BRENNAN CENTER FOR JUSTICE

Comments to the Federal Trade Commission re:
Commercial Surveillance ANPR, R111004

submitted by:

The Brennan Center for Justice at NYU School of Law

November 21, 2022

Rachel Levinson-Waldman, Managing Director
Ivey Dyson, Counsel
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue NW, Ste. 1150
Washington, D.C. 20036

I. Introduction

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize, and defend our country's systems of democracy and justice. The Center is dedicated to protecting the rule of law and the values of constitutional democracy by preserving our liberties while maintaining our security. We have published multiple resources on social media surveillance by governmental entities, such as law enforcement and intelligence agencies, immigration authorities, and school officials and districts.[1] We write to respond to the Federal Trade Commission's Advance Notice of Proposed Rulemaking on commercial surveillance, and we urge the FTC to hold a listening session and workshop on the enforcement of Meta and Twitter's anti-surveillance policies with respect to third-party social media monitoring tools that market and sell their products to law enforcement.[2]

As the Supreme Court has recognized, social media "can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard."[3] Social media is critical for building community; connecting with like-minded people, including on sensitive or controversial topics; engaging in political organizing; sharing artistic expression; and more. As of 2021, nearly three quarters of Americans used at least one social media platform, with around the same percentage of U.S. Facebook users visiting the site every day.[4] This widespread use of social media platforms makes them an attractive source of information and intelligence for law enforcement.

In 2016, Facebook and Twitter announced developer policies prohibiting third-party companies from using social media user data for surveillance. Despite these policies, several companies offer services that gather data from Facebook, Instagram, and Twitter and sell it to law enforcement agencies across the country. These companies use their back-end access to compile publicly available information (including users' public posts and data about their locations, followers, and other connections). These services greatly expand the scope of data available to law enforcement as well as the ease with which they can

1 See, e.g., Faiza Patel et al., *Social Media Monitoring*, Brennan Center for Justice, last modified March 11, 2020, https://www.brennancenter.org/our-work/research-reports/social-media-monitoring; Rachel Levinson-Waldman et al., "Social Media Surveillance by the U.S. Federal Government," Brennan Center for Justice, January 7, 2022, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government; Rachel Levinson-Waldman, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges," *Howard Law Journal* 61 (2018): 523-562, https://www.brennancenter.org/sites/default/files/publications/images/RLW_HowardLJ_Article.pdf; Mary Pat Dwyer, "LAPD Documents Reveal Use of Social Media Monitoring Tools," Brennan Center for Justice, September 8, 2021, https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-reveal-use-social-media-monitoring-tools; and Faiza Patel et al., "School Surveillance Zone," Brennan Center for Justice, April 30, 2019, https://www.brennancenter.org/our-work/research-reports/school-surveillance-zone.

2 These comments do not purport to reflect the views, if any, of the New York University School of Law.

3 Packingham v. North Carolina, 137 S. Ct. 1730 (2017).

4 Pew Research Center, "Social Media Fact Sheet," accessed November 21, 2022, https://www.pewresearch.org/internet/fact-sheet/social-media/.

access millions of data points and review them in real time. Law enforcement has used this type of surveillance to target First Amendment activities, and the tools can amplify the racially disproportionate impacts of both social media monitoring and policing overall.

Below we discuss Meta and Twitter's anti-surveillance policies, how companies selling social media monitoring tools work with local law enforcement, and the impacts of social media monitoring on millions of consumers across the United States. We close by recommending steps the FTC can take to build a public record about the impact of these practices and about the platforms' obligations to protect their users by robustly enforcing their existing policies and strengthening policies where necessary.

II. Executive Summary

Meta (the parent company of Facebook and Instagram) and Twitter have policies in place that prohibit developers from using user data for surveillance purposes. These practices made headlines in 2016 when public records requests revealed that law enforcement agencies across California had been using social media monitoring tools to surveil First Amendment-protected activity, including peaceful protests related to police violence. These services had access to the social media platforms' Application Programming Interfaces (API), which give developers back-end access to publicly available information as well as the ability to query this data in real time. Meta and Twitter took steps in response to these revelations, and their policies have evolved to become more robust. But little is known about how robustly Meta and Twitter implement their policies and there is no comprehensive record of which social media monitoring companies have been penalized or ejected from the platforms for policy violations.

At the same time, some social media monitoring companies claim that they have access to data from Facebook, Instagram, and/or Twitter, and they sell their services and products to law enforcement agencies.[5] The companies often market their services as simplifying investigations and helping officers prevent criminal activity.

[5] See ABTShield, "Executive Summary," accessed November 17, 2022, https://www.brennancenter.org/sites/default/files/2021-12/J153-160-%20White%20paper.pdf; Mike Dvilyanski, David Agranovich, and Nathaniel Gleicher, *Threat Report on the Surveillance-for-Hire Industry*, Meta, December 16, 2021, 7-8, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf (Cobwebs); Lexis-Olivier Ray, "Official Emails Show That LAPD Worked with a Controversial Social Media Surveillance Company during George Floyd Protests," *L.A. Taco*, September 3, 2021, https://www.lataco.com/lapd-social-media-surveillance-protest/ (Dataminr); Benjamin Herold, "Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming," *Education Week*, May 30, 2019, https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05 (Navigate 360; formerly Social Sentinel); Snaptrends, "Social Media Data Collection," accessed November 21, 2022, https://snaptrends.com/social-media-software/data-collection/ (Snaptrends); and Scott McAndrews, Voyager Labs, to Officer [Redacted], Los Angeles Police Department (hereinafter LAPD), October 14, 2020, https://www.brennancenter.org/sites/default/files/2021-11/J930-931-%20Sole%20Source%20Provider%20Letter.pdf (Voyager Labs).

While each tool works differently, they have far-reaching impact. ABTShield, for example, sent about 70,000 tweets per day to the Los Angeles Police Department for a 2020 trial of the tool,[6] flagging tweets on topics chosen by the LAPD, including domestic extremism and American policing.[7] Another tool, Voyager Labs, states that it has the technology to flag individual users as "extremist threat[s]" based on their social media networks.[8] One factor considered by the tool is a user's perceived pride in "Arab heritage."[9]

It is difficult to calculate the impact of social media monitoring tools on Facebook, Instagram, and Twitter users since little is known about how they are used by law enforcement. However, these services are likely to magnify existing risks arising from law enforcement social media monitoring, since they streamline and simplify the surveillance process. For example, the *Intercept* revealed that the social media monitoring tool Dataminr tracked tweets related to protests in the wake of George Floyd's death and shared them with law enforcement.[10] This surveillance can have a chilling effect on activists who often organize online[11] and can be the catalyst for investigations and prosecutions based on First Amendment protected activities.[12]

---

6 Brennan Center for Justice, "Data from the LAPD's Trial of ABTShield," December 15, 2021, https://www.brennancenter.org/our-work/research-reports/data-lapds-trial-abtshield. Notably, Twitter told a reporter that it had terminated ABTShield's access to the platform after these revelations, but it made no further statement on the matter; it is not clear whether the public or other developers would have known of this consequence for violating the platform's policy without the reporter's query. Sam Levin and Johana Bhuiyan, "Revealed: LAPD Used 'Strategic Communications' Firm to Track 'Defund the Police' Online," *Guardian*, December 15, 2021, https://www.theguardian.com/us-news/2021/dec/15/revealed-los-angeles-police-social-media-surveillance-technology.

7 Brennan Center for Justice, "Data from the LAPD's Trial of ABTShield."

8 Rachel Levinson-Waldman and Mary Pat Dwyer, "LAPD Documents Show What One Social Media Surveillance Firm Promises Police," Brennan Center for Justice, November 17, 2021, https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-show-what-one-social-media-surveillance-firm-promises; and Brennan Center for Justice, "LAPD Social Media Monitoring Documents," updated December 15, 2021, https://www.brennancenter.org/our-work/research-reports/lapd-social-media-monitoring-documents.

9 Levinson-Waldman and Dwyer, "LAPD Documents Show What One Social Media Surveillance Firm Promises Police"; and Brennan Center for Justice, "LAPD Social Media Monitoring Documents: J Series," updated December 15, 2021, https://www.brennancenter.org/our-work/research-reports/lapd-social-media-monitoring-documents#j-series (see the section that discusses documents within the J series).

10 Sam Biddle, "Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr," *Intercept*, July 9, 2020, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

11 Elizabeth Stoycheff et al., "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects," *New Media and Society* 21 (2019): 602, 607, 611-12; Brennan Center for Justice, "Doc Society v. Blinken," December 5, 2019, https://www.brennancenter.org/our-work/court-cases/doc-society-v-blinken; and Knight First Amendment Institute, "Twitter, Reddit File in Support of Lawsuit Challenging U.S. Government's Social Media Registration Requirement for Visa Applicants," May 29, 2020, https://knightcolumbia.org/content/twitter-reddit-file-in-support-of-lawsuit-challenging-us-governments-social-media-registration-requirement-for-visa-applicants?_preview_=4d450decff.

