ACLU AMERICAN CIVIL LIBERTIES UNION FOUNDATION Northern California

BRENNAN CENTER FOR JUSTICE

ACLU

Dear Commissioners,

Social media companies have repeatedly promised, going back half a decade, that consumers' social media information will not be used for law enforcement surveillance. Despite those promises, developers of social media surveillance tools[1] still claim that they have access to data from Meta (formerly Facebook)[2] and/or X (formerly Twitter), and they sell their services, data, and products to law enforcement. Law enforcement at both the federal and local levels have recently purchased surveillance software from these vendors. Those developers' claims raise serious questions about whether Meta and X are complying with their binding commitments to protect user privacy.

The American Civil Liberties Union of Northern California ("ACLU NorCal"), the Brennan Center for Justice ("Brennan Center"), and the American Civil Liberties Union ("ACLU") submit this letter to request that the Federal Trade Commission seek further information from X and Meta to determine whether the companies' privacy commitments are being honored as the law requires.

Recent developments raise additional concerns about the capability of both Meta and X to meet their commitments to the FTC. Both X and Meta are undergoing challenges, reducing the size of their workforce, and considering whether changes to their business models are appropriate.[3] Some of those changes could implicate the promises made by the platforms

[1] For purposes of this letter, a "developer of social media surveillance tools" or a "surveillance vendor" is a private entity that collects user information from social media platforms, and sells that information, or inferences about it, to law enforcement agencies.

[2] This letter uses the corporate names used by the companies at the time the events described took place. That is, this letter uses "Facebook" before November of 2021 and "Meta" after and uses "Twitter" before July 2023 and "X" after. This letter also uses "Facebook" to refer specifically to the Facebook social-media product, particularly when it is important to distinguish it from Instagram, another Meta product.

[3] *See* Mike Isaac, *Facebook Renames Itself Meta*, N.Y. TIMES (Nov. 10, 2021), https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html; Katie Paul, *Facebook owner Meta slashes business teams in final round of layoffs*, REUTERS (May 24, 2023), https://www.reuters.com/technology/facebook-owner-meta-starts-final-round-layoffs-2023-05-24/; Shirin Ghaffary, *Mark Zuckerberg says the hardest part of Meta's "year of efficiency" is over*, Vox (May 25, 2023), https://www.vox.com/technology/2023/5/18/23729176/meta-silicon-valley-massive-layoffs-mark-zuckerberg; Alex Heath, *Elon Musk keeps laying off Twitter employees after saying cuts were done*, THE VERGE (Feb. 21, 2023), https://www.theverge.com/2023/2/21/23609522/elon-musk-more-twitter-layoffs-sales-engineering-ads-google-revamp; Kate Conger, et al., *In Latest Round of Job Cuts, Twitter Is Said to Lay Off at Least 200 Employees*, N.Y. TIMES (Feb. 26, 2023), https://www.nytimes.com/2023/02/26/technology/twitter-layoffs.html; Kat Tenbarge & Khadijah Khogeer, *Twitter's chaotic weekend ends with more questions than answers*, NBC NEWS (Jul. 3, 2023), https://www.nbcnews.com/tech/tech-news/twitter-changes-tweetdeck-rate-limit-rcna92369.

relating to law enforcement use of the platforms for surveillance.[4] Even as companies evolve, their promises to consumers must continue to be honored. And especially when companies are bound by existing consent orders—X and Meta have two consent orders apiece—it is of paramount importance that they keep their promises and maintain compliance with those orders.[5]

Technology, moreover, has developed significantly in recent years, with products touting "Artificial Intelligence" features that, according to the companies selling the products, can extract new patterns from enormous quantities of data and make predictions more accurate than ever before. While some of these claims are more hype than fact,[6] it is certainly true that new technology threatens to put people at risk, both when it works as advertised and when it fails to.[7] The recent emergence of new surveillance technology only heightens the importance of X and Meta keeping their promises to protect users from surveillance.

This letter offers a legal analysis, under Section 5 of the FTC Act, of X and Meta's public promises relating to law enforcement use of their platforms for surveillance as well as the apparent failure of those platforms to keep their promises. Because the true nature of the platforms' compliance with the law—or lack thereof—is known only by the platforms, an FTC investigation is necessary to determine whether the law, as well as the consent orders binding both companies, have been violated. In particular, this letter asks the FTC to investigate whether X and Meta have taken affirmative steps to facilitate surveillance vendors' access to user data, such as through APIs or other authorized access.[8]

The business practices of and claims by surveillance vendors detailed in this letter suggest that X and Meta have taken such affirmative steps. Although only one surveillance vendor

---

[4] X, for example, has moved to increase the cost of developer access to its tools, with some estimates putting the price of a "low-cost enterprise plan" at up to $42,000 per month. Jon Porter, *Twitter Announces New API Pricing, Posing a Challenge for Small Developers*, THE VERGE (2023), https://www.theverge.com/2023/3/30/23662832/twitter-api-tiers-free-bot-novelty-accounts-basic-enterprice-monthly-price.

[5] *See* Decision and Order, *In the Matter of Twitter Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf; Decision and Order, *In the Matter of Twitter Inc.*, FTC Docket No. C-4316 (May 26, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062C4316TwitterModifiedOrder.pdf; Decision and Order, *In the Matter of Facebook Inc.*, FTC Docket No. C-4365 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Order Modifying Prior Decision and Order, *In the Matter of Facebook Inc.*, FTC Docket No. C-4365 (Apr. 28, 2019), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf.

[6] *See, e.g.*, *Keep your AI claims in check*, FEDERAL TRADE COMMISSION (2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check.

[7] *See, e.g.*, Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[8] Application Programming Interfaces (API) give developers back-end access to publicly available information as well as the ability to query this data in real time. *See* Twitter Developer Platform, "Enterprise," https://developer.twitter.com/en/docs/twitter-api/enterprise; Twitter Developer Platform, "SearchAPI: Enterprise," https://developer.twitter.com/en/docs/twitter-api/enterprise/search-api/overview.

describes itself as having access to a special "firehose" of user data, the rest boast of such extensive data collection that it is reasonable to infer that they too have some privileged access to user data. We ask the FTC to investigate this possibility.

## I. Allowing surveillance vendors to have developer access on Meta and X is potentially a deceptive business practice that violates Section 5 of the FTC Act.

If there is one lesson from the FTC's decades of privacy-enforcement actions, it is this: companies must keep the privacy promises they make to consumers.[9] After stating clearly—and repeating often—that the special access granted by the platforms to developers would not be used for law enforcement surveillance, X and Meta are required to keep those commitments under the law.

Under Section 5 of the FTC Act, a deceptive practice includes: 1) a representation, omission, or practice that is 2) likely to mislead a consumer acting reasonably in the circumstances 3) with respect to a material fact.[10]

Privacy-related representations, along with conduct that is inconsistent with those representations, are at the core of the FTC's privacy-enforcement program. Indeed, of the 101 internet privacy enforcement cases filed by the FTC between 2008 and 2018, 89 cases were centrally concerned with a deception violation.[11] Recent years have seen no shortage of privacy deception enforcement. [12] As summarized below, X and Meta have made

---

[9] "Think your company doesn't make any privacy claims? Think again — and reread your privacy policy to make sure you're honoring the promises you've pledged. Consumers care about the privacy of their personal information and savvy businesses understand the importance of being clear about what you do with their data." *Privacy and Security Business Guidance*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/privacy-security. Among the numerous cases against companies for failing to keep their privacy promises are *In the matter of* Easy Healthcare Corp., FTC File No. 202 3186 (Jun. 26, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v, *In the matter of* 1Health.io Inc., FTC File No. 1923170 (Jun. 16, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923170-1healthiovitagene-matter, *In the matter of* BetterHelp Inc., FTC File No. 2023169 (Mar. 2, 2023) https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter, *In the matter of* Twitter Inc., File No. 2023063 (May 26, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads, *In the matter of* Facebook Inc., File Docket No. C-4365 (Apr. 28, 2020), https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter, *In the matter of* Uber Technologies Inc., Docket No. C-4662 (Oct. 26, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/152-3054-c-4662-uber-technologies-inc-matter.

[10] 15 U.S.C. § 45; FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) ("Deception Policy Statement").

[11] *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GOVERNMENT ACCOUNTABILITY OFFICE (2019), https://www.gao.gov/assets/700/696446.pdf at 44-52.

[12] For example, in a recent case against 1Health.io, the FTC found violations of Section 5(a) following a series of false or misleading statements made by the company about its privacy and data security practices. In another recent case against BetterHelp, the FTC proposed a $7.8 million penalty because the company revealed users' sensitive personal health information to third parties for advertising despite promising to keep this information private. Consent Order, *In the matter of* BetterHelp Inc., FTC File No. 2023169 (Mar. 2, 2023),

assurances to consumers that bear a strong resemblance to those in past cases investigated and settled by the FTC.

### A. X and Meta have made representations that user data on their platforms will not be used for law enforcement surveillance.

On numerous occasions since October 2016, X has reiterated its longstanding rule against developers' use of platform user data for law enforcement surveillance. Similarly, since March 2017, Meta has stated many times that law enforcement surveillance on its platform is prohibited, and Meta has publicized its policy in congressional hearings and to the press. Often, these representations have followed some revelation about the misuse of data—including by Geofeedia, SnapTrends, Crimson Hexagon, Dataminr, and the Los Angeles Police Department ("LAPD"). Meta's and X's policies are clear that data cannot be used for law enforcement surveillance, and both companies have ensured that press, government, law enforcement agencies, social media users, and the larger public are aware of those policies.

Some background is necessary. In 2015, members of the ACLU chapter in Fresno, California sounded the alarm on the Fresno Police Department's use of a social media surveillance tool called Beware, made by Intrado, a surveillance vendor.[13] In response, ACLU NorCal submitted a request for records from the Fresno Police Department under the California Public Records Act.[14] The records produced confirmed the use of Beware to monitor social media activity and generate "threat level scores" for individuals.[15] The records also revealed promotional materials from another social media surveillance vendor, Media Sonar, encouraging the monitoring of hashtags related to activism for racial justice

---

https://www.ftc.gov/system/files/ftc_gov/pdf/202_3169-betterhelp-consent.pdf. Similarly, in 2018, the FTC found that Uber had falsely assured consumers that internal access to their personal information would be closely monitored on an ongoing basis. Decision and Order, *In the matter of* Uber Technologies Inc., Docket No. C-4662 (Oct. 26, 2018), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_decision_and_order.pdf. Uber conveyed this promise to users by issuing a public statement in response to media controversy "concerning allegations of improper access and use of consumer personal information." *Id*. at [10] - [13].

