POLICY PAPER



A Safe Harbor for Platform Research

By Alex Abdo, Ramya Krishnan, Stephanie Krent, Evan Welber Falcón, and Andrew Keane Woods

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

Knight Institute Policy Papers present the Institute's own positions and recommendations on questions regarding technology policy, privacy, and the future of free speech. The proposals advanced in this series are developed internally by Knight Institute staff, and are grounded in the Institute's experience litigating and researching these issues.

The full series is available at knightcolumbia.org.

I. INTRODUCTION

SOCIAL MEDIA PLATFORMS influence public discourse in profound ways. Billions of users worldwide and hundreds of millions in the United States rely on the platforms to connect with each other as well as with businesses, advocacy organizations, and governments. They depend on the platforms for news, including news about politics, political candidates, and elections. Through their business practices, policies, and design decisions, the platforms influence how we engage with one another and with the communities around us, with far-reaching implications for society. Yet even the social media companies themselves do not fully understand this influence. It is vital that the public understand better how the platforms are shaping public discourse—what relationships they encourage or discourage, what information they amplify or suppress, and what communities they bring together or pull apart.

Digital journalism and research are crucial to this process. Many of the most important stories written about the social media platforms have relied on basic tools of digital investigation. For example, investigations by The Markup revealed that YouTube's ad-targeting blocklist includes keywords

associated with social justice but excludes keywords associated with hate.[1] A study by ProPublica and The Washington Post revealed that Facebook's platform played a central role in the spread of misinformation and threats in the months prior to the attack on the Capitol on January 6, 2021.[2] And a study by a Michigan State University professor detailed the means QAnon has used to evade Twitter's attempts to crack down on misinformation.[3]

Unfortunately, many platforms ban tools that are necessary to this kind of journalism and research—tools including the automated collection of public information and the creation of research accounts. Journalists and researchers who use these tools in violation of the platforms' terms of service risk serious consequences. Their accounts may be suspended or disabled. They risk legal liability for breach of contract. And they face potential civil and criminal liability under the Computer Fraud and Abuse Act, which the Department of Justice and some platforms have in the past interpreted to prohibit certain violations of a website's terms of service. The threat of liability has had a significant chilling effect. Journalists and researchers have modified their investigations to avoid violating the platforms' terms of service, even when doing so has made their work less valuable to the public. In some cases, the fear of liability has led them to abandon important projects altogether.

We need a new approach. After documenting the legal risks that reporters and journalists face in studying the platforms, this white paper proposes a legislative safe harbor that would give legal protection to certain newsgathering and research projects focused on the platforms, so long as the projects respect the privacy of the platforms' users and the integrity of the platforms' services. The safe harbor is limited by design, and its adoption would not obviate the need for other reforms—including reforms relating to platform transparency.[4] Enacting the safe harbor, however, would significantly expand the space for digital journalism and research that is urgently needed.

II. THE IMPORTANCE OF PROTECTING INDEPENDENT PLATFORM RESEARCH

MUCH OF WHAT we know about social media platforms comes from independent research and journalism. By collecting data through automated means, soliciting it from willing users, or probing the platforms' algorithms using research accounts, academics and journalists have drawn insights crucial to diagnosing the ills of social media and to identifying possible responses.

One example of independent research into the platforms is the years-long effort by ProPublica to study Facebook's sale of discriminatory advertisements. In 2016, ProPublica reported that it had been able to purchase an advertisement on Facebook that targeted those looking for a house, but that "excluded anyone with an 'affinity' for African-American, Asian-American or Hispanic people."[5] The following year, ProPublica reported that Facebook allowed advertisers to target users who Facebook determined were interested in the topics of "Jew hater," "How to burn jews," and "History of 'why jews ruin the world.'"[6] Also in 2017, it discovered that Facebook enabled employers to display job ads to only younger users.[7] Other researchers have expanded on ProPublica's findings. In September 2019, researchers at Northeastern University, the University of Southern California, and the nonprofit Upturn discovered that Facebook's algorithms delivered neutrally targeted ads in a discriminatory manner based on race and gender,[8] and in September 2021, the organization Global Witness reported that Facebook's algorithms still delivered ads in a discriminatory manner based on gender.[9]

Another example comes from two researchers at New York University's Tandon School of Engineering—Professor Damon McCoy and Ph.D. candidate Laura Edelson. McCoy and Edelson study the spread of disinformation on Facebook's platform, with a particular focus on the spread of disinformation through advertisements and other forms of paid promotion.[10] Their research has relied on data collected from the transparency tools that Facebook makes available to researchers, but it has also relied heavily on data donated by consenting Facebook users through a browser plug-in McCoy and Edelson maintain, called Ad Observer. The plug-in collects the advertisements that Facebook shows to users, along with limited and anonymous information

about how advertisers targeted the ads. Using data collected through Ad Observer, McCoy and Edelson have conducted groundbreaking research into the spread of disinformation on Facebook's platform, demonstrating, for example, substantial flaws in Facebook's enforcement of its political ad policies.[11]

