A SAFE HARBOR FOR PLATFORM RESEARCH
Protecting independent researchers and journalists who study social media

PUBLISHED BY THE KNIGHT FIRST AMENDMENT INSTITUTE, JANUARY 2022

Why protect independent platform research?
Social media platforms have an immense influence on society, with billions of users worldwide. What we know about platforms and how they affect our daily lives largely comes from independent researchers and journalists, whose work is proving crucial to diagnosing the ills of social media and identifying possible responses. However, they are often vulnerable to legal threats from platforms. A Safe Harbor for Platform Research, published by the Knight First Amendment Institute at Columbia University, proposes a legal safe harbor for certain research and newsgathering projects, as long as those projects respect user privacy and the integrity of the platforms’ services.

Platform disclosures are insufficient
Platforms conduct their own research, but are selective in what they release to the public. Data that is disclosed often has gaps or is out of date. Meta, for example, provides only limited transparency about certain ads—including ads about social issues, elections or politics—but does not provide the ad targeting information associated with these ads. The platform also provides some information about high engagement content, but does not reveal a given post’s “impressions,” or the number of times the content has been seen.

Liability risks are significant
Researchers who study social media platforms risk legal liability because the terms of service of many platforms prohibit the basic tools of digital research, like automated data collection. For example, in October 2020 Facebook sent a cease-and-desist letter to researchers at NYU Cybersecurity for Democracy claiming that their research into disinformation on Facebook’s platform violates the company’s terms. The following August, Facebook suspended team members’ accounts, cutting off their access to the platform’s transparency tools and data.

Researchers also risk liability under the Computer Fraud and Abuse Act, or CFAA; in the past platforms have interpreted CFAA to prohibit certain violations of their terms of service. “In effect,” write the authors of the paper, “the combination of the platforms’ terms of service and the CFAA give the platforms a veto over journalism and research that is especially urgent.”

The Knight Institute’s safe harbor proposal
Social media platforms cannot be the sole arbiters of research on their own practices.

The Institute’s policy paper outlines a safe harbor policy proposal that protects certain public-interest journalism and research. Legal immunity applies only to projects that:

• Collect data that’s publicly available, certain advertising data, or other data that the Federal Trade Commission determines does not unduly burden user privacy;
• Use data collected via automated means, that’s volunteered by users or collected via dedicated research accounts;
• Are in the public interest and use the data exclusively for that purpose; and
• Take reasonable measures to protect user privacy and refrain from disclosing personally identifying data about anyone other than public officials or figures.

Examples of platform accountability research:
• Facebook said it would stop recommending anti-vaccine groups. It didn’t. The Markup, May 2021.
• Facebook lets ads exclude users by race, ProPublica, 2016.

Sample political ads missed by Facebook

Full proposal: A Safe Harbor for Platform Research by Alex Abdo, Ramya Krishnan, Stephanie Krent, Evan Welber Falcón and Andrew Keane Woods.

For more information about NYU Cybersecurity for Democracy: info@cybersecurityfordemocracy.org cybersecurityfordemocracy.org | Twitter: @cyber4democracy