[13] Corin Hoggard, *Fresno Police Scanning Social Media to Assess Threat*, ABC 30 (Feb. 19, 2015), https://abc30.com/fresno-police-social-media-big-brother-software/525999/; Matt Cagle, *This Surveillance Software Is Probably Spying on #BlackLivesMatter*, ACLU OF NORTHERN CALIFORNIA (Dec. 5, 2019), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter; Taymah Jahsi, *It's Time to Shine a Light on Police Surveillance in Fresno*, ACLU OF NORTHERN CALIFORNIA (Sep. 2, 2016), https://www.aclunc.org/blog/its-time-shine-light-police-surveillance-fresno.

[14] Letter from Matthew T. Cagle & Matthew W. Callahan, ACLU of Northern California, to Jerry Dyer, Fresno Police Department Chief of Police, "Public Records Act Request Regarding Social Media Monitoring Software" (Sep. 16, 2015), https://www.aclunc.org/docs/20150916-fresno_social_media_pra.pdf.

[15] Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU OF NORTHERN CALIFORNIA (Dec. 5, 2019), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter; ACLU OF NORTHERN CALIFORNIA, *Social Media Monitoring Software Public Records Act Response* (Dec. 2015), http://www.aclunc.org/docs/201512-social_media_monitoring_softare_pra_response.pdf.

and against police violence, such as "#blacklivesmatter," "#dontshoot," and "#imunarmed," to "help identify illegal activity and threats to public safety."[16]

The Fresno Police Department's social media surveillance was only the tip of the iceberg. Over the next year, pervasive surveillance of social media by law enforcement came to light, including the targeting of protestors and activists of color. From July to September 2016, the ACLU NorCal requested records related to social media surveillance tools from 63 police departments, sheriffs, and district attorneys.[17] Twenty agencies, or 40 percent of those who responded, had acquired social media surveillance tools.[18] Records produced included Geofeedia promotional materials referencing past "successes," including the monitoring of racial-justice protests in Ferguson, Missouri.[19]

These revelations raised grave concerns that social media companies—unbeknownst to their users—were enabling their platforms to be used for law enforcement surveillance purposes. Records included emails from representatives of the social-media monitoring platform Geofeedia referencing "partnerships" and legal arrangements with social media companies, including Twitter and Facebook, for special access to user information.[20] After the ACLU shared those findings in September 2016, Facebook, Instagram, and Twitter immediately ended their data relationships with Geofeedia.[21]

One week after its suspension of Geofeedia, Twitter severed ties with another firm specializing in social media surveillance: Austin, Texas-based startup Snaptrends.[22] Snaptrends—like Geofeedia—incorporated the use of undercover accounts, a feature that enabled police and federal law enforcement to bypass Facebook's privacy options. According to a letter obtained by the *Austin Chronicle* in February 2015, Snaptrends made

---

[16] *Id.*

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

[18] *Id.*

[19] *Id.*

[20] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU OF NORTHERN CALIFORNIA (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[21] *Id; see also,* Lora Kolodny, *Facebook, Twitter Cut Off Data Access for Geofeedia, A Social Media Surveillance Startup,* TECHCRUNCH (Oct. 11, 2016), https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/.

[22] Dell Cameron, *Twitter Cuts Ties with Second Firm Police Use to Spy on Social Media*, DAILY DOT (Oct. 20, 2016), https://www.dailydot.com/irl/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/.

use of "advanced algorithms and processes" to procure a "high density social data footprint" and sold its platform to law enforcement agencies.[23]

In October 2016, the ACLU of California, the Center for Media Justice, and Color of Change sent letters to Twitter and Facebook urging the companies to prohibit access for developers of law enforcement surveillance tools, to develop clear and transparent policies outlining such prohibitions, and to establish auditing mechanisms to identify violations.[24] The ACLU's report was covered by the *New York Times* and *Washington Post* —with their combined millions of readers—in articles highlighting how partnerships between social media companies and developers of surveillance tools were being used for law enforcement surveillance of protestors and activists.[25] Numerous other media outlets covered the story as well, revealing to many millions of social media users across the country that their social media data was being used for surveillance by law enforcement.[26]

Twitter responded six weeks later, in November 2016, clarifying in an official blog post that they "prohibit developers using the Public APIs and Gnip data products from allowing law

---

[23] John Anderson, *APD Tracks Social Media: Local social media monitoring software company met with shady digital spying group*, AUSTIN CHRONICLE (Sep. 4, 2014), https://www.austinchronicle.com/news/2015-09-04/apd-tracks-social-media/.

[24] Letter from Nicole A. Ozer & Peter Bibring, ACLU of California, Malkia Cyril, The Center for Media Justice, and Brandi Collins, Color of Change, to Twitter (Oct. 10, 2016), https://www.aclunc.org/sites/default/files/20161010_ACLU_CMJ_Color_of_Change_Joint_letter_Twitter.pdf; Letter from Nicole A Ozer & Peter Bibring, ACLU of California, Malkia Cyril, The Center for Media Justice, and Brandi Collins, Color of Change, to Meta and Instagram (Oct. 10, 2016), https://www.aclunc.org/sites/default/files/20161010_ACLU_CMJ_Color_of_Change_Joint_letter_Facebook_Instagram.pdf.

[25] *See* Jonah Engel Bromwich, Daniel Victor & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html; Craig Timberg & Elizabeth Dwoskin, *Facebook, Twitter and Instagram Sent Feeds That Helped Police Track Minorities in Ferguson and Baltimore, Report Says,* WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/.

[26] *See, e.g.,* Kristina Cooke, *U.S. Police Used Facebook, Twitter Data to Track Protestors - ACLU*, REUTERS (Oct. 11, 2016), https://www.reuters.com/article/social-media-data/u-s-police-used-facebook-twitter-data-to-track-protesters-aclu-idUSL4N1CH4J1; Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016), https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api; Sam Levin, *ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protestors*, THE GUARDIAN (Oct. 11, 2016), https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter; Steven Musil & Terry Collins, *Facebook, Twitter Accused of Providing User Data for Police Surveillance*, CNET (Oct. 11, 2016), https://www.cnet.com/tech/services-and-software/facebook-twitter-user-data-police-surveillance-aclu/; Queenie Wong, *ACLU: Facebook, Twitter and Instagram Aided Police Surveillance of Protestors*, MERCURY NEWS (Oct. 11, 2016), https://www.mercurynews.com/2016/10/11/aclu-facebook-twitter-and-instagram-aided-police-surveillance-of-protesters/; Tanasia Kenney, *ACLU Blasts Facebook, Twitter and Instagram for Helping Police Track Black Activists Using Social Media Surveillance Product*, ATLANTA BLACK STAR (Oct. 12, 2016), https://atlantablackstar.com/2016/10/12/aclu-blasts-facebook-twitter-and-instagram-for-helping-police-track-black-activists-using-social-media-surveillance-product/.

enforcement—or any other entity—to use Twitter data for surveillance purposes."[27] Twitter stated that "[r]ecent reports about Twitter data being used for surveillance" had caused the company "great concern."[28] In its announcement, Twitter indicated there would be "expanded enforcement and compliance efforts" over the coming months and committed to taking "appropriate action," including termination and suspension for violators.[29]

Facebook followed suit four months later, noting that their "approach involves making careful decisions."[30] The update also stated that the company was "grateful for community leaders" like the ACLU, Color of Change, and the Center for Media Justice who "worked with [Facebook] for the past several months on this update."[31] In March 2017, Facebook announced an update to their platform policies banning the use of data obtained from Facebook "to provide tools that are used for surveillance."[32] The policies specify that "[s]urveillance includes the Processing of Platform Data about people, groups, or events for law enforcement or national security purposes."[33] Facebook emphasized that the goal of the update was to "make our policy explicit."[34]

Facebook and Twitter's new "bans" were covered extensively in the media, providing users with a clear promise that their social media activity would not be used for law enforcement surveillance purposes.[35] And in the years since those promises were initially made, X and

---

[27] Chris Moody, *Developer Policies to Protect People's Voices on Twitter*, TWITTER DEV. PLATFORM BLOG (Nov. 22, 2016), https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter. 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 Enterprise*, TWITTER DEV. PLATFORM, https://developer.twitter.com/en/docs/twitter-api/enterprise; *SearchAPI: Enterprise*, TWITTER DEV. PLATFORM, https://developer.twitter.com/en/docs/twitter-api/enterprise/search-api/overview.

[28] *Id.*

[29] *Id.*

[30] Post by Rob Sherman, FACEBOOK PUB. AFFS. (Mar. 13, 2017), https://www.facebook.com/fbpublicaffairs/posts/1617594498258356.

[31] *Id.*

[32] *Id.*

[33] *Meta Platform Terms*, META, https://developers.facebook.com/terms/.

[34] Post by Rob Sherman, FACEBOOK PUB. AFFS. (Mar. 13, 2017), https://www.facebook.com/fbpublicaffairs/posts/1617594498258356.

[35] *See, e.g.,* Lily Hay Newman, *Facebook's Big 'First Step' to Crack Down on Surveillance*, WIRED (Mar. 17, 2017), https://www.wired.com/2017/03/facebooks-big-first-step-crack-surveillance/; Elizabeth Dwoskin, *Facebook Says Police Can't Use Its Data for 'Surveillance'*, WASH. POST (Mar. 13, 2017), https://www.washingtonpost.com/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*, THE GUARDIAN (Mar. 13, 2017), https://www.theguardian.com/technology/2017/mar/13/facebook-instagram-surveillance-privacy-data; Marty Swant, *Facebook Is Banning Developers from Using Its Data to Build Surveillance Tools*, ADWEEK (Mar. 13, 2017), https://www.adweek.com/performance-marketing/facebook-is-banning-developers-from-using-its-data-to-build-surveillance-tools/; Matt Rocheleau, *The FBI Just Got Access to Twitter Data. Should You Be*

Meta have repeated and reinforced those promises. **Appendix A** to this letter includes a more comprehensive account of the public statements assuring users that their social media information would not be used for law enforcement surveillance.

**B. Given the apparent prevalence of social media surveillance tools using data from X and Meta, those representations are likely to mislead reasonable consumers.**

Consumers who see the representations made by Meta and X in the numerous blog posts, social media posts, and press coverage would understand that the platforms do not allow developers to utilize their information for use in law enforcement surveillance.

Those consumers are likely to be misled because, in the years since Meta and X's actions, evidence has mounted that social media surveillance tools still have special access to information about Meta and X's users and sell or license that information to law enforcement.

