immigration, healthcare, and gun control, often quoting pivotal Civil Rights activists and political leaders. His posts, however, attracted the attention of a far-right hate group who began posting disparaging and racist comments on Chris' profiles and threatening him based on his social and political opinions. In addition, the hate group responded to Chris' posts by sharing false information regarding leaders such as Martin Luther King Jr. and Barack Obama, and linking to "cloaked sites" that were a repository of falsified and manipulated information. At first, Chris chose to ignore them. However, over the course of a couple of days, the hate group bombarded him with so much hateful and harmful content he couldn't use his social media profiles without viewing their content. In addition, many members of Chris' network had read the content shared by the hate group, and much to Chris' dismay were being influenced by their false messaging. At this point, Chris decided he had had enough and engaged the trolls to try and get them to step down. However, in response, the hate group copied Chris' information from his public profiles and set up alternative ones, effectively seeking to defame and impersonate him within his own community as well as externally.

The hate group soon after found out that Chris was organizing a rally supporting the rights of immigrants in the United States. On the day of the rally, Chris was shocked to find that the rally was stormed by members of a local SWAT team as a result of a false tip off by the trolls that there was imminent danger at the event.

The Digital Safety Landscape for Racial and Ethnic Minorities

Early thinking about race and ethnicity online suggested that the internet could reduce or eliminate racial and ethnic disparities that occurred offline.[17] Since then, however, it has become clear that the internet and digital technologies more broadly have introduced new challenges and exacerbated old ones, both online and offline. Racial and ethnic minorities regularly face cases of online abuse such as impersonation and targeted attacks.

The rally was stormed by members of a local SWAT team as a result of a false tip off by the trolls that there was imminent danger at the event.

For example, Southern Poverty Law Center, an organization that monitors hate groups, found a sharp spike in the number of anti-Muslim photos, memes, and posts on social media following the 2016 U.S. election.[18] In a similar study, the

Anti-Defamation League found that there were 2.6 million tweets containing anti-Semitic speech between August 2015 and July 2016.[19] These types of hateful content can often spark, or, as demonstrated in the example above, actively promote cases of online abuse and harassment. According to a Pew Research Center Study, one in four African Americans have faced discrimination online as a result of their race or ethnicity and 54 percent of African American internet users have witnessed severe forms of online abuse against others, including physical threats, stalking, sexual harassment, or sustained harassment. Both experiencing and witnessing such online abuse takes its toll. Those experiencing such abuse are often more likely to retreat from online spaces, self-censor or remain silent altogether. Similarly, 43 percent of African American internet users and 44 percent of Hispanics censored themselves on online platforms after witnessing abuse out of fear that something similar might happen to them.[20]

These forms of online abuse and discrimination based on a person's racial and ethnic background also significantly impact youth of color. Studies have found that as minority youth become older and engage with the internet at a greater rate, they also experience higher levels of discrimination. Over 44 percent of minority youth in these studies have indicated experiencing online discrimination on a social networking site. These experiences are damaging to individuals of all ages. However, for young people, experiencing these types of vitriolic attacks are particularly damaging to mental health outcomes.[21]

Various policies, programs, and platforms exist that aim to better the digital safety landscape affecting racial and ethnic minorities. Given the sometimes tenuous relationship between communities of color and local law enforcement or government officials, grassroots activists of color are often the ones leading the development of new programs and platforms for bettering the digital safety environment while policy lags behind.

Below are some examples of groups working to combat instances of online abuse and harassment against racial and ethnic minorities and provide digital security training, education, and support to these communities in the United States and around the world. These organizations were selected based on their accessibility, public engagement with digital security, efforts to counter online abuse against racial and ethnic minorities, and recognition within communities working to support these communities. However, this is in no way an exhaustive list.

- **Access Now**: An organization focused on protecting human rights in the digital age through "direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon."

- **Anti-Defamation League**: An organization focused on halting the defamation of the Jewish people and securing justice and fair treatment for other communities including racial groups, women, immigrants and refugees and other religious groups.

- **Cryptoparty**: A decentralized, grassroots movement focused on sharing practical digital security advice to individuals regardless of skill level or background.
- **Defend Our Movement**: A web based clearinghouse of the most up-to-date and useful information about protecting your devices and data, including culturally relevant digital safety tips, tools, and support from movement security allies.
- **Equality Labs**: A South Asian organization focused on reducing racism and oppression, including through digital security trainings, community-based research, and rapid response support.
- **Security in a Box**: Provides tools and tactical guides for individuals and communities who face significant digital security threats.