12 See, e.g., Gabriella Sanchez and Rachel Levinson-Waldman, "Police Social Media Monitoring Chills Activism," Brennan Center for Justice, November 18, 2022, https://www.brennancenter.org/our-work/analysis-opinion/police-social-media-monitoring-chills-activism (detailing the story of a climate activist in Minnesota

The use of these tools by local law enforcement may also have a heightened impact on Black and Hispanic consumers, especially youth. Dataminr employees, for example, have reported that they were told to target their online surveillance at housing projects populated primarily by people of color.[13] There is also evidence that social media monitoring tools perform poorly at understanding lingo that does not align with "standard" English, such as African-American Vernacular English, and can struggle as well with reliably translating foreign slang.[14] With social media used to target Black and Hispanic users, particularly teens, for gang activity, the questionable accuracy is problematic.[15]

Given the number of Facebook, Instagram, and Twitter users who may be impacted by police use of social media monitoring services, it is critical to obtain a deeper understanding of how Meta and Twitter are implementing their surveillance policies. Accordingly, we request that the FTC: (1) hold a listening forum with consumers, advocates, activists, and practitioners to delve into and create a public record on the harm caused by local law enforcement's use of social media monitoring tools to surveil and collect information about Facebook, Instagram, and Twitter users; and (2) host a workshop with subject matter experts, including independent experts and former Meta and Twitter employees, to learn more about the use of platform and user data by third party social media monitoring tools, the platforms' interpretations of the reach of their anti-surveillance policies, and their efforts to enforce these policies.

A list of the specific questions from the ANPR addressed by this comment and a summary of our responses can be found in the Annex.

III. Development of Anti-surveillance Developer Policies

a. Initial development and implementation of platforms' anti-surveillance policies

In 2016, open records requests from the ACLU of Northern California showed that local law enforcement agencies across California had been using third-party social media

who was surveilled by local law enforcement on social media and eventually charged and prosecuted based in large part on a Facebook video of her speaking at a rally); https://www.kansas.com/news/local/crime/article243267626.html [paywalled], GoFundMe, "Justice for Rashawn Mayes," accessed November 21, 2022, https://www.gofundme.com/f/justice-for-rashawn-mayes.

[13] Sam Biddle, "Twitter Surveillance Startup Targets Communities of Color for Police," *Intercept*, October 21, 2020, https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/.

[14] See Natasha Duarte, Emma Llanso, and Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis*, November 2017, 4, 15, https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf.

[15] Biddle, "Twitter Surveillance Startup."

monitoring tools to surveil communities of color and target First Amendment activities.[16] These companies offering these tools had access to publicly available information[17] through social media platforms' Application Programming Interfaces (API), which allow developers access to user data, including the ability to query this data in real time.[18] The companies then sold their services to law enforcement agencies, which could use them to collect massive amounts of information without the need for a warrant.[19] One company, Media Sonar, pitched its services to the Fresno, CA police department by identifying social media terms to track for public safety reasons, including hashtags reflecting peaceful activism for racial justice: #blacklivesmatter, #dontshoot, and #itstimeforchange.[20] Snaptrends, another monitoring service, allowed law enforcement to monitor such hashtags in a given geographic area in real time,[21] with results displayed on social media maps[22] with overlays, including demographics.[23]

In response to widespread media attention, civil society advocacy, and public backlash regarding the ACLU's findings, Facebook, Instagram, and Twitter stopped sharing data with several of these companies[24] and announced changes to their developer policies to

[16] Nicole Ozer, "Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs," ACLU, September 22, 2016, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software.

[17] Babel Street, one of these social media monitoring tools, describes "publicly available information" (PAI) as an "umbrella term" that includes "public-generated content" on "public-facing social media websites" like Instagram. Babel Street, "Publicly Available Information Explained," accessed November 18, 2022, https://www.babelstreet.com/blog/pai-explained. In reality, this includes any content posted publicly by social media users or data derived from publicly posted information, including their locations and relationships with other users.

[18] Meta, "Developer Tools," accessed November 18, 2022, https://developers.facebook.com/?no_redirect=1; and Twitter Developer Platform, "About the Twitter API," accessed November 18, 2022, https://developer.twitter.com/en/docs/twitter-api/getting-started/about-twitter-api.

[19] Courts have generally found that there is no privacy interest in a public social media post and, thus, no Fourth Amendment protection that would require law enforcement to acquire a warrant. See, e.g., People v. Harris, 949 N.Y.S.2d 590, 595 (City Crim. Ct. 2012), *appeal dismissed*, 2013 WL 2097575 (N.Y. App. Term 2013) ("If you post a tweet, just like you scream it out the window, there is no reasonable expectation of privacy."). But see Levinson-Waldman, "Government Access to and Manipulation of Social Media," 558 (arguing that, viewed as a whole, recent cases "stand for the proposition that accumulation and retention of a large quantity of personal information implicates Fourth Amendment rights….").

[20] Angeline MacIvor, senior vice president & co-founder, Media Sonar, to Fresno Police Department, January 27, 2015, 10:45 a.m., https://www.aclunc.org/docs/201512-social_media_monitoring_softare_pra_response.pdf#page=56 (the relevant document appears on pages 56–58 of compiled documents produced to the ACLU of Northern California in 2015 through a Freedom of Information Act (FOIA) request).

[21] Snaptrends, "Twitter Location Search," accessed November 18, 2022, https://snaptrends.com/social-media-software/search-twitter-location/.

[22] Snaptrends, "Facebook Search By Location," accessed November 18, 2022, https://snaptrends.com/social-media-software/search-facebook-location/.

[23] Snaptrends, "Social Media Map – Location-Based Insights," accessed November 18, 2022, https://snaptrends.com/social-media-software/map/.

[24] Matt Cagle, "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color," ACLU of Northern California, October 11, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; Lora Kolodny, "Facebook, Twitter Cut Off Data Access for Geofeedia, A Social Media

address the use of user data for surveillance (with Facebook's policy change covering Instagram as well).

Specifically, in November 2016, Twitter wrote in a blog post that Twitter policies "prohibit developers using the Public APIs and Gnip[25] data products from allowing law enforcement — or any other entity — to use Twitter data for surveillance purposes."[26] The company added that Twitter takes "appropriate action" against violators, including by suspending and terminating access to developer APIs and Gnip data, and promised to take on "expanded enforcement and compliance efforts," including adding more resources for "swiftly investigating and acting on complaints about the misuse of Twitter's Public APIs and Gnip data products."[27]

In March 2017, Facebook's deputy chief privacy officer Rob Sherman announced in a post that the company would be adding language to both Facebook and Instagram platform policies that would prohibit developers from using data "obtained from us to provide tools that are used for surveillance."[28] These anti-surveillance policies were widely publicized in the media.[29]

Surveillance Startup," *TechCrunch*, October 11, 2016, https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/; Twitter Public Policy (@Policy), "Based on information in the @ACLU's report, we are immediately suspending @Geofeedia's commercial access to Twitter data," Twitter, October 11, 2016, 11:14 a.m., https://twitter.com/policy/status/785861128589025281; Dell Cameron, "Twitter Cuts Ties with Second Firm Police Use to Spy on Social Media," *Daily Dot*, October 20, 2016, https://www.dailydot.com/irl/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/; and Lani Rosales, "Snaptrends Quietly Lays Off Entire Staff, Ceases Operations," *American Genius*, October 31, 2016, https://theamericangenius.com/business-news/snaptrends-quietly-lays-off-entire-staff-ceases-operations/. Twitter severed access for Media Sonar in October 2016, and Facebook cut ties at some point in 2016. David Gilmour and Dell Cameron, "Twitter Cuts Off Third Surveillance Firm for Encouraging Police to Spy on Activists," *Daily* Dot, December 9, 2016, https://www.dailydot.com/irl/media-sonar-twitter-social-media-monitoring/; and Jordan Pearson, "Facebook Banned This Canadian Surveillance Company From Accessing Its Data," *VICE*, January 19, 2017, https://www.vice.com/en/article/yp3jw5/instagram-banned-this-canadian-surveillance-company-from-accessing-its-data-media-sonar.

[25] Gnip refers to Enterprise Data APIs. These enterprise products include several different APIs which, for example, allow developers to monitor and filter tweets in real time as well as view tweets dating back to the first ever tweet in 2006. See Twitter Developer Platform, "Documentation," accessed November 18, 2022, https://developer.twitter.com/en/docs/twitter-api/enterprise; Twitter Developer Platform, "PowerTrack API," accessed November 18, 2022, https://developer.twitter.com/en/docs/twitter-api/enterprise/search-api/overview; and Twitter Developer Platform, "Search API," accessed November 18, 2022, https://developer.twitter.com/en/docs/twitter-api/enterprise/search-api/overview.