Public records revealed by the Brennan Center—as well as other sources—show that as of November 2022, at least eleven social media surveillance tools still appeared to have special access to Facebook, Instagram, and/or X and have contracts with law enforcement, even after the implementation of Meta and X's anti-surveillance policies in 2016.[36] With a user

*Concerned?*, BOS. GLOBE (Nov. 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 ("Twitter has recently blocked law enforcement agencies from using its data for surveillance and publicly emphasized its ban on the practice."); Rishabh Jain, *Twitter CEO's Account Temporarily Suspended*, YAHOO! (Nov. 23, 2016), https://ca.finance.yahoo.com/news/twitter-ceo-account-temporarily-suspended-064508676.html ("The company also issued new developer policies Tuesday prohibiting surveillance using the social network."); *see also* Colin Lecher, *Facebook Updates Its Platform Policy to Forbid Using Data for Surveillance*, THE VERGE (Mar. 13, 2017), https://www.theverge.com/2017/3/13/14909248/facebook-platform-surveillance-policy-developers-data; Selena Larson, *Facebook Updates Policies to Prohibit Surveillance*, CNN (Mar. 13, 2017), https://money.cnn.com/2017/03/13/technology/facebook-surveillance-ban/index.html; Michelle Meyers, *Facebook Bans Use of Its Data for Surveillance Tools,* CNET (Mar. 13, 2017), https://www.cnet.com/tech/services-and-software/facebook-bans-developers-data-surveillance-tools-aclu/; Deepa Seetharaman, *Facebook Bans Use of User Data for Surveillance*, WALL ST. J. (Mar. 13, 2017), https://www.wsj.com/articles/facebook-bans-use-of-user-data-for-surveillance-1489433901.

[36] These tools are EDGE NPD's ABTShield, Babel Street's BabelX, SocioSpyder's Cobwebs, Dataminr, LookingGlass Cyber Solutions, Media Sonar, NC4, ShadowDragon's SocialNet and OIMonitor, Skopenow, TransUnion's TLOxp, and several tools from Voyager. *See Data from the LAPD's Trial of ABTShield*, BRENNAN CENTER FOR JUSTICE (Dec. 15, 2021), https://www.brennancenter.org/our-work/research-reports/data-lapds-trial-abtshield (revealing that ABTShield sent the LAPD around 70,000 tweets per day during a 2020 pilot); Mike Dvilyanski, David Agranovich, & Nathaniel Gleicher, *Threat Report on the Surveillance-for-Hire Industry*, META, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf (showing that, in December 2021, Meta removed about 200 Cobwebs accounts in 2021 stating that Cobwebs enabled reconnaissance of information from Facebook, Instagram, and Twitter and that information was used for law enforcement activities.); Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests*, THE INTERCEPT (Apr. 29, 2019), https://theintercept.com/2019/04/29/family-separation-protests-surveillance/; Rachel Levinson-Waldman, *Documents Show LAPD Monitoring of Community Meeting on…LAPD Social Media Monitoring*, BRENNAN CENTER FOR JUSTICE (Sep. 9, 2022), https://www.brennancenter.org/our-work/analysis-opinion/documents-show-

base for the three platforms totaling a significant portion of the population of the United States, the potential impact of these tools is substantial.[37]

Local police departments across the country use social media surveillance tools frequently,[38] but federal law enforcement and security agencies may be the biggest purchasers of social media surveillance tools, and research indicates that the surveillance products they use collect data from Meta and X. The agencies using this tech span much of the federal government, with the most prominent being the Department of Homeland Security (DHS) and its component agencies, Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).[39]

The following five surveillance vendors access Meta and X data and sell that information, or inferences about it, to law enforcement agencies: ShadowDragon, Dataminr, Babel Street, Skopenow, and Media Sonar. This letter addresses each in turn.

1. *ShadowDragon collects X and Meta data and sell it to law enforcement for surveillance purposes.*

ShadowDragon is a surveillance company that claims to provide its customers with access to "an ever-expanding network of 200+ sources including social media," using a "global network of collectors to constantly pull in the latest in live data from across the Internet."[40] Its flagship product, SocialNet, analyzes ShadowDragon's vast cache of data to uncover

---

lapd-monitoring-community-meeting-lapd-social-media; Brennan Center for Justice, *C Series and May 20, 2023 Supplemental Production, – DC MPD Social Media Monitoring FOIA*, https://www.brennancenter.org/sites/default/files/2023-10/Pages%20from%20Series%20C%20Sept%202022.pdf, https://www.brennancenter.org/sites/default/files/2023-10/May%2030%2C%202023%20Supplemental%20Production%2C%20Bates%20497-99.pdf (showing that TLOxp used Facebook, Instagram, and Twitter data in 2019 and MPD had TLOxp access as of June 2022). For Babel Street, Dataminr, Media Sonar, Shadowdragon, Skopenow, and Voyager, see Section I(B).

[37] As of July 2022, the United States had 182.3 million Facebook users, 153.6 million active Instagram users, and 83.4 million X users. *See Facebook Statistics and Trends*, DATAREPORTAL (2022), https://datareportal.com/essential-facebook-stats; *Instagram Statistics and Trends*, DATAREPORTAL (2022), https://datareportal.com/essential-instagram-stats; *Twitter statistics and Trends*, DATAREPORTAL (2022), https://datareportal.com/essential-twitter-stats. Because it is unclear whether Meta or X 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.

[38] Comments to the Federal Trade Commission re: Commercial Surveillance ANPR, R111004, BRENNAN CENTER FOR JUSTICE (Nov. 21, 2022), https://www.brennancenter.org/our-work/research-reports/comments-submitted-federal-trade-commission-social-media-monitoring.

[39] DHS and its component agencies, CBP and ICE, are probably the agencies most frequently covered for their social media monitoring. However, agencies unrelated to law enforcement or security also engage in the same type of monitoring. "Many federal agencies use social media, including the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Department of State (State Department), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Postal Service (USPS), Internal Revenue Service (IRS), U.S. Marshals Service, and Social Security Administration (SSA)." https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

[40] *Data: More Than 200 Unique Sources and Datasets*, SHADOWDRAGON, https://shadowdragon.io/data/.

details about individuals' online presence and associations, allowing users to "[d]iscover and visualize networks of bad actors."[41] OIMonitor, another of ShadowDragon's products, is an "online monitoring tool that collects … data from" across the Internet according to users' customized search parameters, "creating an automated gathering process that returns customer-specific threat data."[42] While ShadowDragon has stated that the company uses "crawlers that scrape information from public websites," the scope of ShadowDragon's collection raises concerns it may also have developer access to X and Meta's user data.

At least three law enforcement agencies have purchased licenses for ShadowDragon's products: the Massachusetts State Police, the Michigan State Police, and ICE.[43] The Brennan Center obtained two contracts from ICE's law enforcement and investigative arm, Homeland Security Investigations (HSI), revealing that HSI purchased licenses for SocialNet in July 2020 and August 2021.[44] According to one procurement document, "ShadowDragon['s] SocialNet tool offers access to both" Meta and X.[45] HSI also purchased licenses for OIMonitor, stating that the tool would enhance the division's capabilities "for both cyber or physical criminal investigations and social media forensics."[46]

The Brennan Center also obtained several documents that compile ShadowDragon's findings for HSI agents' queries, demonstrating that ShadowDragon collects information about individuals' X, Facebook, and Instagram profiles, as well as users' Facebook and

---

[41] *SocialNet: Social Media Investigation Tool*, SHADOWDRAGON, https://shadowdragon.io/socialnet/.

[42] Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations Office of Intelligence (Intel), *Statement of Need for Shadow Dragon OI Monitor* [sic] at 1, https://www.brennancenter.org/sites/default/files/2023-10/HSI%20Statement%20of%20Need%20for%20OIMonitor%20ShadowDragon.pdf.

[43] Ryan Kath & Jim Haddadin, *ShadowDragon: Mass. Police Get New Social Media Monitoring Tool*, NBC10 BOSTON (updated Jul. 13, 2021), https://www.nbcboston.com/investigations/shadowdragon-mass-police-get-new-social-media-monitoring-tool/2424128/; Michael Kwet, *ShadowDragon: Inside the Social Media Surveillance Software that Can Watch Your Every Move*, THE INTERCEPT (Sep. 21, 2021), https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware/. According to claims made by ShadowDragon's founder, the FBI has evaluated SocialNet. *Id.*

[44] Contract between U.S. Immigration and Customs Enforcement (hereinafter ICE) and C&C International Computers and Consultants, Inc. (Jul. 16, 2020), https://www.brennancenter.org/sites/default/files/2023-10/HSI%20SocialNet%20July%202020%20Contract.pdf; Contract between ICE and Panamerica Computers, Inc. (Aug. 30, 2021), https://www.brennancenter.org/sites/default/files/2023-10/HSI%20SocialNet%20August%202021%20Contract.pdf. For further information about the documents obtained by the Brennan Center, *see Brennan Center Files Freedom of Information Act Requests for Information on DHS's Use of Social Media Monitoring Tools*, BRENNAN CENTER FOR JUSTICE (last updated Dec. 12, 2023), https://www.brennancenter.org/our-work/research-reports/brennan-center-files-freedom-information-act-requests-information-dhss.

[45] ICE, *ShadowDragon Justification for Exception to Fair Opportunity* at 2, https://www.brennancenter.org/sites/default/files/2023-10/ICE%20ShadowDragon%20Justification%20for%20Exception%20to%20Fair%20Opp..pdf.

[46] Contract between ICE and Software Information Resource Corporation (Jun. 28, 2021), https://www.brennancenter.org/sites/default/files/2023-10/HSI%20Contract%20for%20OIMonitor%20ShadowDragon_0.pdf; Statement of Need, *supra* note 42 at 1.

Instagram postings, and produces the data to its customers.[47] It is unclear whether these queries were conducted on SocialNet or OIMonitor.

*2. Dataminr collects X and Meta data and sells it to law enforcement for surveillance purposes.*

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 posts made on a given day.[48] 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.[49] Dataminr touts that its alerts can surface breaking news stories before any news source reports on it.[50] The company has access to social media platforms like X and Meta, and—as an official X partner—has special access to X's "firehose," allowing it to scan every public tweet.[51]

Documents obtained by the Brennan Center show that the Washington D.C. Metropolitan Police Department (MPD) conducted a trial of Dataminr in January 2017.[52] Following this trial, the Director of the MPD's Joint Strategic & Tactical Analysis Command Center put in a purchase request for the tool,[53] and the MPD entered into a $47,950 contract with the

---

[47] *Brennan Center Files Freedom of Information Act Requests for Information on DHS's Use of Social Media Monitoring Tools*, BRENNAN CENTER FOR JUSTICE (2022), https://www.brennancenter.org/our-work/research-reports/brennan-center-files-freedom-information-act-requests-information-dhss. **X**: June 10, 2021, ShadowDragon report at 14, 28–29; June 24, 2021, ShadowDragon report at 19. **Facebook**: June 24, 2021, ShadowDragon report at 20, 25, 42–43, 47–48; May 21, 2021, ShadowDragon report at 6–7, 9–29, 40–46, 57–205, 212–229, 233–239. **Instagram**: June 24, 2021, ShadowDragon report at 26–29, 33, 39–40; August 11, 2021, ShadowDragon report at 10–35, 40–41, 64–69, 72–76.