Other researchers and journalists have relied on similar tools to further important investigations into the platforms. The media organization The Markup pays Facebook users to use its Citizen Browser, a custom web browser that collects information about the users' Facebook experiences to inform The Markup's reporting on the platform.[12] The resulting stories have shown that Facebook's platform has accelerated the spread of medical misinformation,[13] permitted the targeting of credit-card ads by age,[14] and recommended political groups to users even after the company committed to ending the practice.[15] Mozilla, the company that makes the Firefox browser, has released Mozilla Rally, an add-on to Firefox that allows users to contribute their browsing data to research studies focused on the tech platforms.[16] And the Mozilla-funded project TheirTube uses research accounts to show how YouTube's algorithmic video recommendations differ based on a user's apparent political views.[17] Generally, researchers can use research accounts to simulate platform users with different demographic, engagement, or other characteristics to reveal how the platforms respond to those differences. TheirTube uses six such accounts to simulate the experiences of six YouTube users with different ideological leanings.[18]

As these examples demonstrate, automated collection, data donation, and research accounts have become essential tools. They allow researchers and journalists to collect data at the scale that is necessary to study large platforms and to investigate the ways in which the platforms' algorithms tailor the experiences of each user. If the use of these digital tools were foreclosed, we would know much less about the ways in which the platforms are shaping our world, online and off.

III. WHY DISCLOSURE BY THE PLATFORMS IS NOT SUFFICIENT

SOCIAL MEDIA PLATFORMS do disclose some data to researchers and to the public voluntarily—some make data available to researchers or journalists, publish the results of internal investigations, and issue transparency reports. But these disclosures are not, and cannot be, a substitute for the independent research and journalism that would be protected by the legislative safe harbor proposed below. There are several reasons for this.

A. The platforms share only limited data

Some platforms make data available to researchers through automated interfaces (i.e., application programming interfaces) or through publicly available web portals. These tools enable important research, but the data to which they give access is generally quite limited. Facebook, for instance, gives authorized researchers and journalists access to data through its Ad Library API and the CrowdTangle tool. But the Ad Library API does not include information about the way in which advertisers targeted their ads, which researchers say is critical to understanding the spread of disinformation;[19] and the API is limited by design to ads related to social issues, elections, or politics,[20] even though other ads can be exploited to spread disinformation or to defraud. Meanwhile, Facebook's CrowdTangle tool allows researchers to study the *engagement* of Facebook posts, but does not reveal a given post's *reach*—though the head of Facebook's own NewsFeed has cautioned that engagement does not "represent what most people see on FB."[21]

Some platforms, including Facebook, have also collaborated with outside researchers, but again, these efforts have generally fallen short. The most heralded partnership to date is Social Science One, an initiative that was intended to allow vetted researchers to access certain data sets that Facebook had not previously shared. The promise of the collaboration fizzled, however, when Facebook finally released to researchers a far more limited set of data than it had initially promised.[22]

B. The data the platforms share is incomplete even on its own terms

The data that platforms provide is sometimes incomplete even on its own

terms. For example, the NYU researchers responsible for Ad Observer have shown in a series of studies that Facebook's Ad Library API, which the company claims contains a comprehensive set of political ads, misses tens of thousands of those ads.[23] And late last year Facebook acknowledged that its Social Science One data set contained major errors.[24] The errors will affect the findings of at least several papers whose data will now need to be reanalyzed. [25]

C. The data platforms share is outdated

In addition to being incomplete, platform-provided data tends to be outdated. The first data provided through the Social Science One project was not made available for almost two years,[26] prompting several funders of the project to pull their support.[27] A new Facebook offering—a set of ad-targeting data for ads that ran between August 3 and November 3, 2020—is entirely static, providing a retrospective look at ad targeting in the lead-up to the 2020 election but offering no insight into currently running ads or even ads that ran in the immediate lead-up to the January 6 riots.

D. The platforms can withdraw access to data on a whim

Like other private companies, social media platforms want positive press, and when transparency commitments lead to journalism or research that is critical of the platforms, these commitments tend to fall away. For example, when Facebook received an onslaught of negative news coverage based on data sourced from its CrowdTangle tool, it responded by breaking up the team of employees responsible for developing the tool.[28] One of Facebook's top executives, Nick Clegg, complained that "our own tools are helping journ[alists] to consolidate the wrong narrative."[29] Executives considered adding additional metrics to the CrowdTangle tool to give the public a fuller view of engagement on Facebook but nixed the idea when they learned that doing so would still show that false and misleading news was extremely popular.[30] Brian Boland, who oversaw CrowdTangle until leaving in July 2021, told The New York Times that Facebook "does not want to invest in understanding the impact of its core products, … And it doesn't want to make the data available for others to do the hard work and hold them accountable."[31]