[26] Chris Moody, "Developer Policies to Protect People's Voices on Twitter," Twitter Developer Platform Blog, November 22, 2016, https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.

[27] Moody, "Developer Policies to Protect People's Voices on Twitter."

[28] Facebook Public Affairs, "We are committed to building a community where people can feel safe making their voices heard," Facebook, March 13, 2017, https://www.facebook.com/fbpublicaffairs/posts/1617594498258356.

[29] See, e.g., Rishabh Jain, "Twitter CEO's Account Temporarily Suspended," Yahoo Finance, November 23, 2016, https://ca.finance.yahoo.com/news/twitter-ceo-account-temporarily-suspended-064508676.html; Colin Lecher, "Facebook Updates Its Platform Policy to Forbid Using Data for Surveillance," *Verge*, March 13, 2017, https://www.theverge.com/2017/3/13/14909248/facebook-platform-surveillance-policy-developers-data;

b. Development of current anti-surveillance policies (Q1)

Since both Meta (the new name for the company that owns Facebook and Instagram) and Twitter have updated their surveillance policies to strengthen the provisions prohibiting developers from sharing user data for law enforcement surveillance. Both companies appear also to have implemented more data use checks on developers to ensure they are abiding by data use terms and policies, though it is not clear whether these act as a substantial limitation on developer activity.

Meta

Meta's current Platform Terms and Developer Policies went into effect on August 31, 2020. The Platform Terms state that developers cannot "perform, facilitate, or provide tools for surveillance," which includes processing data "about people, groups, or events for law enforcement or national security purposes."[30] This policy thus appears to be more comprehensive than the initial policy introduced in 2017, which prohibited the use of user data for surveillance but conspicuously did not define surveillance.[31]

Currently, to retain access to Facebook or Instagram data, developers must complete an annual Data Use Checkup (DUC).[32] The DUC confirms that a developer's API access and data usage comply with Meta's Platform Terms and Developer Policies.[33] It is unknown

Selena Larson, "Facebook Updates Policies to Prohibit Surveillance," CNN, March 13, 2017, https://money.cnn.com/2017/03/13/technology/facebook-surveillance-ban/index.html; Deepa Seetharaman, "Facebook Bans Use of User Data for Surveillance," *Wall Street Journal*, March 13, 2017, https://www.wsj.com/articles/facebook-bans-use-of-user-data-for-surveillance-1489433901; Elizabeth Dwoskin, "Facebook Says Police Can't Use Its Data for 'Surveillance,'" *Washington Post*, March 13, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/; Sam Levin, "Facebook and Instagram Ban Developers from Using Data for Surveillance," *Guardian*, March 13, 2017, https://www.theguardian.com/technology/2017/mar/13/facebook-instagram-surveillance-privacy-data; Matt Rocheleau, "The FBI Just Got Access to Twitter Data. Should You Be Concerned?" *Boston Globe*, November 24, 2016, https://www.bostonglobe.com/business/2016/11/24/the-fbi-just-got-access-entire-twitterverse-should-you-concerned/OPcmIvRhDneSVU1xFoXmrK/story.html?event=event12; and Lily Hay Newman, "Facebook's Big 'First Step' to Crack Down on Surveillance," *Wired*, March 17, 2017, https://www.wired.com/2017/03/facebooks-big-first-step-crack-surveillance/.

30 Meta, "Meta Platform Terms," accessed November 16, 2022, § 3(a)(iii), https://developers.facebook.com/terms/.

31 Meta for Developers, "Legacy Facebook Platform Policy," Meta, accessed November 16, 2022, § 3(1), https://developers.facebook.com/docs/development/terms-and-policies/legacy-facebook-platform-policy; and Meta for Developers, "Legacy Instagram Platform Policy," Meta, accessed November 16, 2022, § A(27), https://developers.facebook.com/docs/development/terms-and-policies/legacy-instagram-platform-policy/.

32 Meta for Developers, "Data Use Checkup," Meta, accessed November 16, 2022, https://developers.facebook.com/docs/development/maintaining-data-access/data-use-checkup.

33 Meta for Developers, "Data Use Checkup." Notably, developers are only directly asked about surveillance when they must complete a Data Protection Assessment (DPA). DPA's are typically required when application developers want to request advanced permissions from application users. These permissions allow the app developers access to users' sensitive data points. Notably, the "public_profile" permission is automatically

what steps Meta would take if the company discovered that a developer had been untruthful in its DUC.

Twitter

Twitter makes clear on multiple developer pages that the use of Twitter API for surveillance is prohibited, explicitly stating that the company forbids the use of "Twitter data and the Twitter APIs by any entity for surveillance purposes, or in any other way that would be inconsistent with our users' reasonable expectations of privacy. Period."[34]

Twitter has not defined surveillance in official documents. While a Twitter executive told the Wall Street Journal in September 2020 that surveillance is the "continuing monitoring of specific people and organizations,"[35] Twitter's current Developer Agreement appears to go farther than this. The Agreement, which went into effect on October 10, 2022, states that unless approved by Twitter, developers may not:

> use, or knowingly display, distribute, or otherwise make Twitter Content, or information derived from Twitter Content, available to any entity for the purpose of: (a) **conducting or providing surveillance or gathering intelligence**, including but not limited to investigating or tracking Twitter users or Twitter Content; (b) **conducting or providing analysis or research for any unlawful or discriminatory purpose, or in a manner that would be inconsistent with Twitter users' reasonable expectations of privacy**; (c) **monitoring sensitive events (including but not limited to protests, rallies, or community organizing meetings)**; or (d) **targeting … or profiling individuals based on sensitive personal information, including their** health (e.g., pregnancy) … **political affiliation or beliefs**, racial or ethnic origin, religious or philosophical affiliation or beliefs, sex life or sexual orientation[, or] Twitter Content relating to any alleged or actual commission of a crime[].[36]

Twitter's developer agreement by its terms thus prohibits the use of its data to monitor protests and similar events, regardless of whether a specific individual or group is the focus of the monitoring, and also takes Twitter users' privacy expectations as a touchstone.

granted and does not require a DPA. See Meta for Developers, "Data Protection Assessment," Meta, accessed November 16, 2022, https://developers.facebook.com/docs/development/maintaining-data-access/data-protection-assessment; and Meta for Developers, "Permissions Reference," Meta, accessed November 21, 2022, https://developers.facebook.com/docs/permissions/reference/.

34 See Twitter, "Developer Agreement," accessed November 16, 2022, §§ XII (B), XII (C), https://developer.twitter.com/en/developer-terms/agreement; and Twitter, "Developer Terms: More about restricted uses of the Twitter APIs," accessed November 16, 2022, https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases.

35 Jeff Horwitz and Parmy Olson, "Twitter Partner's Alerts Highlight Divide Over Surveillance," *Wall Street Journal*, November 16, 2022, https://www.wsj.com/articles/twitter-partners-alerts-highlight-divide-over-surveillance-11601417319.

36 Twitter, "Developer Agreement," § XII (B) (emphasis added).

Regarding developers' role in facilitating governmental access to Twitter data, the Agreement states: "In no event shall [a developer] use, or knowingly display, distribute, or otherwise make Twitter Content, or information derived from Twitter Content, available to any Government End User whose primary function or mission includes conducting surveillance or gathering intelligence."[37] Again, this is a wide-ranging prohibition that looks to the mission of the potential government customer, not simply the specific use to which platform data is put.