[48] Dataminr, *Price Quote for Los Angeles Police Department (LAPD)*, https://www.brennancenter.org/sites/default/files/2021-09/H4-6_Dataminr.pdf; and *Dataminr's Real-time AI Platform*, DATAMINR, http://dataminr.com/technology. Insiders have suggested, however, that individual Dataminr employees have, in the past, been the ones to mine through social media posts. Sam Biddle, *Twitter Surveillance Startup Targets Communities of Color for Police*, THE INTERCEPT (Oct. 21, 2020), https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/.

[49] Lexis-Olivier Ray, *Official Emails Show That LAPD Worked with a Controversial Social Media Surveillance Company during George Floyd Protests*, L.A. TACO (Sep. 3, 2021), https://lataco.com/lapd-social-media-surveillance-protest.

[50] Dataminr, *Price Quote for LAPD*, https://www.brennancenter.org/sites/default/files/2021-09/H4-6_Dataminr.pdf.

[51] *Dataminr*, TWITTER PARTNERS, https://partners.twitter.com/en/partners/dataminr; and Sam Biddle, *U.S. Marshals Spied on Abortion Protesters Using Dataminr*, THE INTERCEPT (May 15, 2023), https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/.

[52] [Redacted], Metropolitan Police Department (hereinafter MPD), to Robert Butler et al., RE: Evaluation Criteria for Dataminr Test (Jan. 25, 2017), https://www.brennancenter.org/sites/default/files/2022-11/DC%20MPD%20Production%20Series%20C%20pp%20432-434%20437-438%20472-473.pdf.

[53] Lee Wight, director, Joint Strategic and Tactical Analysis Command Center, MPD, to [Redacted], MPD, (Mar. 9, 2017, 8:09 p.m.), https://www.brennancenter.org/sites/default/files/2022-11/DC%20MPD%20Production%20Series%20C%20pp%20828-829.pdf.

company in 2018.[54] In 2019, Dataminr stated that its law enforcement customers included the NYPD, the Chicago Police Department, and Louisiana State Police.[55] And the LAPD's Situational Awareness Watch unit conducted a trial of the First Alert product the same year.[56]

Most recently, Dataminr leveraged its privileged X "firehose" access to send alerts to the U.S. Marshals Service about the precise time and location of pro-choice protests and rallies soon after the reversal of *Roe v. Wade*.[57] 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.[58] It is unclear what other local law enforcement entities received information from Dataminr. But documents show that Dataminr tracked ongoing protests in Brooklyn, New York; Detroit, Michigan; York, Pennsylvania; and Hampton Roads, Virginia.[59] And other documents reveal Dataminr's wide-ranging network of law enforcement partnerships across the country.[60] For example, the Drug Enforcement Administration signed a contract with Dataminr in February of 2023,[61] and the Department of Defense has an ongoing contract with Dataminr that commenced in 2020.[62] X has taken the position that Dataminr is not in violation of any

---

[54] This information was found through GovSpend, a subscription-only online database containing local, state, and federal contracts information. *See About Us*, GOVSPEND, https://govspend.com/about/. Records are on file with the Brennan Center.

[55] Sam Biddle, *Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr*, THE INTERCEPT (Jul. 9, 2020), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

[56] Andrew Johnston to Jeffrey Brugger, *Re: Dataminr for LAPD: Trial Conclusion - Friday, August 16th* (Aug. 20, 2019, 2:41 p.m.), https://www.brennancenter.org/sites/default/files/2021-09/H.%20Dataminr%20Trial%202019.pdf.

[57] Biddle, *U.S. Marshals Spied on Abortion Protesters Using Dataminr*, https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/.

[58] Biddle, *Police Surveilled George Floyd Protests*, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-blacklives-matter-protests/.

[59] *Id.*

[60] 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 a 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.

[61] *See entries under* "List Of Contract Actions Matching Your Criteria" Heading on the following page: https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=15DDHQ23P00000174+1524.

[62] *Contracts For April 23, 2020*, DEPARTMENT OF DEFENSE, https://www.defense.gov/News/Contracts/Contract/Article/2162978/ ("Dataminr Inc., New York, New

policies despite the platform's ban on law enforcement surveillance, and thus has apparently never limited its access.[63]

*3. Babel Street collects X and Meta data and sells it to law enforcement for surveillance purposes.*

Babel Street markets itself as providing an "advanced data analytics and intelligence platform for the world's most trusted government and commercial organizations."[64] The company's main product, once apparently called "Babel X" and now called the "Babel Street Insights Platform," is described as putting "[Publicly Available Information] at your fingertips to gain faster insight with enriched data on location, language, sentiment, intent, topics, and more through an intuitive web application."[65] It states it collects and analyzes data from "millions of . . . data sources in hundreds of languages,"[66] then returns "real-time, actionable information" and alerts to end users—which includes law enforcement—through its web platform.[67]

Babel Street claims to leverage data from across the "data universe," which includes "publicly available information" (PAI) and "proprietary datasets."[68] According to Babel Street, PAI includes content from social media platforms (notably including Meta's Instagram), public government records, IP addresses, commercial data, and data from the "deep" and "dark" web.[69] Babel Street's marketing Fact Sheet claims their tool searches across 30+ social media sites.[70] Babel Street has pitched their product to both the Los

---

York, has been awarded a firm-fixed-price contract for $258,661,096 for a commercially available license subscription . . .").

[63] Sam Biddle, *Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr*, THE INTERCEPT (Jul. 9, 2020), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/; *see also* Jeff Horwitz & Parmy Olson, *Twitter Partner's Alerts Highlight Divide Over Surveillance*, WALL ST. J. (Sep. 29, 2020), https://www.wsj.com/articles/twitter-partners-alerts-highlight-divide-over-surveillance-11601417319.

[64] *About Us*, BABEL STREET, https://www.babelstreet.com/about-us.

[65] *Babel X*, BABEL STREET, https://www.babelstreet.com/platform.

[66] *Id.*

[67] Brennan Center for Justice, *F Series - LAPD Social Media Monitoring FOIA [hereinafter F Series]*, https://www.scribd.com/document/523036097/F-Series-LAPD-Social-Media-Monitoring-FOIA-2021 at 1.

[68] *F Series*, https://www.scribd.com/document/523036097/F-Series-LAPD-Social-Media-Monitoring-FOIA-2021.

[69] McDaniel Wicker, *Publicly Available* Information *Explained*, BABEL STREET, https://www.babelstreet.com/blog/pai-explained.

[70] *F Series*, https://www.scribd.com/document/523036097/F-Series-LAPD-Social-Media-Monitoring-FOIA-2021 at 1.

Angeles Police Department and Seattle Police Department.[71] DHS,[72] the Federal Bureau of Investigation ("FBI"),[73] Justice Department,[74] and US Military Operations Command[75] are all reported previous or current customers of Babel Street. In May of 2023, Vice reported that CBP was using Babel X to analyze the social media of U.S. citizens and refugees, including linking their posts to Social Security numbers and their location information.[76]

Babel Street likely uses data from Meta and X. Babel Street boasts of its ability to perform "social media threat monitoring" on behalf of government entities.[77] As Babel Street states: "To monitor social media, the Babel Street Insights platform provides AI-enabled searches across all layers of the internet, including the deep and dark web. It scours dozens of social media sites worldwide, along with millions of message boards, online comments, and publicly available chats."[78] Although Babel Street claims to utilize "publicly available information," it is not clear if the scope of their data collection would be possible without developer access to X and Meta's user data or similar permissions.

In December of 2021, the FBI published a contract opportunity to find a vendor offering a "commercial off-the-shelf software that provides social media exploitation."[79] The FBI sought a tool that would provide "the ability to search against relevant social media sources where threat activity occurs," with additional requirements of "data aggregation that leads

---

[71] *F Series*, https://www.scribd.com/document/523036097/F-Series-LAPD-Social-Media-Monitoring-FOIA-2021 at 25; Curtis Waltman, *Meet Babel Street, the Powerful Social Media Surveillance Used by Police, Secret Service, and Sports Stadiums*, VICE (Apr. 17, 2017), https://www.vice.com/en/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums.

[72] Aaron Gregg, *For this company, online surveillance leads to profit in Washington's suburbs*, WASH. POST (Sep. 10, 2017), https://www.washingtonpost.com/business/economy/for-this-company-online-surveillance-leads-to-profit-in-washingtons-suburbs/2017/09/08/6067c924-9409-11e7-89fa-bb822a46da5b_story.html.

[73] *Id.*

[74] *Babel Street Partners to Win $500 Million Data Analytics Solutions and Services BPA at DOJ*, GLOBENEWSWIRE (Oct. 24, 2019), https://www.globenewswire.com/en/news-release/2019/10/24/1935086/0/en/Babel-Street-Partners-to-Win-500-Million-Data-Analytics-Solutions-and-Services-BPA-at-DOJ.html.

[75] Waltman, *Meet Babel Street, the Powerful Social Media Surveillance Used by Police, Secret Service, and Sports Stadiums*, https://www.vice.com/en/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums.

[76] Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, VICE (May 17, 2023), https://www.vice.com/en/article/m7bge3/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees.

[77] *Social Media Threat Monitoring Boosts National Security*, BABEL STREET, https://www.babelstreet.com/blog/social-media-threat-monitoring-improves-national-security.

[78] *Id.*

[79] *Request for Proposals - Social Media Exploitation - Amendment 2*, SAM.GOV, https://sam.gov/opp/63867a4d178d4717ac246d61c955cc05/view.

to social network analysis, geospatial mapping, and image analytics."[80] The tool specified by the FBI was required to be able to "identify persons of interest" and "their associates on social media," run keyword searches, and have geofencing capabilities.[81] The FBI further stated that searching across specific social media platforms was necessary: "The tool shall be able to gather information from the following *mandatory* online and social media data sources: Twitter, Facebook, Instagram, YouTube, LinkedIn, Deep/Dark Web, VK, and Telegram."[82] Other social media platforms were preferred but not required: "Snapchat, TikTok. Reddit, 8Kun, Gab, Parler, ask.fm, Weibo, Discord, additional fringe platforms, and other encrypted messaging platforms."[83] In March of 2022, the FBI finalized the contract with a $27 million purchase of 5,000 licenses of Babel X.[84]

*4. Skopenow collects X and Meta data and sells it to law enforcement for surveillance purposes.*

Skopenow is a surveillance technology company that contracts with local and federal law enforcement entities. Skopenow claims that its tools have the capacity to automatically find, extract, and analyze information from social media; conduct behavioral recognition analysis based on image and text processing;[85] provide subject monitoring and comprehensive search results; notify users via automated alerts when there are developments in a subject they are tracking; and create interactive visualizations by merging location information from consumer reports, social media posts, and metadata.[86]

Skopenow advertises services to law enforcement, government, human-resources entities, insurance companies, and any consumer who wants to find and reconnect with family, classmates, and colleagues.[87] To that end, Skopenow publicly claims to have access to all major social media platforms, court records through databases such as PACER, consumer records, phone numbers, usernames, email addresses, publicly available records, and any information available online.[88]

---

[80] *FBI Attachment B – Statement of Work Amendment 2*, 2 SAM.GOV, https://sam.gov/api/prod/opps/v3/opportunities/resources/files/80522f7489b047949b5f8d9a0a00400f/download?&status=archived&token=.