Other Research

During a preliminary research sprint, it was clear that other communities also face unique vulnerabilities and threats online. The LGBTQ community, for example, is extremely likely to face abuse and harassment online, including hate crimes that disproportionately affect that community more than any other minority group.[22] In the United Kingdom, polling supported by the Stonewall charity found that one in 10 LGBTQ internet users there were targets of online abuse—a figure that increased to one in four for transgender individuals.[23] In addition, elderly citizens are often highly vulnerable to cases of online abuse that result in compromised data and technology systems. This is because they often lack the digital literacy to spot phishing scams and other online threats, making them the single largest group of victims who suffered financial losses as a result of online crimes according to the Federal Bureau of Investigation (FBI).[24] In addition, a Home Instead Senior Care report found that two-thirds of U.S. senior citizens have been the victim or target of an online scam or hack.[25] Further research should expand on the challenges these communities face and explore potentially useful strategies that other marginalized groups deploy.

Existing Policies and Gaps

The United States has a limited set of policies in place that serve to mitigate and potentially criminalize instances of digital abuse against vulnerable communities. The majority of these policies address cases as they relate to youth and women. However, they fail to effectively account for the intersectional nature of online abuse including cases that result in attacks on data and technology systems. The following is a non-exhaustive overview describing relevant policies and statutes in the United States:

- Every state in the United States has some form of anti-bullying legislation.
- All but two states (Alaska and Wisconsin) have legislation that deals specifically with cyberbullying or online harassment.
- Every state except Montana mandates that schools have a formal policy to "help with the identification of the [bullying] behavior and discuss the possible formal and/or informal disciplinary responses."
- In all but five states (Alabama, Michigan, Montana, Nevada, New Hampshire), schools are able to discipline students in appropriate and measured ways in cases related to bullying.
- In federal law, the stalking statute (18 USC § 2261A) criminalizes instances of cyberstalking through the use of an "interactive computer service."
- Almost every state has laws that address cyberstalking, cyberbullying, or both.
- Over 40 states have passed laws that criminalize the posting of nonconsensual intimate images (NCII).
- There is currently pending federal legislation, the Interstate Doxxing Prevention Act, which seeks to outlaw doxxing.

There are also several national, regional, and international instruments for combating technology-facilitated abuse and exploitation of vulnerable groups. These include:

- United Nations Conventions on the Rights of the Child
- United Nations Convention against Transnational Organized Crime
- Council of Europe Convention on Cybercrime
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse
- African Charter on the Rights and Welfare of the Child

- Convention on the Elimination of All Forms of Discrimination Against Women

Currently, legislation in the United States only recognizes a handful of online abuse and harassment instances, including cyberbullying and stalking. As technology continues to develop and evolve, developing corresponding legislation that accounts for these technological changes is challenging. In addition, under the First Amendment there is a constitutional limit to the types of conduct that can be outlawed, and as a result any laws that attempted to criminalize certain forms of harmful conduct may simultaneously impinge on the free speech rights of users.

In addition, prosecuting cases of online abuse that are criminally prohibited by statute can be challenging because of a lack in resources that have been devoted to effectively training law enforcement agents to enforce these laws. When victims of such incidents approach law enforcement, they are typically underserved since the agents, despite usually having the will to help, lack the proper training to manage cases and effectively support victims. Several of our interviewees reported that because of this, many victims, especially youth and women, are often hesitant to come forward about instances of online abuse.

Greater commitment to enforcing existing laws, including providing sufficient training to law enforcement agents is vital. It is also critical that this training addresses the distinction between criminal conduct and protected free speech and free expression.

There is also a significant gap in terms of how society is educated on these issues. Over the past few years high schools and colleges across the United States have adopted more stringent trainings and engaging discussions on topics such as cyber bullying. However, these trainings and discussions have not yet filtered to middle and elementary schools and have also not adopted specific carve outs for discussions on topics such as sexual assault and the many manifestations of online abuse against vulnerable communities. In addition, current procedures for engaging with victims and perpetrators in early education environments are minimal, and as a result there is a dearth of both preventive and supportive services. At the university level, on the other hand, there are generally more prescriptive standards that a victim and perpetrator would be subject to in the event of an online or offline incident of abuse or harassment. However, these standards can lack sufficient enforcement.

Looking Forward

As highlighted during our interviews, a single-pronged approach rarely yields enough momentum and engagement to create lasting change. In order to effectively support the digital safety of vulnerable communities, a multi-pronged approach needs to be adopted which empowers and guides 1) individuals and communities, 2) private sector actors, and 3) public sector actors, including legislative and executive law enforcement agencies. A multi-pronged approach is particularly important since many organizations are currently only able to mobilize in one or two of these verticals. Below is an overview of the types of activities and next steps this multi-pronged approach can engage and deploy.