This prohibition is baked into developer account registration as well. As of July 24, 2018, anyone seeking to use the Twitter API must apply and receive approval for a developer account.[38] To satisfy this process, applicants must specify a use case and state whether they will make Twitter data available to a government entity.[39] Any sharing of data with a government entity must be submitted for review.[40] Developers additionally must abide by the Developer Policy and Developer Agreement as well as restrictions on certain use cases.[41] Regarding implementation of these policies, a Twitter spokesperson in 2021 stated that they "proactively enforce" policies to ensure compliance, but little specific information is available regarding that process or the outcome.[42]

IV. Local Law Enforcement Use of Third-Party Tools to Surveil Consumers (Qs: 3-4)

Despite Meta and Twitter's anti-surveillance policies, local law enforcement agencies around the country continue to use third-party social media monitoring tools. While a comprehensive accounting is not possible, several sources offer a window into this phenomenon. The Brennan Center submitted public records requests to some of the country's largest police departments to obtain information about their use of social media; while the process is ongoing, we have been able to acquire insight into some departments' practices as well as the services offered by some social media monitoring companies. In addition, supplementary research we conducted shows that nearly half of the 332 U.S. law enforcement agencies operating primarily in jurisdictions of more than 100,000 people have policies addressing the collection of social media data. This suggests that over 150 of

37 Twitter, "Developer Agreement," § XII (C).
38 Yoel Roth and Rob Johnson, "New Developer Requirements to Protect Our Platform," Twitter Developer Platform Blog, July 24, 2018, https://blog.twitter.com/developer/en_us/topics/tools/2018/new-developer-requirements-to-protect-our-platform.
39 Twitter, "Developer Platform Use Cases," accessed November 16, 2022, https://developer.twitter.com/en; and Twitter, "Developer Portal," accessed November 16, 2022, https://developer.twitter.com/en/portal/petition/essential/basic-info (only accessible with a Twitter account).
40 Twitter, "Developer Agreement," § XII (C).
41 Twitter, "Developer Terms: More about restricted uses of the Twitter APIs."
42 Levin and Bhuiyan, "Revealed: LAPD Used 'Strategic Communications' Firm."

these departments, whose combined jurisdictions collectively cover over 60 million individuals, use social media in their work.[43]

In addition, our public records requests and other online sources show that at least six social media monitoring tools still use Facebook, Instagram, and/or Twitter and have contracts with law enforcement, even after the implementation of Meta and Twitter's anti-surveillance policies in 2016.[44] However, with the user base for the three platforms totaling over 400 million consumers in the United States, the potential impact of these monitoring tools is substantial.[45]

The details of several of these tools are below.

ABTShield

ABTShield was developed by Polish software company EDGE NPD.[46] It offers public safety agencies and others a warning system that it contends provides clients with real-time analysis of online traffic to identify current or newly developing threats, based on internet articles, tweets, and comments. It claims to have API connections which allow it access to Twitter and public Facebook pages.[47] Between October and November 2020, the Los Angeles Police Department (LAPD) conducted a pilot of ABTShield. During the pilot, ABTShield sent the LAPD approximately 70,000 tweets per day, accompanied by the username of the account posting the tweet and the number of users who viewed the tweet. These tweets were related to six subjects chosen by the LAPD: domestic extremism and white nationalism, potential danger, civil unrest, election security, the conflict between Armenia and Azerbaijan, and American policing. The LAPD also directed ABTShield to track at least three specific social media handles: two antifascist groups and one account providing live updates on protests in LA County through publicly available civilian reports and police scanners. From these handles, ABTShield delivered 1,400 tweets over the

[43] The Brennan Center conducted online research surveying 332 law enforcement agencies; publication of the research is forthcoming on the Brennan Center's website. The total number of people affected by local law enforcement use of social media was calculated based on the number of individuals living in each of the 153 jurisdictions based on the 2020 census.

[44] These tools include ABTShield, Cobwebs, Dataminr, and Voyager Labs, which are discussed below. Other tools include Navigate360 (formerly Social Sentinel) and Snaptrends. Herold, "Schools Are Deploying Massive Digital Surveillance Systems"; and Snaptrends, "Social Media Data Collection." Notably, Facebook and Twitter claimed to have cut off Snaptrends's API access in 2016. Cameron, "Twitter Cuts Ties with Second Firm."

[45] As of July 2022, the United States had 182.3 million Facebook users, 153.6 million active Instagram users, and 83.4 million Twitter users. See Datareportal, "Facebook Statistics and Trends," accessed November 20, 2022, https://datareportal.com/essential-facebook-stats; Datareportal, "Instagram Statistics and Trends," accessed November 20, 2022, https://datareportal.com/essential-instagram- stats; and Datareportal, "Twitter statistics and Trends," accessed November 20, 2022, https://datareportal.com/essential-twitter-stats. Because it is unclear whether Meta or Twitter has removed developer access for these tools, we do not know whether every tool is using APIs or whether they use some other method, such as scraping, to access information.

[46] Brennan Center for Justice, "Data from the LAPD's Trial of ABTShield."

[47] ABTShield, "Executive Summary," 1.

course of the pilot. Finally, ABTShield and LAPD jointly decided on a list of keywords for ABTShield's daily searches.[48] As of 2021, LAPD is no longer using ABTShield.[49] In response to evidence that it had violated developer policies, a Twitter spokesperson told the *Guardian* in December 2021 that it had cut off ABTShield's developer account.[50]

Cobwebs

Cobwebs pitches itself as an AI-powered internet monitoring service that collects and analyzes data from open sources and social media.[51] Its Tangles tool allows customers to conduct real-time monitoring of geo-locations, keywords, and social media profiles.[52] According to documents obtained by the Brennan Center, the Los Angeles District Attorney's office conducted a trial of Cobwebs in October 2020.[53] Cobwebs has also stated that the Hartford, CT police department used the product in 2019.[54] In December 2021, Meta removed about 200 Cobwebs accounts. According to Meta, Cobwebs "enable[d] reconnaissance" of information from Facebook, Instagram, and Twitter, which appears to have been used for targeting related to law enforcement activities in the United States and abroad.[55] It is not publicly known whether Cobwebs has—or could initiate—other accounts on Facebook or Instagram nor whether it still has access to Twitter data.

Dataminr

Dataminr describes itself as an AI-based platform that uses social media to monitor and track events, using an algorithm to filter through all publicly available social media posts

48 Brennan Center for Justice, "Data from the LAPD's Trial of ABTShield."
49 Michael N. Feuer, city attorney, City of Los Angeles, "Re: Brennan Center v. City of Los Angeles, Case No 20STCP03820: Responses to Production Review Questions," June 25, 2021, 7, https://www.brennancenter.org/sites/default/files/2021-09/2021-06-25%20S.%20Kelly%20Ltr.%20to%20S.%20MacLaren%20re%20CPRA%20Production%20Review%20Questions%20-%20Copy.pdf.
50 Levin and Bhuiyan, "Revealed: LAPD Used 'Strategic Communications' Firm."
51 Cobwebs, "Web Intelligence for a Safer World," accessed November 17, 2022, https://cobwebs.com/; and Cobwebs, *AI-Powered Web Intelligence: Automate Your Investigations*, accessed November 17, 2022, 7, https://www.brennancenter.org/sites/default/files/2021-09/Cobwebs%20Promotional%20Paper.pdf.
52 NW3C Webinar to Alex Rozenblat, "Following the Webinar of Cobwebs Technologies and NW3C," August 20, 2019, 4:02 p.m., https://www.brennancenter.org/sites/default/files/2021-09/Cobwebs%20promotional%20email.pdf.
53 James Rowley, director, sales & business development, Cobwebs, "webinar invite on Geo signals," October 6, 2020, 9:40 a.m., https://www.brennancenter.org/sites/default/files/2021-09/G.%20LADA%20using%20Cobwebs.pdf.
54 PR Newswire, "Cobwebs Technologies, an Israeli Firm Presents its Anti-terror Tech to High-Profile U.S. Delegation," July 10, 2019, https://www.prnewswire.com/il/news-releases/cobwebs-technologies-an-israeli-firm-presents-its-anti-terror-tech-to-high-profile-us-delegation-300882579.html. There is an outstanding FOIA request relating to the Hartford PD-Cobwebs partnership. J. Ader, "Connecticut Freedom of Information Act Request," submitted June 15, 2022, https://www.muckrock.com/foi/hartford-97/foia-cobwebs-technologies-hartford-police-department-130326/.
55 Dvilyanski, et al, *Threat Report on the Surveillance-for-Hire Industry*, 7-8.

made on a given day.[56] The platform's First Alert product provides users with breaking and urgent news alerts based on posts that fall into categories chosen by Dataminr users.[57] Dataminr touts that its alerts can surface breaking news stories before any news source reports on it.[58] The company has access to social media platforms like Twitter and Facebook,[59] and—as an official Twitter partner—has special access to Twitter's "firehose," allowing it to scan every public tweet.[60]

Documents obtained by the Brennan Center show that the Washington D.C. Metropolitan Police Department (MPD) conducted a trial of Dataminr in January 2017.[61] Following this trial, the Director of the MPD's Joint Strategic & Tactical Analysis Command Center put in a purchase request for the tool,[62] and the MPD entered into a $47,950 contract with the company in 2018.[63] In 2019, Dataminr stated that its law enforcement customers included the NYPD, the Chicago Police Department, and Louisiana State Police in 2019.[64] And LAPD's Situational Awareness Watch unit conducted a trial of the First Alert product the same year.[65]

In 2020, Dataminr bundled Twitter content and sent alerts to the Minneapolis police department with locations and images of Black Lives Matter protesters after the death of George Floyd.[66] It is unclear what other local law enforcement entities received information from Dataminr. However, documents show that Dataminr tracked ongoing protests in Brooklyn, Detroit, and cities in Pennsylvania and Virginia.[67] The Illinois State Police also reportedly renewed a contract with Dataminr in May 2021 to monitor crime