[81] *Id.* at 2–3.

[82] *Id.* at 3 (emphasis added).

[83] *Id.* at 2, 3.

[84] *Social Media Exploitation*, SAM.GOV, https://sam.gov/opp/3175f72a55e54307b8c46d24ae10ff35/view.

[85] Email re Skopenow Behavioral Recognition, https://www.brennancenter.org/sites/default/files/2021-09/Skopenow%20Behavioral%20Analysis.pdf ("Skopenow is a search engine that automates the investigation process by providing comprehensive digital records that include behavior recognition through image and text analysis, subject monitoring, and comprehensive search results.").

[86] *Homepage*, SKOPENOW, https://www.skopenow.com/.

[87] Rachele' Davis, *An Investigator's Review of Skopenow*, NEW HOPE INVESTIGATIONS (Aug. 21, 2017), https://newhopeinvestigations.com/blog/a-private-investigators-a-review-of-skopenow/2017/8/17 (as of November 6, 2023 this page appears to be offline but an archive copy is on file with the authors).

[88] *Homepage*, SKOPENOW, https://www.skopenow.com/ (archive copy is on file with the authors).

Skopenow is also advertised as a tool that enables its users to "find hidden links between individuals" via its ability to "instantly and anonymously locate and archive" social media information, "location-history, and actionable behavior flags."[89] By furnishing associational data such as activity between two or more searched people along with links related to social media posts, Skopenow "can verify if two individuals share any commonalities within their digital reports, including social media connections, comments or tags within the same content, shared vehicles, and shared personal details, such as relatives, locations, and contact details . . . Mutual friends, work histories, and geolocation specific information are discovered and visualized."[90] Going back to 2018, Skopenow has touted its access to Meta and X data in sample reports that include links to users' profiles, posts, and IP addresses.[91] And according to Skopenow's website, Skopenow captures profiles, posts, comments, connections, and metadata."[92] As with other surveillance vendors, the scope of Skopenow's data collection raises the question of whether it is accessing this data through special arrangements with X and Meta.

These features are used by numerous law enforcement entities. In addition to the LAPD, which conducted a demo series with Skopenow in June 2019[93] and held multiple trial accounts between November 2018 and July 2020,[94] Skopenow boasts many other public-sector clients. According to correspondence between the LAPD and a Skopenow representative, the company's public-sector clients include local entities such as the governments of Broward and Martin Counties, FL as well as the Morristown, NJ Police Department.[95] Skopenow touts the product's ability to assist in criminal investigations by identifying gang affiliations and stalking.[96]

---

[89] *OSINT webinar on Instant-Messaging Apps* at 51:20. *Instant Messaging Apps & OSINT Investigations* https://www.skopenow.com/skopenow-osint-webinars/instant-messaging-apps-osint-investigations at 51:20.

[90] *Automated Open Source Intelligence*, SKOPENOW, https://www.skopenow.com/lawenforcement (archive copy is on file with the authors).

[91] *Social Media and Online Investigative Report*, SKOPENOW, 10–14 (Jul. 7, 2018) (providing IP address and date for particular Facebook users), https://www.fbcinc.com/source/virtualhall_images/IRS_Tech_Expo_-_August/Skopneo/Sample_Report.pdf.

[92] *Automated Open Source Intelligence*, SKOPENOW, https://www.skopenow.com/lawenforcement (archive copy is on file with the authors).

[93] Skopenow Demo, *E-Series - LAPD Social Media Monitoring FOIA [hereinafter E-Series]*, BRENNAN CENTER FOR JUSTICE (Dec. 15, 2021), https://www.brennancenter.org/sites/default/files/2021-09/E.%20Skopenow%20Demo%20June%202019.pdf.

[94] *See Multiple Skopenow Trials*, E-Series, at https://www.brennancenter.org/sites/default/files/2021-09/E.%20Multiple%20Skopenow%20Trials.pdf.

[95] *See Skopenow Public Sector Clients*, E-Series, at https://www.brennancenter.org/sites/default/files/2021-09/Skopenow%20public%20sector%20clients.pdf.

[96] *Automated Open Source Intelligence*, SKOPENOW, https://www.skopenow.com/lawenforcement (archive copy is on file with the authors).

*5. Media Sonar collects X data and sells it to law enforcement for surveillance purposes.*

Media Sonar is a surveillance company that collects many sources of information and makes those sources available to law enforcement in a single consolidated tool. Media Sonar's presentation to LAPD describes the sources of information available to law enforcement as "Surface Web," "Deep Web," and "Dark Web."[97] The "Surface Web" includes "public profiles"; notably, both X and Meta force people to make certain profile information visible to the public.[98]

According to its advertising, Media Sonar leverages profile information to connect disparate accounts and other information to build a "full digital snapshot of an individual's online presence including all related personas and connections." Media Sonar's presentation also suggests that people's real-world identities and relationships can be unmasked using its product (e.g., by providing phone numbers, email addresses, and other usernames to connect "all related personas").[99]

Media Sonar advertises the ability to "track criminal networks and their methods of communication" and "gain insight into past events and future threats through posts, pics, and videos." The software also allows law enforcement to search "social media for crisis specific hashtags."[100] It also advertises the ability to "monitor social media posts of multiple responding aid agencies" and to "quickly search . . . social media for crisis specific hashtags." These representations strongly suggest that Media Sonar is using information from X for surveillance purposes. Media Sonar also claims that it has some method of designating a group of accounts as a "network," and allows for increased tracking of the accounts associated with the network. The connections that people have with others on social media could contain private information, and the monitoring and analysis of those connections over time threatens to be even more revealing, including of people engaged in protests or associations protected by the First Amendment.

X and Meta's assurances to their users—and to the broader public—that they will not allow their platforms to be used for law enforcement surveillance stands in stark contrast to the privileged access that surveillance vendors seem to have to information from people's social

---

[97] *Media Sonar's presentation to LAPD*, BRENNAN CENTER FOR JUSTICE, https://www.brennancenter.org/sites/default/files/2021-09/H.%20Media%20Sonar%20Presentation.pdf.

[98] *Twitter: About profile visibility settings*, https://help.twitter.com/en/safety-and-security/birthday-visibility-settings ("Most of the profile information you provide us is always public, like your biography, location, website, and picture. For certain profile information fields we provide you with visibility settings to select who on Twitter can see this information in your Twitter profile. If you provide us with profile information and you don't see a visibility setting, that information is public."); *Facebook: What is public information on Facebook?*, https://www.facebook.com/help/203805466323736?helpref=faq_content ("Your Public Profile includes your name, gender, username and user ID (account number), profile picture, and cover photo.").

[99] *Media Sonar's presentation to LAPD*, BRENNAN CENTER FOR JUSTICE, https://www.brennancenter.org/sites/default/files/2021-09/H.%20Media%20Sonar%20Presentation.pdf.

[100] *LAPD Social Media Monitoring FOIA- H Series Media Sonar Presentation*, BRENNAN CENTER FOR JUSTICE, https://www.brennancenter.org/sites/default/files/2021-09/H.%20Media%20Sonar%20Presentation.pdf.

media. The disconnect between the platforms' claims and the reality of surveillance of people's social media activity could mislead reasonable consumers. The FTC should investigate whether the platforms have kept their promises.

### C. Privacy promises, including about law enforcement surveillance, are material to social media users.

Under the FTC's Policy Statement on Deception, "A 'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or conduct regarding a product. In other words, it is information that is important to consumers."[101]

The deceptive practices outlined above are material because users of social media platforms care about how their data is used and want companies to protect their safety and privacy by appropriately safeguarding their personal information. This simple fact is a cornerstone of the agency's work as it investigates, settles, and litigates privacy cases.[102]

Furthermore, the representations from X and Meta catalogued above are express claims, which the Commission considers presumptively material.[103] As the Supreme Court wrote in *Central Hudson Gas & Electric Co. v. PSC*, 447 U.S. 557, 567 (1980), and the FTC quoted in the Deception Policy Statement, "we may assume that the willingness of a business to promote its products"—or, as here, a limitation on the use of its products—"reflects a belief that consumers are interested in" what's being promoted. The frequency and specificity of the statements catalogued above and in **Appendix A** demonstrate that X and Meta know very well how much their users care about protecting the information on social media from the prying eyes of the government.

Studies and surveys also confirm, time and again, that consumers want products and services that protect their privacy, including protections from law enforcement. In 2016, the Pew Research Center found that 74% of all Americans believe it is "very important" to be in control of their personal information.[104] In 2019, surveys indicated that a majority of the public was concerned with how both private companies (79%) and government entities (64%) were using their personal information and that the risks of data collection outweigh the benefits for both private companies (81%) and the government (66%).[105] In 2023, a study

---

[101] *FTC Policy Statement on Deception*, FEDERAL TRADE COMMISSION (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[102] *Consumer Privacy*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy ("Consumers care about the privacy of their personal information and savvy businesses understand the importance of being clear about what you do with their data.").

[103] *FTC Policy Statement on Deception*, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[104] *The State of Privacy in Post-Snowden America,* PEW RESEARCH CENTER (Jun. 26th, 2023) https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/.

[105] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019)

conducted by the University of Pennsylvania found that virtually all Americans (91%) want to have control over what marketers can learn about them online.[106] Overall, the studies and surveys affirm that the public remains deeply concerned with data collection, both by government and private actors, and welcomes stronger privacy rights as surveillance practices become more and more pervasive.

## II. Allowing surveillance vendors to have developer access on X and Meta potentially violates the platforms' respective FTC consent orders.

In addition to the potential violation of Section 5, the Commission should also investigate whether X and Meta are in violation of the consent orders that place specific obligations on these two companies given their past (and repeated) violations of the FTC Act.

### A. X is in apparent violation of FTC consent orders.

In 2011, Twitter and the FTC entered into a consent decree ("the 2011 Twitter Order") to resolve agency allegations that Twitter deceived consumers and put their privacy at risk by failing to safeguard their personal information, resulting in two data breaches.[107] The consent decree remains in place through 2031 and imposes a series of obligations on X to prevent it from deceiving consumers or risking their privacy. In 2022, the FTC alleged that Twitter had violated the terms of the 2011 Twitter Order. Twitter settled the dispute by paying a $150 million fine and agreeing to an updated consent decree that imposes new obligations and remains in effect for an additional 20 years, through 2042.[108]

Part I of the 2011 Twitter Order states that X "shall not misrepresent in any manner, expressly or by implication, the extent to which [it] maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information[.]"[109] "Nonpublic consumer information" is defined as: "nonpublic, individually-identifiable information from or about an individual consumer, including, but not limited to, an individual consumer's: (a) email address; (b) Internet Protocol ("IP") address or other persistent identifier; (c) [and] mobile telephone number. . ."[110]

---

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[106] Joseph Turow et al., *Americans can't Consent to Companies' Use of Their Data* (2023) https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf at 13.