Individual and Community-Based Approaches

Community-based organizations, including individuals and activists representing marginalized groups, are often at the forefront of digital safety issues. These include grassroots digital security organizers and social justice non-profits and groups. While positive impacts of technological development often buttress organizing and advocacy efforts, the negative impacts of rapid technological advancements have a disproportionate impact on individuals who speak out on contentious and politically charged topics. Most community-based organizations and political activists we spoke to were, understandably, incredibly focused on one or two very specific issues. This narrow focus allows each community to develop highly specific strategies that fit their community needs, but often at the expense of sharing best practices with others outside of their constituent group. Through our interviews, we identified two areas where individuals and community-based organizations can improve their efforts to augment the overall digital safety environment:

1) Cross-Community Training: The classic “Digital Security Training” model will be familiar for community activists and digital security and safety experts alike. The format of these trainings tend to go in one of two directions: it is either a broad training that covers issues faced by communities in general, or a narrower training that covers community-specific issues. Broad digital security trainings provide basic tools and practices that establish protection against most common risks related to online abuse. The practices highlighted in such trainings include generating strong and diverse passwords in order to protect oneself from being hacked, backing up files, and developing an understanding of personal devices, software, and services and their respective privacy policies.

Community-based organizations, including individuals and activists representing marginalized groups, are often at the forefront of digital safety issues.

The second digital security training model is more narrow and issue-specific, and focuses on highlighting idiosyncratic digital security threats that face particular communities and presenting strategies that are tailored to these threats. Many of the practices highlighted in these trainings are similarly related to securing oneself against online abuse, including compromised data and technology systems, although depending on the community these trainings can also include information on securing oneself against online abuse as well as against surveillance. For example, for female victims of domestic violence, this could include how to secure devices in order to protect personal data and technology systems, such as location data, in order to prevent it from being compromised or monitored by abusers. In our conversations, we found that there is little "cross-community" training taking place, regardless of whether or not a digital security training was geared towards a broader or a more specific audience. However, there is a great deal of potential in cross-community digital security and safety trainings as the tools and remedies that one community engages with could offer valuable lessons and insights to another community.

While the specific vulnerabilities each community faces online are inherently different given the particular sensitivities and characteristics of each group, the tactics for mitigating threats are ultimately very similar. If women's rights activists, for example, have developed a tool or best practice for responding to doxxing, it could be incredibly useful for racial and ethnic minority activists to learn from and adopt. The resiliency of each community can only be amplified if they appreciate the intersectional identities inherent to their constituents, thus necessitating a more focused cross-community training initiative.

2) Threat and Information Sharing Platforms: The speed at which digital safety threats emerge and grow to scale makes it nearly impossible for individuals and community-organizers to keep pace. It is unrealistic to expect an individual who is facing an attack or abuse for the first time to be able to respond effectively. Even for individuals who repeatedly face digital safety attacks, the sheer volume of threats can be overwhelming. The same is true for larger organizations and professional groups that face particular challenges in the digital space. We heard this over and over again during our interviews with activists, attorneys, and organizations representing vulnerable populations. Thus, some of our interviews focused in particular on the critical need to understand and share rapidly developing information related to emerging digital safety threats.

Several organizations we spoke to do a particularly good job at sharing this sort of threat and response information with their constituent members (e.g. International Network Against Cyber Hate (INACH), National Network to End Domestic Violence (NNEDV)). INACH, for instance, maintains an active social media and member organization mailing list in order to provide timely updates on emerging threats. In addition, INACH hosts a yearly conference to allow members to collaborate in-person on more difficult, high-level issues. These organizations have created a model that could serve as a guide for a larger, cross-community threat sharing platform where individuals and organizations alike are able to benefit from timely, targeted responses to rapidly developing threats.

If women's rights activists, for example, have developed a tool or best practice for responding to doxxing, it could be incredibly useful for racial and ethnic minority activists to learn from and adopt.

Private Sector Approaches

The private sector, particularly social media companies, plays an important role when it comes to combating instances of online abuse. Over the past few years, most, if not all, of the major internet platforms who host user-generated content have received significant criticism and pressure around their approaches to moderating abusive and violent content online. Many individuals belonging to vulnerable communities, as well as civil society and advocacy organizations, have called out platforms such as Google, Facebook, and Twitter for failing to remove harmful content targeting these communities, or for removing too much content belonging to these groups, effectively silencing their speech. These calls for action raise many important questions, especially as platforms endeavor to moderate content while preserving freedom of expression. Through our interviews we were able to identify three key areas in which private sector actors can improve in order to bolster the digital safety of vulnerable communities and users on their platforms and combat instances of online abuse while still safeguarding freedom of expression.