E. Researchers need to be able to verify data provided by the platforms

Over the last year, a number of federal legislators have introduced bills that would require the platforms to share more data with the public or with credentialed researchers. For example, the Social Media DATA Act, introduced by Reps. Lori Trahan and Kathy Castor, would require digital platforms to maintain for researchers an ad library with detailed information about ads, including a description of the audience that was targeted. The Platform Accountability and Transparency Act, a draft of which was published by Sens. Chris Coons, Amy Klobuchar, and Rob Portman, would require platforms to share data with researchers pursuing projects that have been approved by the National Science Foundation. It would also give the Federal Trade Commission (FTC) authority to require that platforms make certain information available to researchers or the public on an ongoing basis—including ads and information about ads, information about widely disseminated content and content moderation decisions.[32]

Legislation mandating the disclosure of platform data is necessary, but it will not obviate the need for independent journalism and research. A major reason for this is verifiability. Researchers must be able to ensure that datasets are comprehensive, and relying on the platforms' own disclosures is not enough, as the examples described above demonstrate.

IV. INDEPENDENT PLATFORM RESEARCH: A MINEFIELD OF LIABILITY

Journalists and researchers who independently study the platforms using digital tools risk serious legal liability. They risk breach of contract liability for violating platforms' terms of service. They also risk civil and criminal liability under computer abuse laws like the Computer Fraud and Abuse Act (CFAA). Although the Supreme Court's recent decision in *Van Buren v. United States* significantly narrows the applicability of the CFAA to violations of terms of service, it remains unclear how that statute would be applied to many of the kinds of digital investigations discussed in this paper.

A. Contract law

The platforms impose terms of service on their users, usually in the form of clickwrap agreements that outline the terms of use. These are contracts of adhesion, presented to users on a take-it-or-leave-it basis, and they are typically sweeping agreements that are difficult for even lawyers to understand. Many platforms' terms of service prohibit users from engaging in automated data collection or creating research accounts for any purpose. Platforms also reserve the right to change their terms at any time, and to bar any user from accessing their sites.

Facebook's terms of service are illustrative. They prohibit accessing or collecting data from Facebook's platform using automated means without the company's prior permission.[33] They prohibit creating or using accounts solely for research purposes.[34] They prohibit facilitating or supporting *others* in doing these things.[35] They even purport to prohibit *former* users from engaging in any of this conduct.[36]

Collectively, these terms have the effect of entrenching Facebook's status as gatekeeper to journalism and research about Facebook. Facebook routinely sends cease-and-desist letters to people conducting digital investigations of its platform, asserting that their investigations violate the company's terms. For example, in the fall of 2020 Facebook sent a cease-and-desist letter to the NYU researchers running the Ad Observer plug-in, asserting that the plug-in violates the company's terms of service, which prohibit "collect[ing] data from our Products using automated means (without our prior permission)."[37] When the researchers declined to disable the plug-in, Facebook suspended their Facebook accounts, which had the effect of terminating their access to Facebook's Ad Library API and CrowdTangle tool, severely hampering their research into disinformation on the platform.[38]

The enforceability of Facebook's terms against researchers responsible for tools like Ad Observer is not beyond doubt. Researchers could raise a number of compelling arguments to limit the enforcement of platform terms of service that are inconsistent with public policy. But few researchers are in a position to take their chances with litigation. The cost to society of overbroad platform terms of service is not merely the loss of research that is directly prohibited by the terms, but also the research that never takes place because researchers do not have the will or resources to risk litigating against a corporate behemoth in court.

B. Computer abuse laws

Individuals who study the platforms also face liability under a suite of federal and state laws that regulate computer abuse. The most significant of these laws is the CFAA. The CFAA imposes civil and criminal liability on anyone who intentionally accesses a computer "without authorization" or who "exceeds authorized access," and thereby obtains information from the computer.[39] The Department of Justice and platforms have in some contexts interpreted these vague terms to apply to violations of a website's terms of service.[40]

The Supreme Court recently considered the meaning of the CFAA in *Van Buren v. United States*. In that case, the Court clarified that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to him."[41] The Court thus endorsed a "gates-up-or-down" approach to CFAA liability.[42] Under this approach, an individual violates the CFAA if they access a computer or an area of a computer to which they do not have actual access—in other words, if the gates are down. If the gates are up, then the individual has not violated the CFAA, even if they accessed the information for a prohibited purpose.[43]

While *Van Buren* narrows the scope of the CFAA, it does not fully resolve the statute's application to journalism and research focused on the platforms. Read broadly, the case strongly suggests that the CFAA does not prohibit researchers from engaging in the automated collection of information to which they have lawful access, even if these activities violate the platform's terms of service. But the Court explicitly declined to say this. In footnote 8, the Court noted: "For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[44]

