Online fraud is a great deal more widespread than many understand. Beyond malware, spam, and phishing attacks, beyond credit card scams and product knock-offs, there is a growing threat from new forms of identity fraud enabled by technological design. Platform companies are unable to manage this alone and Americans need governance.1

Online deception is now a multimillion-dollar global industry. My research team tracks dangerous individuals and groups who use social media to pose as political campaigns, social movements, news organizations, charities, brands, and average people. This emerging economy of misinformation is a threat to national security. Silicon Valley corporations are largely profiting from it, while key political and social institutions are struggling to win back the public's trust.2

Platforms have done more than just given users a voice online. They have effectively given them the equivalent of their own broadcast station, emboldening the most malicious among us.3 To wreak havoc with a media manipulation campaign, all one bad actor needs is motivation. Money also helps. But that's enough to create chaos and divert significant resources from civil society,

---


politicians, newsrooms, healthcare providers, and even law enforcement, who are tasked with repairing the damage. 4 We currently do not know the true costs of misinformation.

Individuals and groups can quickly weaponize social media to cause others financial and physical injury. For example,

1. Fraudsters using President Trump's image, name, logo, and voice have siphoned millions from his supporters by claiming to be part of his re-election coalition. 5 In an election year, disinformation and donation scams should be a concern for everyone. 6

2. Along with my co-researchers, Brian Friedberg and Brandi Collins-Dexter, I have studied malicious groups, particularly white supremacists and foreign actors, who have used social media to inflame racial divisions. 7 Even as these imposters are quickly identified by the communities they target, it takes time for platforms to remove inciting content. 8 A single manipulation campaign can create an incredible strain on breaking news cycles, effectively turning many journalists into unpaid content moderators and drawing law enforcement towards false leads. 9

Specific features of online communication technologies need regulatory guardrails to prevent them from being used for manipulative purposes. These include:

1. Registering, buying, and selling fake accounts, comments, and reviews to generate artificial attention, sometimes using botnets and automated text-generators to game algorithmic systems; 10

2. advertising products designed to inflate engagement metrics and/or force misinformation into users’ search returns, feeds and timelines;\textsuperscript{11} 

3. networked factions (groups of loosely affiliated actors) strategically coordinating harassment, distributing hateful content, or inciting violence for profit or political ends;\textsuperscript{12} 

4. misusing platforms’ donation features to raise funds for dangerous or imposter groups;\textsuperscript{13} 

5. promoting misinformation about health care to sell harmful or ineffective treatments; and\textsuperscript{14} 

6. using deceptively edited audio/video, like “deep fakes” and cheap fakes, to drive clicks, likes, and shares.\textsuperscript{15} 

Regarding the last point, the AI technology commonly called ‘deep fakes’ presents an immediate identity threat. Deep fakes are audio and video that realistically depict a person saying and doing things that never happened.\textsuperscript{16} Social media companies are devising policies to prevent deep fakes


from misrepresenting public figures and average citizens, but this does not mean companies will adequately enforce these terms of service and address the damage done to society.

For example, in a recent report, researchers found 96% of deep fakes are pornography mostly targeting women. This poses troubling questions about harassment and consent. Mary Anne Franks and Danielle Citron have advocated for laws prohibiting non-consensual images because the potential for profit, exploitation, and extortion is high. Unfortunately, even the most cutting-edge detection technology can be fooled by skillful deep fakes. For that reason, we need governance.

My co-researcher Britt Paris and I argue that so-called 'cheap fakes' are a wider threat. Like the doctored video of Representative Pelosi, last week’s decontextualized video of Joe Biden seemingly endorsing a white supremacist talking-point poses a substantial challenge. Because the Biden video was clipped from non-augmented footage, platforms refused to take down this cheap fake. Millions have now seen it. Platforms, like radio towers, provide amplification power and as such they have public interest obligations.

The world online is the real world, and this crisis of counterfeits threatens to disrupt the way Americans live our real lives. Right now, malicious actors jeopardize how we make informed decisions about who to vote for and what causes we support, while platform companies’ own products facilitate this manipulation, placing our democracy and economy at significant risk. What makes manipulated content so dangerous is the ease of distribution and the hidden protocols of moderation.

We must expand the public understanding of technology by guarding consumer rights against technological abuse, including a cross-sector effort to curb the distribution of harmful and manipulated content. As danah boyd and I have written, platform companies must address the power of amplification—separately from content—so that media distribution is transparent and accountable.\(^23\) I urge Congress to do the same. Platforms have politics.\(^24\) Regulation and technology must work in tandem, or else the future is forgery.