1) Reporting Mechanisms and Feature Design: For many of the individuals we spoke to, the feature design of these platforms hindered rather than helped their ability to report harmful and abusive content. Many of them cited being unable to find or effectively navigate the reporting forms, and also cited the frustrating lack of clarity that came from receiving very little to no follow up communications from platforms regarding whether their report had been received or actioned. This made it difficult for the users to follow up with the platform on the status of their flag and also required users to engage in a time-consuming process of consistently reaching out to platforms in order to ensure their own safety. In addition, many major social media platforms currently lack appeals processes for flagged content.

In addition, platforms can also increase the accuracy of reporting mechanisms by being more transparent about the content policies and processes that are used to flag and moderate content on their platform. For example, in May 2018, Facebook released a detailed version of their Community Standards, which is meant to be almost identical to the internal guidelines Facebook's content agents use when making moderation decisions.[34] This document outlines the policy rationale for various different types of content and the types of images, texts, and references that are acceptable and prohibited on the platform. Disseminating information on these standards is vital, as it educates users on what content is permissible on a platform and therefore offers clear guidelines for what content should be flagged and what should not.

The feature design of these platforms hindered rather than helped their ability to report harmful and abusive content.

Many of the individuals we interviewed also highlighted that, although major internet platforms have taken significant strides towards promoting greater transparency around their content policies,[35] their approaches to combating online hate and harassment is often flawed. This is because efforts to regulate content often lack context. For example, some platforms' moderation processes involve reviewing individual pieces of content rather than reviewing multiple pieces of content, either sent by a particular user, or received by a particular user, together. This often prevents moderators from identifying and understanding when targeted online attacks are taking place against a particular user, and thus prevents the effective removal of harmful content.

Evaluating the content of posts is also important in identifying content that does not violate company policies and should *not* be removed. For example, human rights groups and activists often repost harmful content published by terror groups or share graphic images of atrocities in an attempt to raise awareness about human rights violations. Given the intent behind these posts, they do not typically violate the content standards of online platforms. However, without background information on the user and their intent, automated systems used to remove content and human moderators often erroneously remove this content, thus impinging on the free expression rights of these groups and users.

The experience of different communities and individuals, however, varies from platform to platform, and often depends on the capacities of a company's Trust and Safety teams.

As new social media products enter the market, the individuals we spoke to also recommended that these engineers and entrepreneurs consider implementing "safety by design." They urged these companies to think about how their platforms could be used for abuse and harassment *before* they actually are, and implement streamlined features that either make it harder to engage in such behavior, or that make it easier for users to report this behavior and secure themselves.

2) Investing in Local Partners: Currently, many platforms fund and liaise with on the ground organizations that have expertise on, and work directly with, vulnerable communities. For example, Twitter hosts a Trust and Safety Council which provides input on the company's safety products, policies and programs. The council is composed of safety advocates, academics and researchers, grassroots advocacy organizations, and community groups. During our interviews, it was continuously emphasized that individual users need to know that they have a support system and a community or organization that they can engage with when engaging with digital safety threats. This is particularly important for helping these individuals understand that they retain their agency and control over their devices and over their online and offline presence. Investing in and engaging with local partners also enables strategy and insight sharing, including cross-community collaboration, which is vital considering that these issues manifest differently across city, state, and national lines. These local organizations are also better equipped than companies when it comes to mitigating and resolving offline manifestations of these online issues.

3) Digital Safety Awareness: Platforms should work to create awareness around digital safety threats and protections as well as acceptable online content and behavioral standards. Many platforms, for example, publish Trust and Safety toolkits that guide users facing digital safety threats on how to protect themselves. Most users, however, do not know that these resources exist, and will often only engage with them once it is too late.

Individual users need to know that they have a support system and a community or organization that they can engage with when engaging with digital safety threats.

Public Sector Approaches

When it comes to safeguarding individuals' digital safety, the public sector and the effectiveness of their efforts are perceived in a mixed manner. Generally, however, the activists and individuals we interviewed agreed that the public sector needs to be doing more. Many criticized the federal government for failing to pass meaningful legislation that secures vulnerable communities from digital safety threats highlighted in this report.

In addition, many of those we interviewed criticized state and local level agents for failing to enforce existing laws around issues such as cyberbullying, doxxing, and online stalking. Still others expressed mixed perspectives on the role and effectiveness of law enforcement when engaging with cases of online abuse. Many of the activists we spoke to highlighted that law enforcement agencies were not trained or equipped enough to handle such cases, while others believed that gradually these agencies were improving, although this improvement process takes time and resources. That being said, there was some recognition of the fact that select states have succeeded in passing legislation and tackling major threats associated with online abuse, such as cyberbullying and the sharing of non-consensual intimate images.