56 Dataminr, "Price Quote for Los Angeles Police Department (LAPD)," accessed November 17, 2022, https://www.brennancenter.org/sites/default/files/2021-09/H4-6_Dataminr.pdf; and Dataminr, "Real-time AI for Event and Risk Detection," accessed November 17, 2022, https://www.dataminr.com/?utm_source=twitter%20official%20partners&utm_medium=website&utm_campaign=Dataminr%20profile. Insiders have suggested, however, that individual Dataminr employees have, in the past, been the ones to mine through social media posts. Biddle, "Twitter Surveillance Startup."
57 Ray, "LAPD Worked with a Controversial Social Media Surveillance Company."
58 Dataminr, "Price Quote for LAPD."
59 Ray, "LAPD Worked with a Controversial Social Media Surveillance Company."
60 Twitter Partners, "Dataminr," accessed November 17, 2022, https://partners.twitter.com/en/partners/dataminr; and Biddle, "Police Surveilled George Floyd Protests."
61 [Redacted], Metropolitan Police Department (hereinafter MPD), to Robert Butler et al., "RE: Evaluation Criteria for Dataminr Test," January 25, 2017, 1:51 p.m., https://www.brennancenter.org/sites/default/files/2022-11/DC%20MPD%20Production%20Series%20C%20pp%20432-434%20437-438%20472-473.pdf.
62 Lee Wight, director, Joint Strategic and Tactical Analysis Command Center, MPD, to [Redacted], MPD, March 9, 2017, 8:09 p.m., https://www.brennancenter.org/sites/default/files/2022-11/DC%20MPD%20Production%20Series%20C%20pp%20828-829.pdf.
63 This information was found through GovSpend, a subscription-only online database containing local, state, and federal contracts information. See GovSpend, "About Us," accessed November 21, 2022, https://govspend.com/about/. Records are on file with the Brennan Center.
64 Biddle, "Police Surveilled George Floyd Protests."
65 Andrew Johnston to Jeffrey Brugger, "Re: Dataminr for LAPD: Trial Conclusion - Friday, August 16th," August 20, 2019, 2:41 p.m., https://www.brennancenter.org/sites/default/files/2021-09/H.%20Dataminr%20Trial%202019.pdf.
66 Biddle, "Police Surveilled George Floyd Protests."
67 Biddle, "Police Surveilled George Floyd Protests."

"24/7" and detect "future criminal action.[68] Dataminr has many more local law enforcement partnerships.[69] Twitter takes the position that Dataminr is not in violation of any policies despite the platform's ban on surveillance, and thus has never limited its access.[70]

NC4

NC4, owned by software company Everbridge, claims to offer the "most comprehensive threat data in the industry."[71] According to its marketing materials, its Risk Center provides "real-time, relevant incident alerts," which customers can tailor by location, incident type, and alert perimeter.[72] It appears that NC4 is in use by the LAPD. In May 2022, the Stop LAPD Spying Coalition, a community group focused on police abolition, held a community event at a nonprofit event space in Los Angeles detailing the LAPD's use of social media monitoring tools to surveil activism for racial and social justice. [73] An attorney from the Brennan Center participated in the event to present our findings regarding the LAPD's testing and use of multiple social media monitoring tools. Citing its source as "social media," NC4 reported that "protesters" planned to hold a "demonstration" at the event location and suggested there could be "associated disruptions."[74] Notably, the alert (reproduced below) mischaracterized the event, which was neither a demonstration nor a protest and did not risk causing any disruptions.

[68] Horwitz and Olson, "Twitter Partner's Alerts Highlight Divide."
[69] In addition to the instances highlighted in this paragraph, the Brennan Center was able to find contracts between Dataminr and other law enforcement agencies through an online government procurement portal, GovSpend. The State of New York Division of State Police had annual contracts with Dataminr from 2017-2022. The Virginia State Police had contracts totaling $124,250 in 2017, 2021, and 2022. The San Diego County Sheriff Department had a 1-year license with Dataminr in 2021 for $142,999. Pennsylvania State Police purchased a First Alert license in 2019 for $79,590. The Austin Police Department had an contract with Dataminr in 2019 for an unspecified amount and purchased "notification software" (likely First Alert) in 2020 and 2022 for a total of $112,000. Records on file with the Brennan Center.
[70] Biddle, "Twitter Surveillance Startup." See also Horwitz and Olson, "Twitter Partner's Alerts Highlight Divide."
[71] Everbridge, "Everbridge Announced Acquisition of NC4," August 1, 2019, https://www.everbridge.com/newsroom/article/everbridge-acquires-nc4/.
[72] Everbridge, "Demo: NC4 Risk Center," accessed November 17, 2022, https://go.everbridge.com/NC4-Product-Demo-Reg-Page.html.
[73] Rachel Levinson-Waldman, "Documents Show LAPD Monitoring of Community Meeting on… LAPD Social Media Monitoring," Brennan Center for Justice, September 9, 2022, https://www.brennancenter.org/our-work/analysis-opinion/documents-show-lapd-monitoring-community-meeting-lapd-social-media.
[74] NC4, "Planned Protest in CA (Los Angeles) – Closed," May 18, 2022, 5:54 a.m., Public Records Request 22-6216, 100, https://lacity.nextrequest.com/documents/15096626.

Robinson St & Beverly Blvd - Protesters plan to hold a demonstration at 6 PM on 5/17.

Incident: Advisory, Planned Protest
Severity: Minor
Confirmation: Media
Source: Social Media

Location:
104 Robinson St
Los Angeles, CA, 90026
United States

Occurred: 21:00 EDT 05/17/2022
Updated: 09:05 EDT 05/16/2022

Assets may be Impacted
1) 1.478 miles NW of **Rampart Station**, 1401 W 6th St, Los Angeles, CA, United States
2) 1.62 miles NE of **Olympic Station**, 1130 S Vermont Ave, Los Angeles, CA, United States
3) 2.788 miles NW of **PAB**, 150 N Los Angeles St, Los Angeles, CA, United States
4) 2.871 miles NW of **Central Station**, 251 E 6th St, Los Angeles, CA, United States

Enhanced ActivMobile: Launch Map

Description:
Media sources report that protesters plan to hold a demonstration near Robinson St and Beverly Blvd from 6:00 PM until 8:00 PM local time on Tuesday, May 17. Stop LAPD Spying Coalition has organized the demonstration to protest alleged LAPD social media surveillance. The size of the protest has not been immediately reported. Associated disruptions may occur in the area.

Skopenow

Skopenow is a surveillance technology company that claims it can automatically find, extract, and analyze data through anonymous social media searches and notify users via automated alerts when there are developments in a subject they are tracking.[75] Skopenow says that it extracts social media data from thousands of sources for its reports.[76] This "digital footprint data" includes social media profiles, comments, posts, and usernames.[77] LAPD conducted several trials of Skopenow between November 2018 and June 2020 as well as a demonstration in June 2019.[78] Skopenow disclosed to LAPD that its other clients

[75] Brennan Center for Justice, "Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement Agencies," updated December 21, 2021, https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement.
[76] Skopenow, "Automated Open Source Intelligence," accessed November 17, 2022, https://www.skopenow.com/lawenforcement.
[77] Skopenow, "Frequently Asked Questions," accessed November 20, 2022, https://www.skopenow.com/faq.
[78] Rob Douglas, CEO, Skopenow, to Douglas Stice, detective, Major Crimes Division, LAPD, November 6, 2018, https://www.brennancenter.org/sites/default/files/2021-09/E.%20Multiple%20Skopenow%20Trials.pdf; Rob Douglas to John Warren, "Skopenow Trial," July 10, 2019, https://www.brennancenter.org/sites/default/files/2021-09/E.%20Multiple%20Skopenow%20Trials.pdf; Skopenow to Harold Crossley, "Upgrade your Skopenow Account Today," March 31, 2020, 9:03 p.m., https://www.brennancenter.org/sites/default/files/2021-09/E.%20Multiple%20Skopenow%20Trials.pdf; Skopenow to [redacted], "Skopenow Update: Your pilot has expired!," September 10, 2020, 9:35 p.m., https://www.brennancenter.org/sites/default/files/2021-09/E.%20Multiple%20Skopenow%20Trials.pdf; and Timothy Bourquin, Officer, Major Crimes Division, LAPD, to Rob Douglas, "Re: LAPD Technology Demo day: June 25," May 24, 2019, 9:09 a.m., https://www.brennancenter.org/sites/default/files/2021-09/E.%20Skopenow%20Demo%20June%202019.pdf.
[78] Rob Douglas to Douglas Stice and Mark A. Dolfi, LAPD, "Re: LA County Follow Up," May 28, 2019, 8:44 p.m., https://www.brennancenter.org/sites/default/files/2021-09/Skopenow%20public%20sector%20clients.pdf;

included the Morristown, N.J. police department and the Martin County Sheriff's Office.[79] Public records also show that Skopenow had a contract with the NYPD in 2022, though the details of the contract are unknown.[80]

Voyager Labs

Voyager Labs (Voyager) positions itself as a social media search tool with access to all major social media platforms including Facebook, Twitter, and Instagram.[81] Voyager has developed and sells a variety of tools to collect and analyze information from social media; the LAPD trialed a Voyager tool called VoyagerAnalytics between July and November 2019.[82] The company promotes its products as assisting law enforcement investigations through the use of artificial intelligence to assemble a "picture… of individuals, groups and topics as well as human behavior, affinity and intent."[83] In its sales pitches to the LAPD, Voyager claimed that its tools can analyze people's social media networks (including users without direct connections to the original target of scrutiny) and automatically flag people as "extremist threats," including on the basis of obviously biased factors, such as "pride in… [one's] Arab heritage."[84]

and records from GovSpend on file with the Brennan Center showing contracts with the Martin County Sheriff's Office.