Van Buren does not explicitly resolve, then, whether journalists and researchers who violate platforms' terms of service in the course of digital investigations are subject to liability under the CFAA. Again, *Van Buren* suggests that only restrictions governing information *access*, but not information *use*, are relevant to CFAA liability. But as the Court's opinion recognizes, the line between use restrictions and access restrictions is not always clear.[45] A platform could recast a prohibition on "accessing or collecting information

using automated means" as a categorical prohibition on "accessing *the platform* if you access or collect information using automated means." It is not clear whether this limitation would count as a gate under *Van Buren*. Nor is it clear whether the analysis would change if a platform expressly revoked a user's authorization to access the platform in response to a perceived violation of use restriction.

Even within the realm of technological or code-based barriers, the scope of CFAA liability is unclear. Some technological barriers regulate only the method of access, not access itself. For example, rate limits and CAPTCHAs are technological barriers to accessing a website too frequently or with the assistance of an automated script. Would circumventing these barriers trigger CFAA liability? What about creating an account using a fictitious name on a platform like Facebook that is presumptively open to all comers, where anyone can create an account, and where the user accesses only information that anyone could see simply by virtue of having an account (that is, without friending other Facebook users)?

Many of the digital research tools necessary for independent platform research could implicate these limitations. Indeed, several already have, as detailed above. Despite *Van Buren*, the application of the CFAA to research and journalism focused on the platforms remains unclear.

V. PROTECTING PRIVACY

The platforms have good reasons for banning the automated collection of information from their sites *as a general matter*. These companies make it easy for hundreds of millions of people to share an extraordinary amount of information about themselves online, in a format that often lends itself to easy picking by commercial competitors, data aggregators, and intelligence services. And from Cambridge Analytica to Clearview AI, there is no shortage of actors interested in exploiting the personal information of platform users. Users expect platforms to protect their data from bad actors, and platforms have an obligation to do so.

But none of this requires platforms to squelch responsible research and journalism that would serve the public interest.

As an initial matter, it is important to recognize that research and journalism about the platforms often serve users' interests—including their interests in privacy—quite directly. This is in part because digital journalism and research are essential to uncovering the exploitation or mishandling of user data by *the platforms themselves*. For example, data journalists at Gizmodo developed a tool that its researchers and the public could use to study the algorithm Facebook uses to make "creepily accurate"[46] friend recommendations. The tool respected user privacy; all of the data it collected remained on the users' computers unless they explicitly decided to share some of it with Gizmodo.[47] Using the tool, the journalists discovered that Facebook relied on "shadow profile" data to draw sometimes invasive connections between users.[48] For example, the journalists learned that sex workers who had scrupulously separated their real identities from their professional ones were being recommended to their clients as friends.[49] Facebook responded to Gizmodo's investigation with a cease-and-desist letter, claiming that the media outlet's research tool violated the platform's terms of service.[50] Another study run by academic researchers from Princeton and Northeastern universities revealed that Facebook used phone numbers that had been provided by users solely for the purpose of account security (specifically, for two-factor authentication) as a basis for targeting ads.[51]

To its credit, Facebook has acknowledged that its terms of service "sometimes get in the way of" important research and journalism,[52] but it has refused to create an exception to its terms of service for that work. In 2018, the Knight Institute asked Facebook to amend its terms of service to create a contractual safe harbor for the automated collection of data and for the creation of research accounts used to further public-interest and privacy-preserving investigations of the platform.[53] Facebook considered the idea over a period of months but ultimately rejected it, claiming that it could not distinguish between good-faith and bad-faith uses of these tools.

The reality, however, is that it is possible—indeed essential—to distinguish between desirable and undesirable uses of the basic tools of digital investigation. And the law draws exactly this kind of distinction in other contexts. Under the Health Insurance Portability and Accountability Act of 1996, for example, Congress has authorized research relying on extremely sensitive personal health information—mostly with patient consent but in

some circumstances without it. As a society, we have decided that medical research is socially valuable and can be authorized without undue risk to patient privacy. Regulators in Europe have arrived at the same conclusion with respect to research and journalism focused on the social media platforms. The General Data Protection Regulation has an exemption for the processing of personal data "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,"[54] and the Digital Services Act would oblige specific categories of platforms to make data available to vetted researchers.[55]

It is time for regulators in the United States to establish similar protections here for research and journalism focused on the platforms.