[107] *See* Decision and Order, *In the Matter of* Twitter Inc., FTC Docket No. C-4316 (Mar. 2, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[108] *See* Decision and Order, *In the Matter of* Twitter Inc., FTC Docket No. C-4316 (May 26, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023062C4316TwitterModifiedOrder.pdf.

[109] 2011 Twitter Order at 2.

[110] *Id.*

X appears to be in violation of Part I of the 2011 Twitter order. As shown in Section I(B)(4), X seems to provide covered information—like IP addresses and usernames—to surveillance vendors, like Skopenow.[111] This contradicts X's repeated claims that it does not allow developers to use covered information for law enforcement surveillance purposes.[112] Thus, X appears to be in violation of the 2011 order because it misrepresents the extent to which it maintains and protects the privacy of this nonpublic consumer information.

### B. **Meta is in apparent violation of FTC consent orders.**

In 2012, Facebook and the FTC entered into a consent decree (the "2012 Facebook Order") over charges that Facebook had deceived consumers by telling them they could keep their information on Facebook private, but then repeatedly allowing that "private" information to be shared and made public.[113] The 2012 Facebook Order requires the company to take several steps to make sure it lives up to its promises in the future, including giving consumers clear and prominent notice of how their data will be used and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established.[114]

Meta may be in violation of Part I of the 2012 Facebook Order when it claims not to allow developers to access data for law enforcement surveillance purposes. Part I of the 2012 Facebook Order requires, in relevant part, that Meta "shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to . . . the extent to which [it] makes or has made covered information accessible to third parties[.]" 2012 Facebook Order at 3–4.

"Covered information" is defined in the 2012 Facebook Order as:

> information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; (g) physical location; or (h) any information combined with any of (a) through (g) above.[115]

---

[111] *Lite Sample Commercial Report*, FEDERAL BUSINESS COUNCIL (Jul. 7, 2018) at 20-22, https://www.fbcinc.com/source/virtualhall_images/IRS_Tech_Expo_-_August/Skopneo/Sample_Report.pdf.

[112] *See* Section I(A); Appendix A.

[113] *See* Decision and Order, *In the Matter of* Facebook Inc., FTC Docket No. C-4365 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf ("2012 Facebook Order").

[114] *Id.* at 4.

[115] *Id.* at 3.

As shown in Section I(B)(4), Meta appears to provide covered information—like IP addresses, usernames, and geolocation information—to surveillance vendors, such as Skopenow.[116] This appears to contradict Meta's repeated claims that it does not allow developers to use covered information for law enforcement surveillance purposes.[117] Thus, in making these claims, Meta appears to be in violation of the 2012 Facebook Order by "misrepresent[ing] . . . the extent to which it maintains the privacy . . . of covered information."[118]

## III. The use of social media data for law enforcement surveillance has concrete, negative impacts on consumers.

Consumers use social media with the assumption that a simple like, tweet, or connection will not incur police scrutiny. Meta and X's policy changes and data privacy promises reaffirm to users that their data is protected from surveillance and misuse by law enforcement. In reality, however, law enforcement's use of social media data has routinely resulted in concrete harms to users, and these harms are magnified when agencies have access to tools that can supercharge their access and analysis.[119] Cases of assumed criminality, mistaken judgments, and targeting based on social media data impact not only individual users but also their families, friends and associates, and communities.[120]

---

[116] *Lite Sample Commercial Report*, FEDERAL BUSINESS COUNCIL (Jul. 7, 2018) at 5, 10-17, https://www.fbcinc.com/source/virtualhall_images/IRS_Tech_Expo_-_August/Skopneo/Sample_Report.pdf.

[117] *See* Section I(A); Appendix A.

[118] 2012 Facebook Order at 3. In 2018, the FTC alleged Facebook violated the 2012 Facebook Order by failing to screen app developers before granting them access to user data, by misrepresenting users' ability to control the use of facial recognition with their accounts, and by sharing the data of users' Facebook friends with third-party app developers, among other things. Facebook settled the dispute by paying a $5 billion fine and agreeing to an updated consent decree—effective in 2020—which imposed new obligations to prevent further misuse of consumer personal information. *See* Order Modifying Prior Decision and Order, *In the Matter of* Facebook Inc., FTC Docket No. C-4365 (Apr. 27, 2020), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf.

Meta is likely also in violation of the FTC's 2020 Modified Facebook Order, which contains the same prohibition against misrepresentations and expands the definition of covered information. *Id.*

[119] Social media monitoring tools allow law enforcement to gather and analyze more information on more individuals at a much faster speed than any manual collection. For example, Voyager Labs, which offers its social media monitoring tools to law enforcement, was sued by Meta in January 2023 for accessing publicly viewable profile information—like photos, videos, friend lists, posts, and self-disclosed location information—from around 1.2 million Facebook user profiles belonging to employees of non-profits, universities, the armed forces, and government as well as union members, parents, and retirees. See Meta Platforms, Inc. v. Voyager Labs LTD., No. 23-CV-00154-AMO, 2023 WL 4828007, at *1 (N.D. Cal. Jul. 26, 2023).

[120] Following the Supreme Court's decision overturning *Roe v. Wade*, a patchwork of states across the United States have banned abortions. *See Tracking the States Where Abortion is Now Banned*, N.Y. TIMES (Aug. 26, 2022), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html. Advocates have sounded the alarm with concern that social media and digital information could be used against those receiving or supporting abortion in states that have criminalized the procedure. *See* Wash. Post Editorial

The examples detailed below—related to protesters and immigrants—represent a subset of possible particularized harms resulting from the use of social media data for law enforcement surveillance.

### A. Law enforcement has used social media surveillance to target and wrongly arrest protestors and activists of color.

As the ACLU detailed in its September 2016 report, social media surveillance tools have been used by law enforcement to target protests and activists of color.[121] Marketing materials for Media Sonar and Geofeedia touted their ability to monitor racial justice protests and referred to unions and activist groups as "overt threats."[122] Federal law enforcement has monitored social media to target racial justice protestors in Portland, Oregon as well as journalists from the *New York Times* and *Lawfare* covering the protests.[123]

Beyond simple monitoring, police use of social media has resulted in assumed criminality and mistaken judgments leading to wrongful arrests. The NYPD wrongly arrested 19-year-old Jelani Henry based on "likes" and photos on social media that the district attorney believed proved he was a member of a violent gang.[124] Henry was denied bail and jailed for over a year and a half before his case was finally dismissed. Police in Wichita, Kansas wrongly arrested a teenager based on mistaken interpretation of a Snapchat, which they interpreted as inciting a riot but was actually denouncing violence.[125] A Black racial justice activist was arrested in part for his anti-police Facebook posts.[126] While detained, he lost his vehicle, job, and home.[127] And in 2015, the Director of Civil Rights for the Oregon Department of Justice was profiled and subject to further surveillance after an investigator used a digital surveillance tool to search for the #BlackLivesMatter hashtag, among

---

Board, *After the Abortion Ruling Digital Privacy Is More Important Than Ever*, WASH. POST (Jul. 4, 2022), https://www.washingtonpost.com/opinions/2022/07/04/abortion-ruling-digital-privacy-important/; Lily Hay Newman, *The Surveillance State is Primed for Criminal Abortion,* WIRED (May 24, 2022), https://www.wired.com/story/surveillance-police-roe-v-wade-abortion/.

[121] Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU (Sep. 22, 2016), https://www.aclu.org/news/privacy-technology/police-use-social-media-surveillance-software.

[122] *Id.*

[123] Shane Harris, *DHS Compiled 'Intelligence Reports' on Journalists Who Published Leaked Documents*, WASH. POST, (Jul. 30, 2020), https://www.washingtonpost.com /national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html.

[124] Rachel Levinson-Waldman, Harsha Panduranga & Faiza Patel, *Social Media Surveillance by the U.S. Government 6*, BRENNAN CENTER FOR JUSTICE (Jan. 7, 2022) https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

[125] *Id.*

[126] Sam Levin, *Black Activist Jailed for His Facebook Posts Speaks Out About Secret FBI Surveillance*, THE GUARDIAN (May 11, 2018), https://www.theguardian.com/world/2018/may/11/rakem-balogun-interview-black-identity-extremists-fbi-surveillance.

[127] *Id.*

others.[128] These harms are present when law enforcement relies too exclusively on direct access to social media as an investigative tool; law enforcement use of surveillance tools that analyze social media information at an immense scale threatens to further amplify the harms to people and communities.

Social media has also been used to facilitate the targeting of protests, including against the Trump administration's immigration policies.[129] Drawing on social media data, DHS compiled dossiers and placed travel alerts on advocates, journalists, and lawyers whom the government suspected of helping migrants at the U.S border.[130]

### B. Law enforcement has used social media surveillance to ban and deport individuals.

DHS and the Department of State have also used social media for immigration vetting, monitoring of noncitizens within U.S. borders, and deportation of noncitizens. As this letter describes below, the use of individualized social media analysis in the immigration context can cause grave harm. And automated tools that operate at scale risk increasing those harms.

DHS and the State Department have expanded their collection of social media handles for screening and vetting purposes, through a combination of mandatory and optional questions on visa and other travel-related forms.[131] Social media vetting is entirely unproven, however, and has often resulted in mistakes.[132] Indeed, the Office of the Director of National Intelligence acknowledged, in a document recently obtained through a FOIA lawsuit, that gathering social media handles from visa applicants added "no value" to the screening process.[133] As one example of the difficulty of interpreting social media, particularly across language or cultural differences, a British national was wrongly denied entry to the United States in 2012 when DHS agents misinterpreted a tweet saying he was

---

[128] *Attorney General Ellen Rosenblum Took Her Time Addressing Allegations of Illegal Surveillance By Her Agency*, WILLAMETTE WEEK (2015), https://www.wweek.com/news/2015/11/18/attorney-general-ellen-rosenblum-took-her-time-addressing-allegations-of-illegal-surveillance-by-her-agency/.

[129] *See* Ryan Deveraux, *Homeland Security Used A Private Intelligence Firm to Monitor Family Separation Protests*, THE INTERCEPT (Apr. 29, 2019), https://theintercept.com/2019/04/29/family-separation-protests-surveillance/.

[130] Rachel Levinson-Waldman, Harsha Panduranga & Faiza Patel, *Social Media Surveillance by the U.S. Government*, BRENNAN CENTER FOR JUSTICE (Jan. 7, 2022), https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

[131] Faiza Patel, Rachel Levinson-Waldman, Sophia Denuyl & Raya Koreh, *Social Media Monitoring: How The Department Of Homeland Security Uses Digital Data In The Name Of National Security*, BRENNAN CENTER FOR JUSTICE (May 22, 2019) https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf.