79 Rob Douglas to Douglas Stice and Mark A. Dolfi, LAPD, "Re: LA County Follow Up," May 28, 2019, 8:44 p.m., https://www.brennancenter.org/sites/default/files/2021-09/Skopenow%20public%20sector%20clients.pdf; and records from GovSpend on file with the Brennan Center.

80 Records from GovSpend on file with the Brennan Center.

81 Scott McAndrews, director of sales, Voyager Labs, to Officer [Redacted], LAPD, October 14, 2020, https://www.brennancenter.org/sites/default/files/2021-11/J930-931-%20Sole%20Source%20Provider%20Letter.pdf; and VoyagerAnalytics, "User Guide: Version 5.3," Voyager Labs, April 2019, 2, https://www.brennancenter.org/sites/default/files/2021-11/J983-1007-%20User%20Guide.pdf.

82 Scott McAndrews, director of sales, Voyager Labs, to Rebecca Nagy et al., LAPD, "Voyager Labs trial starting next week (logistics & info insider)," July 10, 2019, 1–2, https://www.brennancenter.org/sites/default/files/2021-11/J0-Voyager%20Trial%20July-November%202019.pdf; Yulia Shvetsova, Intelligence Analyst, Voyager Labs, to Rebecca Nagy et al., LAPD, "Re: Voyager Trial Ending," November 15, 2019, 4:03 p.m., https://www.brennancenter.org/sites/default/files/2021-11/J0-Voyager%20Trial%20July-November%202019.pdf; and Voyager Labs, "LAPD VoyagerAnalytics Trial Highlights," September 18, 2019, https://www.brennancenter.org/sites/default/files/2021-11/J903-916-%20Trial%20Highlights%20July%202019.pdf. Voyager describes VoyagerAnalytics as an "AI-based analysis platform" that is "designed to analyze massive amounts of unstructured open … data" with the goal of revealing "actionable insights." Voyager Labs, "VoyagerAnalytics," accessed November 17, 2022, https://www.voyager-labs.com/platforms/voyageranalytics/.

83 Voyager Labs, "Law Enforcement," accessed November 17, 2022, https://www.voyager-labs.com/solutions/law-enforcement/.

84 Levinson-Waldman and Dwyer, "LAPD Documents Show What One Social Media Surveillance Firm Promises Police"; and Brennan Center for Justice, "LAPD Social Media Monitoring Documents."

V. Consumer Impact (Qs: 4-5, 13)

It is difficult to quantify the impact of third-party social media monitoring tools on users of Facebook, Instagram, and Twitter. However, online monitoring is generally known to chill engagement and facilitate police targeting of First Amendment protected activities. As in the real world, people of color are more likely to be targeted and affected by online monitoring by law enforcement. Social media monitoring tools will magnify these harms by enabling officers to identify activities, associations, individuals, and posts more quickly and cheaply, supercharging officer capacity, and impact, far beyond what police could accomplish by scanning social media on their own.[85] Indeed, this increased capacity has been lauded as an added value offered by third party tools.[86] The concrete impacts of social media monitoring, described below, are well recognized—and as law enforcement agencies' capacity to use social media for monitoring and tracking is magnified, the effects of that monitoring are likely to be magnified as well. Moreover, consumers will likely be unable to discern many of these harms due to the covert nature of social media surveillance and the expectation that Meta and Twitter enforce their anti-surveillance policies.

a. Local law enforcement agencies use social media monitoring tools for targeted surveillance of First Amendment activity.

Social media is central for organizing First Amendment-protected activities, including protests, community building, and advocacy directed at local, state, and federal government. Because of this, law enforcement agencies have used Facebook, Instagram, and Twitter to collect information about these activities, often targeting activists of color and groups advocating for racial justice.

---

85 For example, Voyager Labs advertises its AI investigative tools to "exponentially increase the productivity and outcomes" of law enforcement investigative teams. Voyager Labs, "Make the Invisible Visible: AI-Based Investigative Solutions," accessed November 21, 2022, https://www.voyager-labs.com/. ShadowDragon has bragged that one law enforcement agency evaluated its SocialNet tool, stating that "what used to take us two months in a background check or an investigation is now taking between five to 15 minutes." Michael Kwet, "Shadowdragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move," *Intercept*, September 21, 2021, https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/. ShadowDragon also shares on its webpage a pull-quote from a user who states that "What was once for me a manual and arduous process – i.e., navigate to first social network, search known data points of investigative target, document results, continue to next social network – became an embarrassingly easy single click. This tool doesn't just save time. Using SocialNet for OSINT [open source intelligence] is an absolute game-changer." ShadowDragon, "SocialNet," accessed November 21, 2022, https://shadowdragon.io/socialnet.

86 Voyager Labs, "LAPD VoyagerAnalytics Trial Highlights," 5; and Scott McAndrews, Voyager Labs, to Rebecca Nagy, "FW: another update from Chief," September 30, 2020, 5:52 p.m., https://www.brennancenter.org/sites/default/files/2021-11/J3500-3502-%20Unable%20to%20purchase%20Voyager.pdf.

The Boston Police Department, for example, used Geofeedia to track mentions of the terms #BlackLivesMatter, #MuslimLivesMatter, #Ferguson, and #protest.[87] Similarly, the LAPD used Geofeedia (prior to the institution of the platforms' anti-surveillance policies) to track social media terms relating to activism for racial justice and protests against police brutality, including #sayhername, #BLMLA (Black Lives Matter-Los Angeles), Tamir Rice, and Sandra Bland.[88]

The 2020 racial justice protests for offered additional opportunities for targeting, as Dataminr fed information regarding Black Lives Matter protests to local police. The company used social media to compile a dossier of gatherings against police violence in cities across the U.S. and directed staff to watch for a variety of topics, including posts referencing officers involved in the murder of George Floyd. Days after George Floyd's death, Dataminr sent alerts to the Minneapolis police department; one tweet, which did not reference any violent activity, read: "peaceful protest outside US Bank Stadium in downtown Minneapolis. End racism. End police brutality. End inequality and inequities. #JusticeForFloyd #Minneapolisprotest #BlackLivesMatters[.]" Dataminr sent several other First Alerts to the Minneapolis police with locations of other protests.[89]

Targeting constitutionally protected activity has both online and real-world consequences. When people know they may be monitored online due to their political activity and viewpoints, they may choose to censor their online activity or associations to reduce the risk of governmental monitoring,[90] and are less likely to participate in online political speech.[91]

While this is troubling for all social media users, it is especially problematic for activists who rely on social media for community organizing or sharing knowledge about certain causes. Shanai Matteson, a climate activist from Minnesota who had been targeted by police due in part to her online activity peacefully organizing against an oil pipeline, told us that once she realized her social media was being surveilled for information that could be used against her, she stopped sharing or making posts:

87 Associated Press, "Social Media Surveillance Unfairly Targeted Muslims, Report Says," Fox News, February 7, 2018, https://www.foxnews.com/tech/social-media-surveillance-unfairly-targeted-muslims-report-says; and Iqra Asghar, "Boston Police Used Social Media Surveillance for Years Without Informing City Council," ACLU, February 8, 2018, https://www.aclu.org/news/privacy-technology/boston-police-used-social-media-surveillance-years-without.

88 Geofeedia, "Attachment 1: List of Keywords or Phrases Currently Used," accessed November 11, 2022, https://www.brennancenter.org/sites/default/files/2021-09/H.%20Search%20terms.pdf.

89 Biddle, "Police Surveilled George Floyd Protests."

90 Brennan Center for Justice, "Doc Society v. Blinken"; and Knight First Amendment Institute, "Twitter, Reddit File in Support."