VI. A LEGISLATIVE FIX: A SAFE HARBOR FOR RESEARCH AND JOURNALISM

THE MOST STRAIGHTFORWARD way to enable independent research and journalism focused on the platforms would be to establish a legislative safe harbor for that work. A safe harbor would immunize certain investigations from legal liability, eliminating the deterrent caused by the companies' terms of service, the CFAA, and state-law analogs to the CFAA. Attached to this white paper is a draft of a legislative safe harbor that was developed by the Knight Institute and recently incorporated nearly verbatim into the draft Platform Accountability and Transparency Act proposed by Sens. Chris Coons, Rob Portman, and Amy Klobuchar.[56]

Broadly speaking, the Institute's legislative safe harbor would immunize from legal liability certain newsgathering and research projects that involve the collection of information from social media platforms if the projects satisfy a number of criteria designed to protect the privacy of users and the integrity of the platforms.

First, the safe harbor would apply to the collection of only certain kinds of information from the platforms—information that is publicly available, certain information about advertisements, and other categories of information that the FTC determines can be collected by journalists and researchers without unduly burdening user privacy.

Second, the safe harbor would apply at the outset to only three specific methods of collection. It would apply to collection using automated means—for example, the automated collection of public posts by government officials or candidates for office. It would apply to the collection of data voluntarily donated by users—for example, the collection via a browser extension of advertisements shown to a consenting user. And it would apply to the collection of information using research accounts—for example, collection through social media accounts designed by researchers to test how platforms respond to users of different perceived races, genders, political ideologies, etc. The safe harbor would not apply, however, to uses of these methods that would materially burden the operation of a platform.

Third, the safe harbor would apply to a research or newsgathering project only if the purpose of the project were to inform the general public about matters of public concern, and only if the information collected were not used for any other purpose. This restriction would ensure that the safe harbor's protections would extend only to public-interest investigations and not to commercial data aggregation, private investigations, or malicious data collection. It would also deny protection to ostensibly good-faith investigations that later turned out to be malicious in nature.

Finally, the safe harbor would require those invoking its protection to take reasonable measures to protect the privacy of platform users. The FTC would issue regulations describing those measures more precisely, but, at a minimum, the safe harbor would forbid researchers and journalists from disclosing any data that would readily identify a user without that user's consent (unless the user is a public official or public figure), and it would require researchers and journalists to safeguard the data they collect from breaches. The safe harbor would also forbid the use of any data to facilitate surveillance by any government entity.[57]

A few more points about the safe harbor warrant emphasis:

- The safe harbor would apply not to researchers and journalists as such, but to specific investigative projects. Anyone can rely on the safe harbor—if they comply with its requirements. The safe harbor takes this approach because a great deal of useful research and journalism is done by people without formal credentials; because it is notoriously

difficult to define "researcher" and (especially) "journalist"; because investing platforms or the government with the power to define these terms, or to apply them in specific cases, would undermine the value of the safe harbor; and because laws that narrowly define "journalist" and "researcher" might confront First Amendment obstacles.

- The safe harbor leaves it to courts to decide whether any given project is entitled to legal protection. Under this legislative proposal, journalists and researchers would have to consider in the first instance whether their projects fall within the safe harbor. However, any journalist or researcher who is sued by a platform for breach of terms of service, or violation of the CFAA (or analogous state statute), would have to demonstrate to a court that their project did in fact comply with the safe harbor's requirements. In practice, platforms are likely to challenge some projects informally before considering legal action, and as a result, some journalists and researchers will have to (and want to) defend their projects to the platforms to avoid the possibility of litigation.
- Importantly, the safe harbor protects journalists and researchers against legal action by platforms, but it does not require platforms to remove existing technical barriers, and indeed it does not preclude platforms from erecting new ones. The safe harbor would protect journalists and researchers who overcome technical barriers, however—so long as their projects comply with the safe harbor's requirements. In practice, many journalists and researchers are able to do so because their activities are not at the same scale as those of commercial or malicious data aggregators.
- This proposal requires the FTC to further define some of the safe harbor's terms through notice-and-comment rulemaking. For example, it requires the FTC to specify the "publicly available information" that can be collected under the safe harbor. The legislative proposal does not itself provide an exhaustive definition of this term because it is difficult to provide a legislative definition that accounts for variation in platform design and because platform design will change over time. The FTC is better positioned than Congress to define this term—and some of the statute's other terms—and to amend the definitions as

necessary as technology and business practices change.

- The proposal would not relieve platforms of their obligation to protect users against third parties whose activities are not compliant with the safe harbor. Nor would it deprive them of the tools to do so. For example, platforms would (still) be able to erect technical barriers to impede the activities of commercial data aggregators. They would (still) be able to sue third parties under their terms of service, where the third parties' activities did not comply with the safe harbor's requirements. The proposal would simply give journalists and researchers a defense against legal action when their activities meet those requirements.

PLATFORM RESEARCH SAFE HARBOR

A Bill
To increase public understanding of the social media platforms and their impact on society by creating a legal safe harbor that protects certain public-interest journalism and research on the platforms while protecting the privacy of users and the integrity of the platforms.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1 Short Title
This Act may be cited as the "Safe Harbor for Social Media Research Act."