Based on our interviews we were able to identify three key areas in which public sector actors can improve in order to bolster the digital safety of vulnerable communities and users.

1) Enforcement: More progress needs to be made at both the federal and state levels to enforce existing laws around online abuse. In states with existing statutes that provide strong protections for victims of online abuse, prosecutors must be willing to take on cases that will effectively support the victim and send a deterrent message to others who may break the law. In addition, more resources need to be devoted to training public sector officials, ranging from legal professionals to law enforcement officials in enforcing these laws.

2) Law Enforcement Training: Many of the activists we spoke to said that their engagement with law enforcement around cases of online abuse varied based on the law enforcement officer assigned to their case. This is because there is a lack of uniformity and variability in the training officers receive on these issues. Many law enforcement agents still do not consider cases of online abuse and compromised data and technology systems to be serious threats. Currently, the Computer Crime Intellectual Property Crime Group at the U.S. Department of Justice and the Internet Crime Complaint Center (IC3) at the FBI are considered some of the only functioning models for addressing these issues at the federal level in the United States.

However, these organizations typically only address large, national-level cases of fraud and crime where damages are large and the targets are often corporations. Law enforcement agencies at the city, state, and federal level therefore need to receive formal training on how to handle and respond to cases at the individual and community level. There has been progress on this in some states. For example, the New Jersey State Police (NJPD) has a High Tech Crime Bureau which includes a Cyber Crimes Unit. Similarly, the state of Michigan has established a Michigan Cyber Command Center (MC3) which includes a Computer Crimes Unit (CCU) and the Michigan Internet Crimes Against Children (ICAC) Task Force. In addition, organizations such as the National White Collar Crime Center (NWC3) have begun producing resources for law enforcement agents looking to receive training around cyber crime issues.

Based on our interviews, the six core recommendations for improving law enforcement awareness, training, and response to cases involving threats to digital safety, particularly those related to online abuse are:

- Before law enforcement agents can begin to address the idiosyncratic digital safety challenges vulnerable communities face, they need to receive comprehensive training in the basics of cybercrime mitigation and cybercrime forensics. Only after this fundamental base of knowledge is established can they begin addressing individual community needs effectively.

- Law enforcement training on digital safety issues should encompass, but not be limited to, understanding how to effectively engage with victims, how to triage cases, and how to educate victims on mitigation strategies to prevent more incidents going forward.

- Law enforcement agents should be required to receive continued education around digital safety threat issues, especially given that technology continues to rapidly evolve and change.

- There should be a centralized reporting system focused on cases at the individual and community level that victims engaging with threats to their digital safety can turn to. The United Kingdom has adopted such a centralized reporting system. Titled Action Fraud, it is the country's national fraud and cybercrime reporting center.

- Law enforcement agencies that have received training on mitigating and managing digital safety threats should be at the front line of disseminating information on protection and prevention to other organizations, including educational institutions.

- Once law enforcement agents are well versed in digital safety threats and mitigation strategies, they should receive sensitivity and awareness training that pertains to different communities including youth, women, and ethnic and racial minorities.

3) Fostering a Cultural Change Through Institutions: Digital safety threat prevention and mitigation for vulnerable communities through enforcement of existing laws and training for law enforcement are vital avenues for promoting cultural change. But other institutions must also be engaged in order for this norm change to be sustainable and long-term. Many of our interviewees highlighted the responsibility of educational institutions in imparting insights and norms on individuals earlier, rather than later, in life.

Educational institutions also have a responsibility for education across generations. Our interviewees stressed that discussions around acceptable digital behaviors and how to be good digital citizens need to start earlier, in lower levels of education. This is also a particularly important time period as it is when many young technology users are first engaging with technology. These efforts are particularly important in relation to online abuse, such as the sharing of non-consensual intimate imagery, cyber sexual harassment, and online and offline consent, as well as in relation to abuse-related threats, like hacking and phishing, that aim to compromise data and technology systems. This preventive approach was perceived as more impactful in fostering cultural and norm change than the reactive approach of initiating these conversations in higher education, when individuals have likely already experienced or perpetrated such behaviors.

Conclusion

Around the world, cases of online abuse and harassment against marginalized and vulnerable groups are becoming more prevalent. These negative online experiences significantly influence how these individuals and groups navigate the digital space and they can have deleterious impacts on their mental health and ability to exercise basic rights such as free speech and free expression. The inclusion of digital safety tools, mechanisms and resources in the broader digital security landscape is therefore vital, as this will enable the digital space to become an equitable and secure environment.