91 Elizabeth Stoycheff et al., "Privacy and the Panopticon," 602, 607, 611-12.

> I thought much, much more about the visibility of what I was saying. I'm a person who wants to share and reflect on my experiences in a public way because that's part of my activism. Once I realized we were being surveilled and information was being used against us in different ways, I stopped sharing and making these kinds of posts. … It made me think, am I safe to share things publicly? Photos of my children? Life events? Political beliefs?[92]

In Memphis, a lawsuit against the city by the ACLU of Tennessee produced revelations about the city's online monitoring and creation of dossiers about activists online.[93] An activist from Memphis shared with us how the "paranoia" caused by social media surveillance undermined his activism:

> During the trial they pulled up screenshots. People say they won't like my posts because of that reason: They saw what the police department was pulling up and they saw the retaliation. … [Since 2016] we had built a really diverse coalition of different people and different groups from people all over the city. We were gaining momentum. But you could feel the paranoia. Not being able to do social media organizing ... our numbers dwindled.[94]

The impact of police monitoring of First Amendment-protected activity extends beyond the chilling effect it has on activists who understand they may currently be, or may become, the subjects of online scrutiny. It can also have concrete consequences, including overreaching investigation and prosecution that is animated by constitutionally protected activity.[95] For example, police in Kansas arrested a Black teenager in 2020 on charges that he had contributed to inciting a riot through a Snapchat post; in fact, his post denounced violence rumored to be coming toward his hometown.[96] And Shanai Matteson, the climate activist mentioned above, was charged and tried for "conspiring, aiding, and abetting" trespass onto an oil pipeline—a charge based only on a video posted on Facebook of her giving a speech at a rally.[97]

---

92 Sanchez and Levinson-Waldman, "Police Social Media Monitoring Chills Activism."
93 Antonia Noori Farzan, "Memphis police used fake Facebook account to monitor Black Lives Matter, trial reveals," *Washington Post*, Aug. 23, 2018, https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/.
94 Interview on file with the Brennan Center.
95 Sanchez and Levinson-Waldman, "Police Social Media Monitoring Chills Activism."
96 Leiker, "Outcry Follows Arrest of 2 Men Over Social Media Post That Urged Violence in Wichita Area"; and GoFundMe, "Justice for Rashawn Mayes."
97 Sanchez and Levinson-Waldman, "Police Social Media Monitoring Chills Activism."

b. Social media monitoring tools used by law enforcement are likely to have an outsized impact on individuals of color.

Social media monitoring tools may create racially disparate impacts through their design and implementation.[98] For example, one 2020 academic study on the use of the social media monitoring tool DigitalStakeout (which had API access to Twitter posts as of 2016) showed that the Corvallis (Oregon) police department's log files from the tool—which contained links to social media posts flagged by predetermined keywords related to law enforcement, terror, and narcotics—had an "apparent higher representation" of Black and Hispanic Twitter users compared to the demographic of Twitter users in the region. While the sample size was too small to prove statistical significance, the authors argued that the study proved that social media monitoring is another avenue to introduce disparities into the justice system and that, unless the population monitored through social media tools mirrors the population of the jurisdiction, bias will result in a "skewed view" or "undue attention" to certain communities.[99]

Indeed, the targeting may be intentional, reflecting police bias. As one group of scholars observed, "the online targeting of distinct communities, and individuals within them, made clear in indictments and other court documents, policy announcements, and strategy outlines, point very convincingly to possible racial and religious bias and profiling when it comes to the way in which online spaces are policed."[100] A New Jersey defense attorney we spoke to shared his view that the police "identify types of social media that they think will cover the people they're looking for. They're using race and age in their choice of where to look." He told the story of a prosecutor who stated, "we can send as many police as we want to a Black or Brown neighborhood, why can't we send them to a Black or Brown part of the internet?"

Additionally, research shows that automated tools suffer from shortcomings in understanding posts by Black or Hispanic users or in dialects that don't align with "standard" English. For example, one study of natural language processing tools found that they miscategorized African American Vernacular English as non-English, with one system incorrectly identifying it as Danish with 99.9% confidence.[101] Natural language processing tools that are trained using one language can also struggle to accurately understand other languages; one person we interviewed who formerly worked in criminal

98 See Desmond Upton Patton et al., "Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations," *Social Media + Society* 3 (2017): 3, https://journals.sagepub.com/doi/10.1177/2056305117733344 (stating that the technology provided by Geofeedia to law enforcement "inherently allow for racist practices as the parameters they employ are user defined and not response driven. If communities of color are socially constructed as problematic sites, then this is where the technological gaze goes …").

99 Glencora Borradaile et. al., "Whose Tweets Are Surveilled for the Police: An Audit of a Social-Media Monitoring Tool via Log Files," *FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020): 570, 579, https://dl.acm.org/doi/abs/10.1145/3351095.3372841.

100 See Patton et al., "Stop and Frisk Online," 7.

101 Duarte, Llanso, and Loup, *Mixed Messages*, 4.

justice lacked confidence in Voyager's ability to accurately interpret non-English slang, like Dominican or Puerto Rican slang, outside of cultural context. In a notorious example, Facebook's own translation tool made an error with serious consequences; a Palestinian man who put up a post saying "good morning" in Arabic was arrested by Israeli police after the platform mistranslated his words as "attack them."[102]

The use of these tools against has real-world impact for communities of color, especially as images and other data gleaned from social media contribute to the wide reach of gang databases,[103] which are typically populated almost entirely with individuals of color. Social media monitoring tools seeking to prove their worth, and whose employees have little guidance or training in assessing actual threats posed by online exchanges, may flood local law enforcements with thinly sourced warnings of potential violence in Black neighborhoods. Employees of the social media monitoring tool Dataminr, for example, reported that they had been specifically directed to monitor areas with a predominantly minority population to pick up ostensible threats. Dataminr employees also reported that they look over "thousands of tweets, posts, and pictures" to find signs indicating that a person might belong to a gang, with a focus on Black and Latino gangs and on poor areas or housing projects with mostly people of color. The results are then pushed to police for further action.[104]

c. Social media surveillance is used to target youth of color for gang activity.

Because social media monitoring tools do not screen for the ages of users whose information is shared with law enforcement, teenagers' online information may be swept up and sent to police. Around 32% of teens use Facebook, 62% use Instagram, and 23% use Twitter.[105] The rate of use for Black and Hispanic youth on Instagram and Twitter is slightly higher than that of white youth.[106]

Black and Hispanic youth may instead find their activity monitored for gang activity by law enforcement. The NYPD "gang database" and NYPD gang policing have been

[102] Alex Hern, "Facebook Translates 'Good Morning' Into 'Attack Them', Leading to Arrest," *Guardian*, October 24, 2017, https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest.
[103] See Statement of Chief Dermot Shea, chief of detectives, New York City Police Department, Before the New York City Council Committee on Public Safety, Committee Room, City Hall, June 13, 2018, 4, https://legistar.council.nyc.gov/View.ashx?M=F&ID=6326528&GUID=F3BFCD82-3FB5-4540-BD17-66D1FA51921B. For a database of stories related to gang databases across the U.S., see Marshall Project, "Gang Database: A Curated Collection of Links," updated July 14, 2022, https://www.themarshallproject.org/records/3980-gang-database.
[104] Biddle, "Twitter Surveillance Startup."
[105] Emily A. Vogels, Risa Gelles-Watnick, and Navid Massarat, "Teens, Social Media and Technology 2022," Pew Research Center, August 10, 2022, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.
[106] Vogels et al., "Teens, Social Media, And Technology 2022."

criticized for targeting Black and Hispanic youth,[107] with evidence that the department has monitored Black children as young as 10 years old.[108] For youth whose communities, families, or neighborhoods may include gang members, social media is a minefield: using certain emojis or hashtags, or being connected in any way with gang members on social media, can be considered "evidence" of gang membership and contribute to conspiracy charges.[109]

This monitoring, while already problematic, can be further complicated by tools that do not understand the nuance of teenage social media use. Previous research suggests that over half of teens on social media share inside jokes or cloak messages in some way and that Black teens are more likely to post fake information to their profiles.[110] According to an insider at Dataminr, this presented issues when tracking gang activity: there was no way for analysts to know whether content flagged as gang activity was simply "mere adolescent tough-guy posturing" with no basis in reality.[111] One researcher studying the interactions of youth gang members found that their social media posts depicting inoperable firearms, fake narcotics, and counterfeit money were "online hyperbole," and that rival gangs were aware of these manufactured posts. These posts were an attempt by gang members to "defend and repair their reputations in … *non-violent* ways."[112] A social media monitoring

[107] See, e.g., Jake Offenhartz, "The NYPD's Expanding Gang Database Is Latest Form of Stop & Frisk, Advocates Say," *Gothamist*, June 13, 2018, https://gothamist.com/news/the-nypds-expanding-gang-database-is-latest-form-of-stop-frisk-advocates-say. See Josmar Trujillo and Alex S. Vitale, *Gang Takedowns in the De Blasio Era: The Dangers of 'Precision Policing,'* Policing & Social Justice Project, Brooklyn College, 2019, 6, https://policingandjustice.squarespace.com/s/2019-New-York-City-Gang-Policing-Report-FINAL.pdf (finding that between August 2003-August 2013, 99% of the 20,000 people added to the NYPD's gang database were non-white, with 30% entering the database as children, and that 98% of the 17,000 people added between 2013-18 were Black or Hispanic); and Rose Hackman, "Is the Online Surveillance of Black Teenagers the New Stop-and-Frisk?," *Guardian*, April 23, 2015, https://www.theguardian.com/us-news/2015/apr/23/online-surveillance-black-teenagers-new-stop-and-frisk.