SEC. 2. Definitions

In this Act:

(1) The term "Commission" or "FTC" means the Federal Trade Commission established under the FTC Act.

(2) The term "platform" means a digital service that facilitates public interactions between two or more users who interact through the service via the

Internet.

(3) The term "research account" means an account that is created and used solely for the purposes described in section 3(a) and for no longer than is necessary to achieve those purposes.

SEC. 3. Establishing a safe harbor for journalism and research on the social media platforms

(a) No civil claim will lie, nor will any criminal liability accrue, against any person for collecting covered information as part of a newsgathering or research project on a platform, so long as—

(1) The information is collected through a covered method of digital investigation;

(2) The purpose of the project is to inform the general public about matters of public concern;

(3) With respect to information that is collected through a covered method of digital investigation—

(A) the information is not used except to inform the general public about a matter of public concern;

(B) the person takes reasonable measures to protect the privacy of the platform's users; and

(C) the information is not provided to, used to facilitate surveillance by, or used to provide any other service to a government entity.

(4) With respect to the creation and use of a research account, the person takes reasonable measures to avoid misleading the platform's users; and

(5) The project does not materially burden the technical operation of the platform.

(b) No later than 180 days after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5—

(1) Defining "covered method of digital investigation," which phrase, as defined, must encompass—

(A) the collection of data from a platform through automated means;
(B) the collection of data voluntarily donated by users, including through a browser extension or plug-in; and

(C) the creation or use of research accounts.

(2) Defining "covered information," which phrase, as defined, must encompass—

(A) publicly available information, except that such term should not exclude data merely because an individual must log into an account in order to see it;

(B) information about ads shown on the platform, including the ads themselves, the advertiser's name and disclosure string, and information the platform provides to users about how an ad was targeted;

(C) any other category of information the collection of which the FTC determines will not unduly burden user privacy.

(3) Defining "reasonable measures to protect the privacy of the platform's users" under subsection (a)(3)(B) of this section, including by specifying—

(A) what measures must be taken to prevent the theft and accidental disclosure of any data collected;

(B) what measures must be taken to ensure that the data at issue

is not used except to inform the general public about matters of public concern; and

(C) what measures must be taken to restrict the publication or other disclosure of any data that would readily identify a user without the user's consent, except when such a user is a public official or public figure;

(4) Defining "reasonable measures to avoid misleading the platform's users" under subsection (a)(4) of this section.

(5) Defining "materially burden the technical operation of a platform" under subsection (a)(5).

(c) The Commission may, as necessary, in consultation with relevant stakeholders, amend regulations promulgated pursuant to subsection (b) to the extent such amendment will accomplish the purposes of this title.

(d) At the end of each calendar year, the Commission shall require each operator of any platform that had more than 100,000,000 monthly active users for a majority of months during the preceding 12 months to submit an annual report to the Commission that addresses whether the measures prescribed under subsections (b)(3) and (b)(4) of this section are adequately protecting the platform's users.

VII. CONCLUSION

OUR CURRENT LEGAL regime restricts and deters journalism and research that is vital to the public's ability to understand how social media platforms are shaping public discourse. In effect, 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 safe harbor that the Knight Institute proposes would eliminate that veto by protecting important research and journalism that respects user privacy and the integrity of the platforms.

NOTES

1 Leon Yin & Aaron Sankin, *How We Discovered Google's Social Justice Blocklist for YouTube Ad Placements*, The Markup, Apr. 9, 2021, https://perma.cc/B8ZV-YAHT.

2 Craig Silverman, Craig Timberg, Jeff Kao, & Jeremy B. Merrill, *Facebook Hosted Surge of Misinformation and Insurrection Threat in Months Leading Up to Jan. 6 Attack, Records Show*, ProPublica, Jan. 4, 2022, https://perma.cc/VPS3-9BJ8.

3 Tom Porter, *QAnon networks are evading Twitter's crackdown on disinformation to pump out pro-Capitol-riot propaganda, study says*, Business Insider, Jan. 6, 2022, https://perma.cc/M5VS-PCZU.

4 *See, e.g.*, Laura Edelson, Jason Chuang, Erika Franklin Fowler, Michael M. Franz & Travis Radout, *A Standard for Universal Digital Ad Transparency*, Knight First Amendment Institute at Columbia University, Dec. 9, 2021, https://perma.cc/9QWA-X7FB; Nate Persily, *A Proposal for Researcher Access to Platform Data: The Platform Transparency and Accountability Act*, Journal of Online Trust and Safety, Oct. 2021, https://perma.cc/5TZP-DFNG.

5 Julia Angwin & Terry Parris, Jr., *Facebook Lets Advertisers Exclude Users by Race*, ProPublica, Oct. 28, 2016, https://perma.cc/7ZRL-7CRV; *see also* Julia Angwin, Ariana Tobin & Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica, Nov. 21, 2017, https://perma.cc/5VD5-EG32.