As outlined in this report, the digital safety challenges that women, youth and racial and ethnic minorities face are similar in many ways. However, many of these communities do not regularly engage with one another to share experiences and best practices related to protecting themselves from digital safety threats. This is an area in which we hope to see future progress and work. In addition, this report highlights a number of approaches that the private and public sectors can employ to meaningfully augment the digital safety of these communities, while also respecting the First Amendment and right to free expression. We hope the recommendations outlined in this report will serve as a valuable guide for these actors going forward.

Appendix

Appendix 1: Digital Safety Threats and Risks

A non-exhaustive overview of the types of digital safety threats and risks an individual can face when engaging with cases of online abuse.

Blackmail

An often criminal act in which coercion and threats to reveal true or false information about an individual to the public or a particular party are made in order to make a gain—most commonly money or property.[36]

Cyberbullying

Cyberbullying is cyber harassment when applied to minors.[37] "Bullying that takes place over digital devices like cell phones, computers and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior."[38]

Cyber Harassment

"The use of Information and Communications Technology (ICT) to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm. Unlike physical harassment involving face-to-face contact, cyber harassment requires the use of ICT and is verbal, sexual, emotional or social abuse of a person, group of organization. The cyber harasser's primary goal is to exert power and control over the targeted victim(s)."[39] Cyber harassment is typically thought to apply to adult-aged individuals.

Cyber Stalking

"The use of Information and Communications Technology (ICT) to stalk, control, manipulate or habitually threaten a child, adult, business or group. Cyberstalking is both an online assailant tactic and typology of psychopathological ICT user. Cyberstalking includes direct or implied threats of physical harm, habitual surveillance and gathering information to manipulate and control a target."[40]

Defamation

"The act of making untrue statements about another which damages his/her reputation."[41]

Doxxing

"Releasing personal information about a target — information that hadn't been public, identifies someone who had been anonymous, or is embarrassing. This could be an address, credit card, photos or any other data uncovered by doxxers and typically posted online. Motives vary from personal revenge to vigilante justice or just mischief."[42]

Flaming

"The act of posting or sending offensive messages over the Internet. These messages, called "flames", may be posted within online discussion forums or newsgroups, or send via e-mail or instant messaging programs."[43]

Hacking

"Unauthorized intrusion into a computer or a network." A hacker may "alter system or security features to accomplish a goal that differs from the original purpose of the system."[44]

Hate Speech

"A communication that carries no meaning other than the expression of hatred for some group, especially in circumstances in which the communication is likely to provoke violence. It is an incitement to hatred primarily against a group of persons defined in terms of race, ethnicity, national origin, gender, religion, sexual orientation, and the like."[45]

Impersonation

In a digital context, impersonation can be understood as pretending "to be someone else online (or by text message) without that person's permission if you mean to cause harm."[46]

Compelled Harm or Suicide

Compelling an individual to harm themselves or commit suicide.

Phishing

"A form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims."[47]

Ransomware

"Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with harm, usually by denying you access to your data. The attacker demands a ransom from the victim, promising—not always truthfully— to restore access to the data upon payment."[48]

Non-Consensual Intimate Image (NCII) Sharing

"The distribution of sexually graphic images of individuals without their consent. This includes both images originally obtained without consent (e.g. by using hidden cameras, hacking phones, or recording sexual assaults) as well as images consensually obtained within the context of an intimate relationship."[49] One common example of the non-consensual sharing of images is revenge porn.

Sextortion

"A serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them images of a sexual nature, sexual favors, or money. The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from your electronic devices unless you comply with their demands."[50]

Swatting

"False reporting an emergency to public safety by a person for the intent of getting a ('SWAT team') response to a location where no emergency exists." Often times the reported crime will be serious in nature such as a "home invasion, shooting or hostage situation, to ensure a robust police response." "Swatters often use caller ID spoofing and other tactics to make the call appear legitimate while simultaneously hiding their identities."[51]

Trolling

"The art of deliberately, cleverly, and secretly pissing people off, usually via the internet, using dialogue."... "The most essential part of trolling is convincing your victim that either a) truly believe in what you are saying, no matter how outrageous, or b) give your victim malicious instructions, under the guise of help."[52]

Appendix 2: Possible Consequences of Digital Safety Threats

A general list of possible consequences or side effects that affect victims and communities subject to cases of digital safety threats.

Individual Impacts

- Self-harm and suicidal ideations
- Depression and post-traumatic stress, including from increased anxiety
- Deterioration of physical health, including from increased rates of substance abuse and risky sexual behavior
- Increased violent behavior
- Alienation and fear of others (especially in youth)
- Lowered academic achievement and aspiration
- Loss of self-esteem and confidence
- Absenteeism from school

Community Impacts

- Self-censorship resulting from the fear of retribution or attack
- Paranoia and anxiety towards other groups, including government and law enforcement, leading to fear of reporting crimes
- Restricted access to digital tools and platforms

Notes

[1] "Half of U.S. Businesses Report Being Hacked," Insur ance Journal, September 29, 2017, https://www.insurancejournal.com/news/national/2017/09/29/465954.htm.

[2] Aaron Smith, Americans & Cybersecurity, January 26, 2017, http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[3] Maeve Duggan, Online Harassment 2017, July 11, 2017, http://www.pewinternet.org/2017/07/11/online-harassment-2017/.

[4] "Urgent Action Needed to Combat Online Violence Against Women and girls, says new UN report," UN Women, September 24, 2015, http://www.unwomen.org/en/news/stories/2015/9/cyber-violence-report-press-release.Duggan, Online Harassment.

[5] Duggan, Online Harassment

[6] For example, the majority of research pertaining to religious minorities was focused on communities and case studies outside of the United States.

[7] Alexander T. Vazsonyi et al., "Online and Offline Bullying Perpetration in a Rural Developmental Context: The Impact by Social Media Use," Journal of Rural Social Sciences 31, no. 2 (2016): http://journalofruralsocialsciences.org/pages/Articles/JRSS%202016%2031/2/JRSS%202016%2031%202%2086-106.pdf.

[8] United Nations Office on Drugs and Crime, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, 2015, http://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.

[9] United Nations Office on Drugs and Crime, Study on the Effects.

[10] Gay, Lesbian & Straight Education Network, Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet, 2013, https://www.glsen.org/sites/default/files/Out%20Online%20FINAL.pdf.Vazsonyi et al., "Online and Offline".

[11] Gay, Lesbian & Straight Education Network, Out Online.

[12] "Harmful Digital Communications Act 2015," Parliamentary Counsel Office: New Zealand Legislative, last modified March 2017, http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html.

[13] "Urgent Action".

[14] Tariq Khokhar, "Chart: In These Countries, Internet Use is Higher Among Women than Men," World Bank Data Blog, March 8, 2017, https://blogs.worldbank.org/opendata/chart-these-countries-internet-use-higher-among-women-men.

[15] Michaela Smiley, "Let's Close the Internet Gender Gap," Mozilla Internet Citizen, March 8, 2017, https://blog.mozilla.org/internetcitizen/2017/03/08/closing-the-internet-gender-gap/.

[16] World Wide Web Foundation, Women's Rights Online: Translating Access into Empowerment, October 20, 2015, https://webfoundation.org/research/womens-rights-online-2015/.

[17] Glaser, J., & Kahn, K. (2005) Online prejudice and discrimination: From dating to hating. In Y. Amichai-Hamburger (Ed.), The social net: Understanding our online behavior, (pp. 247-274). Oxford: Oxford University Press.

[18] Stephen Piggott, "Anti-Muslim Sentiment Dominated Extremist Twitter Accounts After the Election," Southern Poverty Law Center Hatewatch, December 15, 2016, https://www.splcenter.org/hatewatch/2016/12/15/anti-muslim-sentiment-dominated-extremist-twitter-accounts-after-election.

[19] Anti-Defamation League Task Force on Harassment and Journalism, Anti-Semitic Targeting of Journalists During the 2016 Presidential Campaign, October 19, 2016, https://www.adl.org/sites/default/files/documents/assets/pdf/press-center/CR_4862_Journalism-Task-Force_v2.pdf.

[20] Maeve Duggan, 1 in 4 Black Americans Have Faced Online Harassment Because of Their Race or Ethnicity, July 25, 2017, http://www.pewresearch.org/fact-tank/2017/07/25/1-in-4-black-americans-have-faced-online-harassment-because-of-their-race-or-ethnicity/.

[21] Brendesha M. Tynes, PhD, "Online Racial Discrimination: A Growing Problem for Adolescents," American Psychological Association Psychological Science Agenda, December 2015, https://www.apa.org/science/about/psa/2015/12/online-racial-discrimination.aspx.

[22] Haeyoun Park and Iaryna Mykhyalyshyn, "L.G.B.T. People Are More Likely to Be Targets of Hate Crimes Than Any Other Minority Group," New York Times, June 16, 2016, https://www.nytimes.com/interactive/2016/06/16/us/hate-crimes-against-lgbt.html.

