THE REPAIR™ PLAN

ADL

Repairing Our Internet Ecosystem to Push Hate and Extremism Back to the Fringes of the Digital World

Online hate and extremism have increased dramatically in recent years, and the consequences have included violent attacks and serious harm, even death. Online platforms often lack adequate policies to mitigate these challenges or fail to enforce these policies effectively. National and state laws and policies require significant updating to hold online platforms and individual perpetrators accountable for enabling hate and extremism. With this plan, ADL offers a comprehensive framework for platforms and policymakers to take meaningful action to decrease online hate and extremism. Like ADL's PROTECT Plan, REPAIR focuses on domestic extremism and terrorism, but goes beyond these issues to address other manifestations and harms of online hate, including online harassment, antisemitism, racism and extremist disinformation.

REPAIR offers a comprehensive framework to meaningfully decrease online hate. There is no single fix to the phenomenon, but REPAIR presents a clear path forward.

To push hate and extremism to the fringes of the digital world, we all must prioritize:

Regulation and reform
Enforcement at scale
People over profit
Access to justice
Interrupting disinformation
Research and innovation

SUMMARY

Regulation and reform

- Government must carefully reform, not eliminate, Section 230 of the Communications Decency Act (CDA 230) to hold social media platforms accountable for their role in fomenting violence, extremist disinformation, and other forms of hate leading to harm. Reform, however, must not result in an overbroad suppression of free speech, nor unintentionally cement the monopolistic power of Big Tech. Government must also pass laws and exercise oversight to help ensure regular reporting by platforms, increased transparency, and independent audits regarding content moderation, algorithms, and engagement features.
- Platforms must be transparent about the functions and impact of their algorithms and engagement features, agree to independent verification, adopt a civil rights lens, and involve communities targeted.

Enforcement at scale

- Government must protect consumers by holding platforms accountable for adopting and consistently enforcing policies designed to identify and combat hate and harassment across sites and platforms, regardless of source and targets.
- Platforms must establish and enforce anti-hate policies at scale and regularly evaluate and report on how product features (e.g., potentially biased algorithms and moderators) and policy enforcement (e.g., different standards for elected officials) fuel discrimination, hate and extremism. Product features like Facebook Groups that have amplified antisemitism, scaled racism and launched destructive conspiracy movements should be re-evaluated. As Jonathan Greenblatt said in the Stanford Social Innovation Review, "If Mark Zuckerberg and his engineers can't improve Facebook Groups, we need to put it out to pasture permanently."

People over profit

- Government must focus on how consumers—and advertisers—are impacted by business models that optimize for engagement and must consider how both algorithmic amplification and monopolistic power impact online hate.
- Platforms must stop recommending or amplifying organizations or content that is associated with hate, misinformation or conspiracies to users—even if it results in less engagement from users. They also must put more resources toward protecting victims and targets of online harassment, countering disinformation and improving content moderation instead of prioritizing the bottom line.

Access to justice

- Government must close gaps in state and federal laws that deny victims redress for serious digital-abuse crimes such as doxing, swatting and non-consensual distribution of intimate imagery.
- Platforms must provide effective resources for users to protect themselves from cyberhate and harassment and report violative content. They must immediately take down content found to pose serious harm to targets of abuse.

Interrupting disinformation

- Government must investigate the nature and impact of product designs that allow hatemongers and extremists to exploit platforms and spread dangerous and hate-based disinformation. They must also support research to identify and encourage new ways of countering dangerous disinformation and interruptions to radicalization.
- Platforms must incorporate anti-hate-by-design practices to mitigate exploitation of social media to spread disinformation, invest in strategies to off-ramp those on the path to radicalization, enforce policies consistently, and work with civil society to mitigate this threat. Just as privacy-by-design has been promoted with some notable success, "anti-hate by design" must be promoted and widely incorporated, and made a fundamental consumer expectation.

Research and innovation

- Government and platforms must focus on research that could slow the spread of online hate, including: (1) measuring online hate; (2) hate and extremism in online games; (3) off-ramping vulnerable individuals who have been radicalized; (4) the connection between online hate speech and hate crimes; (5) new methods of disinformation (e.g. deep fakes); (6) the role of internet infrastructure providers and online funding sources in supporting and facilitating the spread of hate and extremism; (7) the role of monopolistic power in spreading online hate; (8) audio content moderation.
- Researching these areas is crucial to developing innovative yet sustainable solutions to decrease online hate.