6 Julia Angwin, Madeleine Varner & Ariana Tobin, *Facebook Enabled Advertisers to Reach 'Jew Haters,'* ProPublica, Sept. 14, 2017, https://perma.cc/97SK-NN39.

7 Julia Angwin, Noam Scheiber & Ariana Tobin, *Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads*, ProPublica, Dec. 20, 2017, https://perma.cc/8AVA-LFAG.

8 Muhammad Ali, Piotr Sapiezynski, Miranda Bogen et al., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, Sept. 12, 2019, https://perma.cc/F64S-S8QY.

9 Global Witness, *How Facebook's ad targeting may be in breach of UK equality and data protection laws*, Sept. 9, 2021, https://perma.cc/5WLX-U5DK.

10 The Knight Institute represents McCoy and Edelson in their personal capacities in their dispute with Facebook over their research, discussed further below.

11 Nancy Watzman, *The political ads Facebook won't show you*, Medium, May 12, 2021, https://perma.cc/4GD3-3HCK; *see also* Cybersecurity and Democracy, *Researchers' audit reveals flaws in Facebook's identification of political ads*, Medium, Dec. 9, 2021, https://perma.cc/TET5-N58T.

12 Citizen Browser, *The Markup*, https://perma.cc/U598-FVLT.

13 Corin Faife & Dara Kerr, *Facebook Said It Would Stop Recommending Anti-Vaccine Groups. It Didn't.*, The Markup, May 20, 2021, https://perma.cc/X4KN-ZUX2.

14 Corin Faife & Alfred Ng, *Credit Card Ads Were Targeted by Age, Violating Facebook's Anti-Discrimination Policy*, The Markup, Apr. 29, 2021, https://perma.cc/AD43-NTRR.

15 Corin Faife & Alfred Ng, *After Repeatedly Promising Not to, Facebook Keeps Recommending Political Groups to Its Users*, The Markup, June 24, 2021, https://perma.cc/6YV5-4L46.

16 Mozilla Rally, https://perma.cc/WS23-FHLT.

17 TheirTube, https://perma.cc/HHX7-Q74J.

18 TheirTube, *About*, https://perma.cc/WQ4R-4GAP.

19 NYU Ad Observatory, *FAQ*, https://perma.cc/2DTV-CCQQ.

20 Facebook, *Facebook Ad Library API*, https://https://perma.cc/PG4L-8M9Q.

21 John Hegeman (@johnwhegeman) Twitter (July 20, 2020, 7:38 PM), https://perma.cc/F8NE-RLHE.

22 Craig Timberg, *Facebook Made Big Mistake in Data it Provided to Researchers, Undermining Academic Work*, Wash. Post, Sept. 10, 2021, https://perma.cc/CS45-4URP.

23 Cybersecurity for Democracy, *supra* note 11..

24 Timberg, *supra* note 22.

25 *Id.*

26 Gary King & Nathaniel Persily, *Unprecedented Facebook URLs Dataset Now Available for Academic Research through Social Science One*, Soc. Sci. One, (Feb. 13, 2020), https://perma.cc/EV6X-D2KS.

27 Alex Pasternack, *Frustrated Funders Exit Facebook's Election Transparency Project*, Forbes, Oct. 28, 2019, https://perma.cc/6F9G-2MJU.

28 Kevin Roose, *Inside Facebook's Data Wars*, N.Y. Times, July 14, 2021, https://perma.cc/4TYL-WWWF.

29 *Id*.

30 *Id*.

31 *Id*.

32 As discussed below, the bill also includes the legislative safe harbor drafted by the Knight Institute, with only minor differences.

33 *See id*. § 3(1) (Stating that "you must: Use the same name that you use in everyday life. Provide accurate information about yourself. Create only one account (your own) and use your timeline for personal purposes."); *id*. TOS § 3(2)(3) ("You may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data that you do not have permission to access.").

34 *See id*. § 3(2)(1) ("You may not use our Products to do or share anything: That is . . . misleading.")

35 *See id*. § 3(2) ("You therefore agree not to engage in the conduct described below (or to facilitate or support others in doing so)").

36 *See id*. § 4(2) ("If you delete or we disable your account, these Terms shall terminate as an agreement between you and us, but the following provisions will remain in place: 3, 4.2-4.5"); *see also* Louis Barclay, *Facebook Banned Me for Life Because I Helped People Use It Less*, Slate, Oct. 7, 2021, https://perma.cc/L5HD-DH5S.

37 Facebook TOS § 3.2.3, https://perma.cc/LWX7-JH6Z.

38 Laura Edelson & Damon McCoy, *We Research Misinformation on Facebook. It Just Disabled Our Accounts.*, N.Y. Times, Aug. 10, 2021, https://perma.cc/4C5Z-FDV3.