[108] Hackman, "Is the Online Surveillance of Black Teenagers the New Stop-and-Frisk?" *Guardian*, April 23, 2015, https://www.theguardian.com/us-news/2015/apr/23/online-surveillance-black-teenagers-new-stop-and-frisk; Ben Popper, "How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars," *Verge*, December 10, 2014, https://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison; and New York Police Department, "Detectives," accessed November 21, 2022, https://www.nyc.gov/site/nypd/bureaus/investigative/detectives.page. See Trujillo and Vitale, *Gang Takedowns in the De Blasio Era*, 10.

[109] Sara Robinson, "When a Facebook Like Lands You in Jail," Brennan Center for Justice, July 6, 2018, https://www.brennancenter.org/blog/when-facebook-lands-you-jail. See Popper, "How the NYPD Is Using Social Media to Put Harlem Teens Behind Bars"; Trujillo and Vitale, *Gang Takedowns in the De Blasio Era*, 7; and Sara Dorn, "New York Gangs Are Using Emojis as a Secret Language to Plan Crimes," *New York Post*, August 3, 2019, https://nypost.com/2019/08/03/new-york-gangs-are-using-emojis-as-a-secret-language-to-plan-crimes/.

[110] Mary Madden et al., "Teens, Social Media, and Privacy," Pew Research Center, May 21, 2013, https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/; and Mary Madden et al., "Part 3: Reputation Management on Social Media," Pew Research Center, May 21, 2013, https://www.pewresearch.org/internet/2013/05/21/part-3-reputation-management-on-social-media/.

[111] Biddle, "Twitter Surveillance Startup."

[112] Forrest Stuart, "Code of the Tweet: Urban Gang Violence in the Social Media Age," *Social Problems* 67 (May 2020): 197, 203, https://academic.oup.com/socpro/article-abstract/67/2/191/5481058?redirectedFrom=fulltext.

tool is not likely to be privy to this insider knowledge, heightening the risk that it will push these posts to law enforcement, who might then escalate police interaction with the teens.

VI. Conclusion and Recommendations (Q92)

The number of social media monitoring tools that appear to still be accessing Facebook, Instagram, and/or Twitter through developer APIs and providing user data to local law enforcement agencies is concerning in light of the number of social media users in the United States and the impacts of law enforcement surveillance. To their credit, Meta and Twitter have set out anti-surveillance policies that, if robustly enforced, would make significant progress towards mitigating and even eliminating these harms.[113] However, since the first news stories on the topic broke in 2016, there has been little public information about the implementation of these policies. The dearth of information stymies the development of clear and effective solutions and allows these tools to continue providing consumer data to local law enforcement agencies. It is thus critical to obtain more information from social media companies about the enforcement of their anti-surveillance policies and from consumers, advocates, and practitioners regarding the impact of social media surveillance.

Accordingly, given the prevalence and impact of this practice on consumers, we recommend the FTC undertake the following steps:

1. **Hold a listening forum with consumers, advocates, and practitioners to create a public record on the harm caused by local law enforcement use of social media monitoring tools to surveil and collect information from Facebook, Instagram, and Twitter users.**

The listening forum should address questions including:

- To the extent that Meta and Twitter have fallen short in adequately monitoring and enforcing their surveillance policies, what is the scope of the resulting harm?
    - Which consumers are most affected?
    - To what extent do social media monitoring tools magnify the impact of law enforcement surveillance?

[113] For example, Snaptrends was forced to freeze business operations and lay off all staff in November 2016 after Facebook removed its API feed access. Rosales, "Snaptrends Quietly Lays Off Entire Staff." Additionally, the 2016 crackdown by Meta and Twitter put police departments on notice. In 2019, LAPD wrote an email to Voyager expressing concerns about Voyager's monitoring capabilities after the Geofeedia "failure". [Redacted] to Scott McAndrews, Voyager Labs, "Re: Use Cases for Voyager – Meeting Next Week," September 18, 2019, 5:14 p.m., https://www.brennancenter.org/sites/default/files/2021-11/J2712-2713-%20Email%20re%20Trial%20Midpoint.pdf.

- What are consumer expectations regarding these surveillance policies, and do consumers understand the impact of policy violations? Do youth have a different expectation or understanding?

- What are the impacts of social media monitoring by local law enforcement agencies on communities of color?

2. **Host a workshop with subject matter experts, inviting independent experts and former Meta and Twitter employees to learn more about the use of platform and user data by third party social media monitoring tools, the platforms' interpretations of the reach of their anti-surveillance policies, and their efforts to enforce these policies.**

The workshop should address questions including:

- To what extent do local law enforcement agencies understand Meta and Twitter's policies and how the use of such tools interacts with these policies?

- What are Meta and Twitter doing to monitor and enforce their anti-surveillance policies? What issues are they facing in enforcing such policies? What additional measures are feasible?

- Why does Twitter not consider Dataminr's activities surveillance? What tools has Twitter punished for surveillance activities and how does that activity differ from Dataminr's?

- Should Meta and Twitter be required to include information about surveillance violators in transparency reports? What would this information include? For instance: How many data protection assessments have involved questions about use of user data for surveillance, how many investigations have been undertaken, and how many social media monitoring tools have been removed?

- Should Meta and Twitter be required to report annually to the FTC regarding the scope of surveillance on their platforms and the specific efforts they are undertaking to combat these practices?

Respectfully submitted this 21st day of November, 2022.

Rachel Levinson-Waldman, Managing Director
Ivey Dyson, Counsel
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue, NW, Ste. 1150
Washington, DC 20036

BRENNAN CENTER FOR JUSTICE

ANNEX

Question	Comment Section	Answer
1. Which practices do companies use to surveil consumers?	III(b)	• Meta and Twitter share publicly available data, including users' public posts, locations, events and more, with developers through Application Programming Interfaces. • Third-party social media tools sign up for this developer access and sell their product to state and local law enforcement. • While Meta and Twitter policies prohibit developers from using their access for surveillance or from sharing data with law enforcement, tools continue to do so.
3. Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?	IV	• It is unclear how robustly Meta and Twitter enforce their policies and it is unknown how common this practice is. • After the announcement of Meta's (new) and Twitter's (improved) surveillance policies in 2016, at least 6 tools that have contracts with local law enforcement confirmed their use of Facebook, Instagram, or Twitter.
4. How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?	IV, V	• Social media monitoring tools are likely to amplify the already recognized harms of online surveillance. • Social media monitoring tools have been used to target First Amendment activities. • Social media monitoring tools may be designed and used in ways that have a racially disproportionate impact.
5. Are there some harms that consumers may not easily discern or identify? Which are they?	V	• Consumers (i.e., Meta and Twitter users) will frequently be unable to discern these harms because social media surveillance is typically silent; if an individual does not become the subject of a specific police action or investigation, they may never know that their data was obtained and analyzed by these social media monitoring tools–along with millions of

		other innocent users–and shared with law enforcement.
13. The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?	V	• Social media monitoring tools do not screen for the ages of users whose information is shared with law enforcement. • Black and Hispanic youth are disproportionately characterized as engaging in gang-related activity, with social media posts and connections used by law enforcement as evidence. Social media monitoring tools, which do not have the ability to understand the nuance of teenagers' social media activity, may magnify this impact.
92. To what extent should the Commission, if at all, make regular self-reporting, third-party audits or assessments, or self-administered impact assessments about commercial surveillance practices a standing obligation? How frequently, if at all, should the Commission require companies to disclose such materials publicly? If it is not a standing obligation, what should trigger the publication of such materials?	VI	• The FTC should hold a listening forum with consumers, advocates, and practitioners to obtain more insight into, and create a public record about, the harm caused by local law enforcement's use of social media monitoring tools to surveil Facebook, Instagram, and/or Twitter users. • The FTC should host a workshop with subject matter experts, inviting independent experts and former Meta and Twitter employees to testify regarding the use of platform and user data by third party social media monitoring tools, the platforms' interpretations of the reach of their anti-surveillance policies, and their efforts to enforce those policies. • Together, these sessions should inform guidance from the FTC regarding platfoms' disclosures about violations and enforcement of their anti-surveillance policies, including incorporating this information into the platforms' regular transparency reports.