[23] May Bulman, "Attacks on LGBT People Surge Almost 80% in UK Over Last Four Years," Independent, September 7, 2017, https://www.independent.co.uk/news/uk/home-news/gay-lgbt-hate-crimes-stats-rise-four-year-physical-verbal-homophobic-abuse-community-a7933126.html.

[24] Federal Bureau of Investigation Internet Crime Complaint Center, Internet Crime Report, 2016, https://pdf.ic3.gov/2016_IC3Report.pdf.

[25] Two-Thirds of Seniors Have Been Scammed Online: Survey," Home Instead Senior Care, https://www.homeinstead.com/news/two-thirds-of-seniors-have-been-scammed-online-survey.

[26] Stop Bullying, "Laws & Policies," Stop Bullying, https://www.stopbullying.gov/laws/index.html.

[27] Currently, specific U.S. federal legislation on cyberbullying does not exist, but in many cases federal civil rights laws are applicable. However, the level of abuse must be significant to lead to federal action, and many civil rights laws do not protect vulnerable communities such as the LGBTQ community on the basis of their sexual orientation.

[28] Cyberbullying Research Center, "Bullying Laws Across America," Cyberbullying Research Center, https://cyberbullying.org/bullying-laws.

[29] Cyberbullying Research Center, "Bullying Laws," Cyberbullying Research Center.

[30] "Cyberstalking Federal Criminal Statutes," The University of North Carolina at Chapel Hill, http://cyberstalking.web.unc.edu/federal-criminal-statutes/.

[31] National Conference of State Legislation, "Telecommunications and Information Technology Crime," National Conference of State Legislation, http://www.ncsl.org/default.aspx?tabid=13495.

[32] Cyber Civil Rights Initiative, "40 States + DC Now Have Revenge Porn Laws," Cyber Civil Rights Initiative, https://www.cybercivilrights.org/revenge-porn-laws/.

[33] H.R.6478 - Interstate Doxxing Prevention Act, H.R. Doc. (2016). https://www.congress.gov/bill/114th-congress/house-bill/6478?r=59.

[34] Facebook, Community Standards Enforcement Report, https://transparency.facebook.com/community-standards-enforcement.

[35] For more on how domestic and international technology platforms have been promoting transparency around their content policies, and on best practices for improving such transparency, see New America's Open Technology Institute's Transparency Reporting Toolkit on Content Takedown Reporting.

[36] Merriam-Webster's Dictionary of Law, [Page 53], https://books.google.com/books?id=JYs74quLWLIC&pg=PA53#v=onepage&q&f=false.

[37] IPredator, "Cyber Harassment Internet Defamation & Internet Trolls," iPredator, https://www.ipredator.co/cyber-harassment/.

[38] Stop Bullying, "What Is Cyberbullying," Stop Bullying, https://www.stopbullying.gov/cyberbullying/what-is-it/index.html.

[39] IPredator, "Cyber Harassment," iPredator.

[40] IPredator, "Cyber Harassment," iPredator.

[41] "Defamation," ALM Media Properties, https://dictionary.law.com/Default.aspx?selected=458.

[42] "What is Doxing," NBC News, https://www.nbcnews.com/feature/101/video/what-is-doxing-440902723506.

[43] Sharpened Productions, "Flaming," TechTerms Dictionary, https://techterms.com/definition/flaming.

[44] "Hacking," Techopedia, https://www.techopedia.com/definition/26361/hacking.

[45] "Hate Speech Law and Legal Definition," US Legal, https://definitions.uslegal.com/h/hate-speech/.

[46] Paul Saputo, "Online Impersonation," Saputo Law Firm, PLLC, last modified November 5, 2015, https://saputo.law/criminal-law/texas/online-impersonation/.

[47] "Phishing," TechTarget, https://searchsecurity.techtarget.com/definition/phishing.

[48] Josh Fruhlinger, "What is Ransomware? How it Works and How to Remove It," CSO, November 13, 2017, https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[49] Cyber Civil Rights Initiative, "Cyber Civil Rights Initiative," Frequently Asked Questions, https://www.cybercivilrights.org/faqs/.

[50] Federal Bureau of Investigation, "What is Sextortion?," FBI Video Repository, https://www.fbi.gov/video-repository/newss-what-is-sextortion/view.

[51] Jamie Ducharme, "Swatting Led to an Innocent Man's Death in Kansas. Here's What to Know About It," TIME, December 31, 2017, http://time.com/5082806/what-is-swatting-tyler-barriss-troy-livingston/.

[52] Glen Coco, "Why Does Nobody Know What 'Trolling' Means?," VICE News, May 10, 2012, https://www.vice.com/en_us/article/ppqk78/what-trolling-means-definition-UK-newspapers.