39 18 U.S.C. § 1030(a)(2)(c).

40 *See, e.g.*, *Sandvig v. Barr*, 451 F. Supp. 3d 73, 81–82 (D.D.C. 2020) (discussing Department of Justice testimony indicating that the government could "bring a CFAA prosecution based" on terms-of-service violations causing "de minimis harm").

41 *Van Buren v. United States*, 141 S. Ct. 1648, 1662, 210 L. Ed. 2d 26 (2021).

42 *Id*. at 1649.

43 *Id*.

44 *Id*. at 1659 n.8.

45 *Id*. at 1662 (noting that "[b]ecause purpose-based limits on access are often designed with an eye to information misuse, they can be expressed as access or use restrictions").

46 Surya Mattu & Kashmir Hill, *Facebook Wanted Us to Kill This Investigative Tool*, Gizmodo, Aug. 7, 2018, https://perma.cc/S28Y-WMUU.

47 Kashmir Hill & Surya Mattu, *Keep Track of Who Facebook Thinks You Know with This Nifty Tool*, Gizmodo, Jan. 10, 2018, https://perma.cc/4GYN-EAH7 ("We designed this tool with your privacy in mind. Your Facebook password and any data gathered from Facebook are stored on your computer. Only you have access. We gather no data, though if you see something (or rather someone) interesting, we'd love to hear from you.").

48 Kashmir Hill, How *Facebook Figures Out Everyone You've Ever Met*, Gizmodo, Nov. 7, 2017, https://perma.cc/W38N-EMYT.

49 Kashmir Hill, *How Facebook Outs Sex Workers*, Gizmodo, Oct. 11, 2017, https://perma.cc/J5BX-BBJ6.

50 *See supra* note 46.

51 Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information*, Gizmodo, Sept. 26, 2018, https://perma.cc/ZT3M-3HX3 (discussing a research paper by Professors Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezynski, and Alan Mislove).

52 Alison Frankel, *Knight Institute demands Facebook amend its rules for journalists, researchers*, Reuters, Aug. 7, 2018, https://perma.cc/2S5P-E89U.

53 *See* Knight Institute, *Facebook Should Lift Restrictions on Public-Interest Journalism and Research* https://perma.cc/84HF-9MAB.

54 Regulation 2016/679 of the European Parlia-

ment and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 89, 2016 O.J. (L 119) 17 (EU).

55 European Commission, Proposal for a Digital Services Act (DSA), 15 December 2020, https://perma.cc/VB3M-BZHU; *see also* Mathias Vermeulen, *The Keys to the Kingdom*, Knight Institute, July 27, 2021, https://perma.cc/EK47-JXND.

56 Platform Accountability and Transparency Act (Draft Bill), S. ____, 117th Cong., https://perma.cc/8C7Z-NSMN. The Knight Institute is thankful for feedback on its proposal from Laura Edelson, Damon McCoy, Seth Berlin, Max Mishkin, Esha Bhandari, Daniel Kahn Gillmor, Michelle Richardson, Daphne Keller, Nate Persily, Ben Lee, Jessica Ashooh, Ethan Zuckerman, Nabiha Syed, Rebecca Weiss, Kurt Opsahl, and a number of individuals at Mozilla. We have not asked these individuals or their organizations to endorse the legislative safe harbor, however, and the views expressed in this white paper should not be attributed to them.

57 The draft bill published by Sens. Coons, Portman, and Klobuchar omits this restriction from the Institute's safe harbor.

About the Authors

Alex Abdo is the inaugural litigation director of the Knight First Amendment Institute at Columbia University. He has been involved in the conception and litigation of nearly all of the Institute's legal challenges.

Ramya Krishnan is a staff attorney at the Knight First Amendment Institute and a lecturer in law at Columbia Law School. Her litigation focuses on issues related to government transparency, protest, privacy, and social media.

Stephanie Krent is a staff attorney at the Knight First Amendment Institute, where she focuses on government transparency, federal employee free speech rights, and government surveillance of speech at the border.

Evan Welber Falcón is a legal fellow at the Knight First Amendment Institute. He previously worked on litigation involving free expression, privacy, and surveillance in the U.S., Latin America, Europe, Africa, and Asia.

Andrew Keane Woods is a professor of law at the University of Arizona College of Law. Woods' teaching and research interests include cybersecurity, the regulation of technology, and international law, both public and private.

© 2022, Alex Abdo, Ramya Krishnan, Stephanie Krent, Evan Welber Falcón, and Andrew Keane Woods.

About the Knight First Amendment Institute

The Knight First Amendment Institute at Columbia University defends the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. It promotes a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government.

knightcolumbia.org

Design: Point Five
Illustration: © Daniel Hertzberg



KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY