Combating Hate and White Nationalism in the Digital World

By Aastha Uprety and Danyelle Solomon  August 8, 2018

While the digital world has bolstered the free exchange of ideas and revolutionized the global economy, it also provides new fertile ground for old evils. The spread of violent white nationalist ideology online, rampant algorithmic bias, and homogeneity in the technology industry threaten to undo decades of racial progress and further entrench inequality.

Historically, racial progress in the United States has almost inevitably been followed by racist pushback. The Civil War, emancipation, and Reconstruction were followed by more than 80 years of state-sanctioned violence against African American communities. The gains coming out of the Civil Rights era of the 1960s were immediately met with white backlash and resentment that seeped into the nation’s politics. Policies targeted communities of color with draconian actions, not the least being the weaponization of the criminal justice system. More recently, the historic election of President Barack Obama was followed by a resurgence of violent white nationalism—the alt-right movement¹—which was key to the election of Donald Trump.

This perplexing pendulum of racial progress followed by a rise in racism helps explain the recent resurgence of white nationalism in the United States. This maddening cycle owes itself to Americans’ addiction to collective denial and selective ignorance when it comes to the nation’s history.²

A progressive digital agenda that promotes inclusivity and diversity is needed to address this latest swing and mitigate hate and violence. Without proper oversight, regulation, and accountability to combat the ugliest online realms, society will never reap the full benefits of the digital world. To that end, this issue brief offers some concrete steps policymakers and industry leaders can take to fight racism online and within the industry.
Monitor and mitigate hate online

In 2017, hundreds of white nationalists, using the online chat and voice app Discord, gathered to organize and plan the so-called Unite the Right rally in Charlottesville, Virginia—a violent protest that used the removal of a statue of Confederate Gen. Robert E. Lee as a pretense. On August 11, the torch-wielding mob marched through the city chanting the Nazi slogan “blood and soil” and beat students on the University of Virginia campus. The following day, the mob assaulted counter protesters with mace and clubs. One member rammed his car into a crowd of civilians, killing one woman and injuring dozens more.3

The attacks in Charlottesville were a wake-up call revealing the digital world’s potential for incubating violent ideologies and inspiring domestic terrorists. In reality, hate groups have long relied on online technology to advance their agendas; the digital world provides channels through which hate groups can operate anonymously and communicate without detection. Their ability to reach narrow audiences across a large geography allows these groups to raise money, spread racist propaganda, and lure and indoctrinate new followers.

Halting the spread of violent white nationalism online will require nonprofits and private sector companies in the media and technology industries to devote substantial resources toward research and the development of best practices to address this threat. This research should seek to fully identify and understand patterns of behavior; platforms for communication and indoctrination; and mechanisms for exchanging money and weapons.

In the meantime, media and technology companies should begin implementing clear terms-of-use policies, expand enforcement mechanisms, and put in place measures to ensure transparency and accountability.

Most platforms have terms of use, which lay out the rules users must agree to and abide by to use the service.4 As private companies, online platforms have the right to regulate content on their platform. Companies should monitor hate speech and, if appropriate, act when content violates their terms of use policy. In order to be sufficient, terms of use should state that:

• Users may not engage in promoting hate or violence based on race, color, religion, gender, sexual orientation, gender identity, or disability and that users who do so are subject to suspension or termination.

• Content that fits the above category is subject to removal. A thorough understanding by content reviewers of social, cultural, and political norms can help determine what content warrants removal.

• Users may appeal if they believe they were wrongly affected by the policy.
Expanding enforcement mechanisms should involve employing artificial intelligence, user flags, and well-trained human content reviewers to help to identify and remove hateful content. Some companies have responded to hateful content on their platforms with appropriate actions. For example, following the rally in Charlottesville, PayPal disabled some key right-wing groups from receiving donations on their platform. In addition, Reddit deleted a few of its most hateful subreddits in 2015, which led to a nearly 90 percent decrease in hate speech by users who once frequented those forums.

Along with clearly defined terms of use and robust enforcement mechanisms, companies must commit to transparency and accountability. To protect freedom of expression and ensure that content reviewers take relevant context into account, clear pathways should be in place for users who are denied services due to terms-of-use violations to appeal such decisions. Companies should disclose the methods through which reviewers determine which content to remove and if a user’s actions warrant suspension or termination. In addition, companies should regularly release data on how many users have been denied services, why the users were removed, how many appealed, and how many appealed successfully. Facebook, for example, released its Community Standards Enforcement Preliminary Report, which provides some data on community standards violations and subsequent content removal. YouTube released a similar report on enforcement of their community guidelines. Public access to such information is helpful to researchers studying the impact of content monitoring and removal on curbing online hate.

Lack of oversight on social media platforms helped facilitate Russia’s interference in the 2016 elections. Russian-purchased fake ads targeted users based on their ethnicity, interests, and prior internet histories, and attempted to show discontent and suppress voter participation among key groups such as African Americans. Some ads also targeted conservative voters by using anti-Muslim and anti-immigrant language. In fact, more than half of Russian ads on Facebook used race as a central theme. This instance was a chilling attack on U.S. democracy and also served as an illustration of how content that fuels racial resentment can dominate social media platforms. In May, Facebook committed to undergoing a civil rights audit, partly due to a letter from a group of civil rights organizations in response to both Russian ads and hate speech on the platform. It has also removed fake Russian pages ahead of the midterm elections.

The digital world’s incubation of violent white nationalist groups has allowed them to spread their influence and organize domestic terror attacks in communities of color. The same online tools used by foreign actors to undermine the U.S. democracy further demonstrate how vulnerable these platforms can be to misuse. Nonprofits and companies that provide online services to users must demonstrate their commitment to combating extremism—while protecting free expression—through research, clearly defined terms of use, effective enforcement, and transparency.
Remove online racial bias in all its forms

Racial bias is the implicit or explicit prejudice against racial minorities that results from predominant, often harmful, societal stereotypes about certain racial groups.\textsuperscript{15} In the digital world, racial bias often manifests itself in algorithms used to design social media platforms and search engines.\textsuperscript{16} Algorithms, the functions used by computer programs to make automated decisions, can reflect both the biases of their human programmers as well as the biases in the data these algorithms use to make decisions.\textsuperscript{17} When algorithms produce racially biased outputs on online platforms, companies can discriminate—intentionally and unintentionally—against users of color or promote propaganda that reinforces false narratives and that plays to negative stereotypes. This is not only wrong from an ethical perspective; algorithmic bias also damages the economy by excluding consumers and validates extremist views. Companies must do more to combat racial bias in online algorithms.

Some social media platforms drive content to a user by relying on algorithmic predictions of what the user wants to see based on prior interests, which can sometimes result in intentional or inadvertent discrimination. Targeted ads for credit cards, for example, raise questions about who could be on the receiving end of predatory marketing, especially if race is a distinguishing factor.\textsuperscript{18} Some vendors will price discriminate, or offer different prices to different potential consumers based on an internet user’s ZIP code.\textsuperscript{19} While common, this practice can result in racial discrimination by geography.

While targeting specific audiences is part of the appeal and efficiency of online marketing, advertisers and online platforms must be mindful of practices that may cause harm or unfairly target racial minorities. For example, researchers found that Google posted ads for criminal background checks, as well as credit cards with exorbitant fees and high interest rates on an African American fraternity’s website.\textsuperscript{20} Recently, Facebook has also come under fire for allowing advertisers to target specific audiences by categories including “Ethnic Affinity,” which enabled sellers to basically racially discriminate by excluding users associated with certain characteristics from seeing their ad.\textsuperscript{21} For example, sellers could exclude user traits such as “African Americans” and “Spanish speakers” from their target audience.\textsuperscript{22} After this practice was uncovered, the National Fair Housing Alliance sued Facebook,\textsuperscript{23} claiming that the social media company was violating the Fair Housing Act. Online platforms such as Facebook should commit to updating the algorithms and guidelines used to detect whether an ad is discriminatory. Facebook should be able to catch and prevent not only blatant discrimination—such as preventing a user whose interests include the topic “African American” from seeing a specific ad—but also more discrete discrimination, such as housing redlining via limiting audiences to certain ZIP codes.

Search engine algorithms can also reflect racial bias. One study found that entering black-identifying names into Google displayed ads suggestive of the person having an arrest record, a phenomenon that did not occur as frequently for white-identifying
names. For example, a search for the first names “Latanya” and “Latisha” displayed ads for a background check service, but a search of the names “Kristen” and “Jill” rendered neutral results. Unfortunately, platforms have attempted to justify these instances as objective depictions of online content, but platforms need to take seriously the influence they have over public opinion. Hate groups can take advantage of search engine algorithms to target individuals and elevate their websites in search results, which is only exacerbated when platforms fail to monitor and minimize hate content online. For example, Dylann Roof, who murdered nine African Americans at a church in Charleston, South Carolina, pointed to online searches as the beginning of his descent into the white supremacist online world of hate. Roof said that when he typed “black on White crime” into Google, the search results were populated with propaganda declaring the prevalence of black people assaulting and killing white people, which in part fueled his racial animus.

Technology companies must take steps to prevent racial bias on their platforms by ensuring algorithms do not inadvertently exclude marginalized groups from the digital marketplace or promote violent extremist propaganda.

Implement effective diversity and inclusion policies

Another manifestation of structural racism in the digital world is the lack of diversity within the most powerful technology and social media companies in the world. According to data from 2016, the technology workforce in Silicon Valley was only 2.2 percent black and 4.7 percent Hispanic. This persistent lack of inclusion is a problem that costs companies billions, reduces product quality, and limits the development of innovative solutions to combat online hate and prevent algorithmic bias. To address this issue, the industry must devote significant resources toward recruiting candidates with diverse backgrounds and building safe and inclusive workplace environments.

One effective method of recruiting and hiring more diverse candidates is to target multicultural professional associations at colleges and universities. Another option is the diverse-slate hiring approach, which short lists more than one candidate from underrepresented minority groups and can increase the likelihood of hiring a minority. Diverse hiring should be a priority at all levels of employment, from engineers to executives. Recently, Facebook committed to increasing the diversity of its board members, and Google has pledged to focus their efforts on hiring black and Hispanic women.

However, hiring is not the only concern: Many high-tech companies have trouble retaining employees from underrepresented minority groups. A 2017 study found that 37 percent of people who left their jobs in a technology industry or function listed unfair treatment as a major factor in their decision to leave, and this trend was most prevalent
among underrepresented people of color. This kind of turnover costs companies an estimated $16 billion per year in employee replacement. Additionally, women of color who work in technology roles face unique challenges, including being less likely to be in managerial positions and being paid less than their male counterparts.

To solve the problem of retention, companies must commit to fostering inclusive workplace cultures through methods that go beyond diversity training, such as establishing a diversity executive or council to continually lead inclusion efforts and creating employee resource groups for different minority employees. Companies must also commit to comprehensive and transparent methods for reducing the pay inequity between white workers and underrepresented populations, especially women of color.

The rise of hate online should be another reminder that technology companies must open their doors to underrepresented minorities and leverage those varied perspectives to find new solutions for the greater good. A focus on diversity in recruitment and workplace retention is a good place to start.

Conclusion

The internet is not immune to America’s sordid legacy and, like most of America’s institutions, is equally as porous to racism. While most Americans use the internet to communicate with family and friends or to conduct business and pay bills, there are some that use these platforms for harm. As this nation continues to increase its reliance on technology, it is imperative that technology industries and policymakers work together to develop and implement strategies and policies that mitigate racism, hate, and extremism online.

Aastha Uprety is a fellow for Race and Ethnicity at the Center for American Progress. Danyelle Solomon is the senior director of Race and Ethnicity at the Center.
Endnotes


20 Sweeney, “Online ads roll the dice.”


22 Ibid.


25 Ibid.


28 Ibid.


37 Beasley, “There Is a Supply of Diverse Workers in Tech, So Why Is Silicon Valley So Lacking in Diversity?”

38 Scott, Klein, and Onowakpuri, “Tech Leavers Study.”