[132] *Id.*

[133] Charlie Savage, *Visa Applicants' Social Media Data Doesn't Help Screen for Terrorism, Documents Show*, N.Y. TIMES (Oct. 5, 2023), https://www.nytimes.com/2023/10/05/us/social-media-screening-visa-terrorism.html.

going to "destroy America," which is British slang for partying, and "dig up Marilyn Monroe's grave," which was a joking reference to a television show.[134]

Further, DHS has implemented programs monitoring the social media of noncitizens inside the United States. Immigration and Customs Enforcement monitors students within the United States who switch from studying "nonsensitive" to "sensitive" topics (e.g., nuclear physics, biomedical engineering, robotics).[135] ICE programs targeting visa overstays monitor the social media of visitors who applied for visas from specific State Department posts abroad and visitors flagged as "high risk."[136] ICE's Open-Source Team, which uses publicly-available information, including social media, to locate and track specific individuals, has published three "success stories"—all involving individuals from Muslim-majority countries.[137]

Lastly, DHS and ICE have used social media to locate, arrest, and deport individuals. In one case, ICE officers arrested an individual buying roofing supplies at a Home Depot store after he "checked in" on Facebook.[138] He had lived in the United States since he was a year old and had U.S. citizen children.[139] He told the judge at his sentencing that he was "sorry" and had simply "[come] back to be with [his] family."[140] While these examples may not all involve the use of the kinds of tools covered by this letter, they illustrate the harm that can arise from use of social media surveillance to make high-stakes decisions—harms that are magnified when the government's capabilities are supercharged through the use of powerful tools and expansive repositories of information.

## G. Conclusion

The fact that social media monitoring tools appear still to be accessing Facebook, Instagram, and/or X 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 on individuals and communities.

Given the above, the Commission should determine, by engaging directly with X and Meta in the context of ongoing investigations, whether surveillance vendors are operating with authorization, such as through developer access, on the platforms. The Commission should

---

[134] *Id.* at 4.

[135] Faiza Patel, Rachel Levinson-Waldman, Sophia DenUyl & Raya Koreh, *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security 24*, BRENNAN CENTER FOR JUSTICE (May 22, 2019), https://www.brennancenter.org/sites/default/files/2019-08/Report_Social_Media_Monitoring.pdf.

[136] *Id.* at 7, 24.

[137] *Id.* at 24.

[138] Max Rivlin Nadler, *How ICE Uses Social Media to Surveil And Arrest Immigrants*, THE INTERCEPT (Dec. 22, 2019), https://theintercept.com/2019/12/22/ice-social-media-surveillance/.

[139] *Id.*

[140] *Id.*

further determine what efforts X and Meta are making to ensure that their promises regarding the use of people's personal information for surveillance are being kept. Those efforts by the platforms should include auditing and enforcement structures to make sure that X and Meta enforce their respective prohibitions on surveillance. The Commission should determine whether such structures are in place and operating effectively.

As noted above, X and Meta are undergoing significant changes in their businesses. The Commission's investigation should also seek to understand how the companies' recent changes—from firing workers to shifting business priorities—have affected their ability to keep their promises to their users and the public.

Finally, the Commission should, as the Brennan Center requested in their comments in response to the Federal Trade Commission's advance notice of proposed rulemaking on commercial surveillance and data security practices, convene a listening session and a workshop focusing on social-media surveillance, the harm it causes, and the extent of the platforms efforts to stop it.

Sincerely,

Jacob A. Snow
Senior Staff Attorney
Technology and Civil Liberties Program
ACLU Foundation of Northern California
jsnow@aclunc.org

Rachel Levinson-Waldman
Managing Director, Liberty & National Security Program
Brennan Center for Justice
levinsonr@brennan.law.nyu.edu

Cody Venzke
Senior Policy Counsel
ACLU
CVenzke@aclu.org

Ivey Dyson
Counsel, Liberty & National Security Program
Brennan Center for Justice
dysoni@brennan.law.nyu.edu

# Appendix A

**October 2016: Facebook and Twitter Respond to Geofeedia.**

On October 11, 2016, the ACLU revealed that Geofeedia, which allowed users to search for social media content Facebook, Twitter, and Instagram, as well as nine other social media networks—in specific locations, helped Baltimore police monitor and respond to protests that broke out after Freddy Gray died in police custody in April 2015.[141] Geofeedia facilitated access to Facebook, Twitter, and Instagram, as well as nine other social media networks. Following that release, Facebook and Twitter explained their developer policies and announced they were removing Geofeedia from their platforms.

Facebook reiterated its data use policies for developers, which did not yet explicitly bar surveillance. First, Jodi Seth, Facebook's Director of Policy Communications, stated that Geofeedia—subject to Facebook's platform policy—was required to provide a privacy policy explaining the data they were collecting and how it would be used and to receive user consent to that policy.[142] Second, in a statement to *TechCrunch*, a spokesperson added, "If a developer uses our APIs in a way that has not been authorized, we will take swift action to stop them and we will end our relationship altogether if necessary."[143] Third, *The Washington Post* also noted that Geofeedia was improperly using data, based on Facebook's statements.[144] On October 20, *The Daily Dot* reported that a spokesperson emailed that Facebook "terminated Geofeedia's access to the Instagram and Topic Feed API because it

---

[141] ACLU of Northern California, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, MEDIUM (Sep. 22, 2016), https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48.

[142] Bromwich, Victor, & Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html ("Jodi Seth, director of policy communications at Facebook, said that Geofeedia had access to data that had been made public on the social network, and that access was subject to the limitations in its platform policy. That policy asks developers to 'provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data.' It also asks that they 'obtain adequate consent from people before using any Facebook technology that allows us to collect and process data about them.'").

[143] Lora Kolodny, *Facebook, Twitter Cut Off Data Access for Geofeedia, A Social Media Surveillance Startup,* TECHCRUNCH (Oct. 11, 2016), https://techcrunch.com/2016/10/11/facebook-twitter-cut-off-data-access-for-geofeedia-a-social-media-surveillance-startup/ ("[Geofeedia] only had access to data that people chose to make public. Its access was subject to the limitations in our Platform Policy, which outlines what we expect from developers that receive data using the Facebook Platform. If a developer uses our APIs in a way that has not been authorized, we will take swift action to stop them and we will end our relationship altogether if necessary.").

[144] Timberg & Dowskin, *Facebook, Twitter and Instagram Sent Feeds That Helped Police Track Minorities in Ferguson and Baltimore, Report Says,* WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/ ("Facebook, which owns Instagram, said in a statement that Geofeedia was accessing its data improperly: 'This developer only had access to data that people chose to make public. . .. If a developer uses our [user data] in a way that has not been authorized, we will take swift action to stop them and we will end our relationship altogether if necessary.'").

was using these APIs in ways that exceeded the purposes for which they were provided . . . We will do the same for other developers that violate our policies."[145]

On October 11, Twitter suspended Geofeedia's commercial access to data because its Developer Policy prohibited selling user data for surveillance. From its Public Policy Account (then @Policy, now @GlobalAffairs), Twitter announced "Based on information in the @ACLU's report, we are immediately suspending @Geofeedia's commercial access to Twitter data."[146] Over email, a spokesperson told *The Hill* that Twitter had a longstanding rule that prohibits sale of user data for surveillance, and that Twitter's Developer Policy bans the use of data to surveil users.[147] Additionally, on October 20, after public records requests revealed another company, SnapTrends, was providing surveillance services to law enforcement, the *Daily Dot* reported a Twitter spokesperson confirmed that SnapTrends would no longer have access to Twitter's commercial data.[148]

**November–December 2016: Twitter Publicizes Its Developer Policy.**

On November 22, 2016, Twitter clarified that its platform barred the use of user data for surveillance. Chris Moody, Twitter's Vice President of Data and Enterprise Solutions, posted the following on Twitter's blog:

> "Recent reports about Twitter data being used for surveillance, however, have caused us great concern. As a company, our commitment to social justice is core to our mission and well established. And our policies in this area are long-standing. Using Twitter's Public APIs or data products to track or profile protesters and activists is absolutely unacceptable and prohibited.
>
> To be clear: We prohibit developers using the Public APIs and Gnip data products from allowing law enforcement — or any other entity — to use Twitter data for surveillance purposes. Period. The fact that our Public APIs and Gnip data products provide information that people choose to share publicly does not change our policies in this area. And if developers violate our policies, we will take appropriate action, which can include suspension and termination of access to Twitter's Public APIs and data products.

---

[145] Dell Cameron, *Twitter Cuts Ties with Second Firm Police Use to Spy on Social Media*, THE DAILY DOT (Oct. 20, 2016), https://www.dailydot.com/irl/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/ .

[146] @Policy, TWITTER (Oct. 11, 2016, 11:14 AM), https://twitter.com/Policy/status/785861128589025281.

[147] Ali Breland, *Facebook, Twitter block surveillance tool*, THE HILL (Oct. 11, 2016, 4:57 PM), https://thehill.com/policy/technology/300482-facebook-twitter-block-surveillance-tool/ ("Twitter does have a 'longstanding rule' prohibiting the sale of user data for surveillance as well as a Developer Policy that bans the use of Twitter data "to investigate, track or surveil Twitter users.").

[148] Dell Cameron, *Twitter Cuts Ties with Second Firm Police Use to Spy on Social Media*, THE DAILY DOT (OCT. 20, 2016), https://www.dailydot.com/irl/twitter-snaptrends-geofeedia-social-media-monitoring-facebook/. ("SnapTrends serviced police and national intelligence agencies across the country with algorithms to provide a 'social data footprint.' Twitter made its decision after the Daily Dot requested comments on a cache of internal police records, obtained through public records requests, revealed these contracts.").

> We have an internal process to review use cases for Gnip data products when new developers are onboarded and, where appropriate, we may reject all or part of a requested use case. Over the coming months, you'll see us 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."[149]

Moody's personal twitter account[150] and the Twitter Dev Account (@TwitterDev) publicized the update and a link to the blog post.[151] On December 12, 2018, in a letter to the ACLU of Northern California, Colin Crowell, Twitter's Vice President of Global Public Policy, reiterated that "the use of Twitter data for surveillance is strictly prohibited, and we continue to expand our enforcement efforts."[152]

**March 2017: Facebook Updates Its Platform Policy.**

On March 13, 2017, Facebook announced updates to Facebook's and Instagram's policies to explicitly prohibit surveillance. On its Facebook and Privacy account[153] and its Public Affairs[154] account, Facebook stated:

> "Today we are adding language to our Facebook and Instagram platform policies to more clearly explain that developers cannot 'use data obtained from us to provide tools that are used for surveillance.' Our goal is to make our policy explicit. Over the past several months we have taken enforcement action against developers who created and marketed tools meant for surveillance, in violation of our existing policies; we want to be sure everyone understands the underlying policy and how to comply."[155]

---

[149] Moody, *Developer Policies to Protect People's Voices on Twitter*, TWITTER DEV. PLATFORM BLOG (Nov. 22, 2016), https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter.

[150] @chrismoodycom, TWITTER (Nov. 22, 2016, 1:37 PM), https://twitter.com/chrismoodycom/status/801132611837915136 ("An important update to our developer community: https://blog.twitter.com/developer/en_us/topics/community/2016/developer-policies-to-protect-peoples-voices-on-twitter").

[151] @TwitterDev, TWITTER (Nov. 22, 2016, 1:33 PM), https://twitter.com/TwitterDev/status/801131588348063744 ("Given recent reports we want to provide clarity on our policies that protect people's voices on Twitter.").

[152] Letter from Colin Crowell, Twitter Vice President, Global Public Policy, to ACLU of Northern California (Dec. 12, 2016), http://www.aclunc.org/docs/20161212_twitter_letter_to_aclu.pdf.

[153] @Facebook and Privacy, FACEBOOK (Aug. 1, 2023), https://www.facebook.com/fbprivacy (The account has 2.6 million followers).

[154] @Facebook Public Affairs, FACEBOOK (Aug. 1, 2023) https://www.facebook.com/fbpublicaffairs/ (The account currently has 20k followers).

[155] @Facebook and Privacy, FACEBOOK (Mar. 13, 2017), https://www.facebook.com/fbprivacy/posts/1624880004207125; @Facebook Public Affairs, FACEBOOK (Mar. 13, 2017), https://www.facebook.com/fbpublicaffairs/posts/1617594498258356.

Rob Sherman, Facebook's Deputy Chief Privacy Officer, publicized the announcement, sharing a link to the Facebook and Privacy account post and stating, "We're clarifying that Facebook's policies don't allow developers to build tools that use Facebook data for surveillance."[156]

**April 2018: Facebook Reiterates Platform Policy in Senate Hearing.**

The Senate Committee on Commerce, Science, and Transportation and the Senate Committee on the Judiciary held a hearing on April 10, 2018 titled "Facebook, Social Media Privacy, and the Use and Abuse of Data."[157] Three senators submitted written questions for Mark Zuckerberg's response.

First, Senator Dianne Feinstein asked what limits Facebook has placed on how personal information can be used by third parties.[158] Zuckerberg wrote that "developers may not use data obtained from Facebook to provide tools that are used for surveillance."[159]

Second, Senator Patrick Leahy asked whether Facebook cooperates with law enforcement or companies working on their behalf in any ways that allow for user profiling or predictive analytics.[160] Although Zuckerberg responded that Facebook cannot speculate on how governments profile, he wrote, "[W]e prohibit developers from using data obtained from us to provide tools that are used for surveillance."[161]

Third, Senator Cory Booker asked why communities of color should trust that Facebook had addressed the surveillance issue after the Geofeedia revelations and whether Facebook's terms of service changes were sufficient.[162] Zuckerberg reiterated that the March 2017 policy

---

[156] *Rob Sherman*, FACEBOOK (Mar. 13, 2017), https://www.facebook.com/rmsherman.

[157] *Facebook, Social Media Priv., and the Use and Abuse of Data, Joint Hearing before the Senate Comm. on Com., Sci., and Transp. and the Senate Comm. on the Judiciary*, 115th Cong. (Apr. 10, 2018), https://www.congress.gov/115/chrg/CHRG-115shrg37801/CHRG-115shrg37801.pdf.

[158] *Id.* at 311.

[159] *Id.* ("Developers can access Account Information in accordance with their privacy policies and other Facebook policies. All other data may not be transferred outside the Facebook app, except to service providers, who need that information to provide services to the Facebook app. With the exception of Account Information, developers may only maintain user data obtained from Facebook for as long as necessary for their business purpose. Developers may not use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan. Developers must protect the information they receive from Facebook against unauthorized access, use, or disclosure. For example, developers may not use data obtained from Facebook to provide tools that are used for surveillance.").

[160] *Id.* at 322.

[161] *Id.* ("Facebook is not familiar with government agencies' practices regarding profiling and/or predictive analytics and therefore cannot speculate what would "allow for" such agencies to use such techniques. Facebook discloses account records to Federal, State, or local agencies and authorities only in accordance with our terms of service and applicable law. Additionally, we prohibit developers from using data obtained from us to provide tools that are used for surveillance.").

[162] *Id.* at 363.

language changes clearly explain that developers cannot use data obtained from Facebook to provide tools that are used for surveillance.[163]

**July 2018: Facebook Again Repeats Its Surveillance Prohibition Following its Investigation of Crimson Hexagon.**

On July 20, 2018, Facebook suspended Crimson Hexagon from its platform while it investigated the analytics firm's U.S. government contracts and data usage.[164] Facebook told *The Wall Street Journal* it had not been aware of some of Crimson Hexagon's contracts but was launching a broad inquiry into how the firm collects, shares, and stores user data.[165] Ime Archibong, Facebook's Vice President for Product Partnerships, stated that Facebook had tightened access to user data in recent years, and while it allows outside parties to produce "anonymized insights for business purposes," Facebook prohibits the use of its data for surveillance.[166] A Facebook spokesperson told *Engadget*, "We don't allow developers to build surveillance tools using information from Facebook or Instagram. . . . We take these allegations seriously, and we have suspended these apps while we investigate."[167] *ThreatPost* reported a similar spokesperson statement.[168] On August 22, Facebook reinstated Crimson Hexagon's access to its platform, though *Fast Company* noted Facebook's May 2018 statement that it had suspended 200 third-party apps for improper collection and misuse of user data.[169]

---

[163] *Id.* ("In March 2017, we added language to our Facebook and Instagram platform policies to more clearly explain that developers cannot use data obtained from us to provide tools that are used for surveillance. Our previous policy limited developers' use of data but did not explicitly mention surveillance. We found out that some developers created and marketed tools meant for surveillance, took action, and we clarified our policy.").

[164] Kirsten Grind, *Facebook Suspends Analytics Firm on Concerns About Sharing of Public User-Data*, WALL ST. J. (Jul. 20, 2018), https://www.wsj.com/articles/facebook-probing-how-analytics-firm-shares-public-user-data-1532104502.

[165] *Id.* ("Facebook, in response to questions from The Wall Street Journal this week about its oversight of Crimson Hexagon's government contracts and storing of user data, said Friday it wasn't aware of some of the contracts. On Friday, it said it was suspending Crimson Hexagon's apps from Facebook and its Instagram unit, and launching a broad inquiry into how Crimson Hexagon collects, shares and stores user data.").

[166] *Id.* ("'Facebook has a responsibility to help protect people's information, which is one of the reasons why we have tightened' access to user data in many ways in recent years, said Ime Archibong, Facebook vice president for product partnerships, in a statement.").

[167] Mallory Locklear, *Facebook could have another Cambridge Analytica on its hands*, ENGADGET (Jul. 20, 2018), https://www.engadget.com/2018-07-20-facebook-suspends-crimson-hexagon-data-collection.html.

[168] Lindsey O'Donnell, *Facebook Suspends Analytics Firm Over Surveillance Concerns*, THREATPOST (Jul. 23, 2018), https://threatpost.com/facebook-suspends-analytics-firm-over-surveillance-concerns/134286/ ("A Facebook spokesperson told Threatpost that the social media company doesn't allow developers to build surveillance tools using information from Facebook or Instagram: 'We take these allegations seriously, and we have suspended these apps while we investigate.'").

[169] Alex Pasternack, *Facebook reinstates data firm it suspended for alleged misuse, but surveillance questions linger*, FAST CO. (Aug. 22, 2018), https://www.fastcompany.com/90219826/why-did-facebook-re-friend-a-data-firm-that-raised-spying-concerns.

Twitter relies on Crimson Hexagon's services to analyze its own network.[170] In response to questions, a Twitter spokesperson repeated that Twitter prohibits the use of data for surveillance and has invested heavily in rigorously enforcing rules against developers.[171]

**July–October 2020: Twitter Again Reiterates Its Policy After Concerns About Dataminr.**

In May 2016, Twitter cut off U.S. intelligence agencies from accessing Dataminr, a company in which Twitter owned a 5% stake and that had been authorized by Twitter to access its real-time stream of public tweets and sell those tweets to clients.[172] However, on July 9, 2020, *The Intercept* reported that Dataminr continued to enable law enforcement surveillance by relaying social media content directly to police across the country during George Floyd and Black Lives Matter protests. Notably, Dataminr was able to continue taking advantage of its privileged access to Twitter information, despite Twitter's bar on tracking protests. Twitter spokesperson Lindsay McCallum told *The Intercept* of Dataminr's tools, "We see a societal benefit in public Twitter data being used for news alerting, first responder support, and disaster relief. . . . [Dataminr's First Alert tool] is in compliance with our developer [surveillance] policy."[173]

On October 21, *The Intercept* reported additional details on how Dataminr targets communities of color for police, and while McCallum declined to answer questions about Dataminr's surveillance practices, she stated that "Twitter prohibits the use of our developer services for surveillance purposes. Period. . . [Twitter has] done extensive auditing of Dataminr's tools, including First Alert, and have not seen any evidence that they're in violation of our policies."[174]

**November 2021: Meta Asks LAPD to Halt Surveillance, Citing Policy.**

On September 8, 2021, the Brennan Center for Justice released documents showing how the Los Angeles Police Department (LAPD) uses Voyager Labs to analyze user data from

---

[170] *Id.*

[171] *Id.* ("In response to questions about Crimson Hexagon, a Twitter spokesperson reiterated its policy. 'We prohibit the use of our data products for surveillance purposes, or for any purpose that is inconsistent with our users' expectations of privacy. Period. These rules apply to all users of our developer platform, not just government entities. We have invested heavily in our data compliance program over the last several years and we rigorously enforce our rules against violating developers—up to and including permanent suspension of access to Twitter data in any form. If we learn of any developer breaking our rules, we will investigate and take appropriate action[.]'").

[172] Christopher S. Stewart & Mark Maremont, *Twitter Bars Intelligence Agencies From Using Analytics Service*, WALL ST. J. (May 8, 2016), https://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682 (noting that Twitter refused to comment on why Dataminr had been allowed to enable surveillance for two years despite existing Twitter policy).

[173] Sam Biddle, *Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr*, THE INTERCEPT (Jul. 9, 2020), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/.

[174] Sam Biddle, *Twitter Surveillance Startup Targets Communities of Color for Police*, THE INTERCEPT (Oct. 21, 2020), https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/.

Facebook and enable law enforcement to create fake accounts.[175] On November 11, 2021, Roy L. Austin, Jr., Meta's Vice President and Deputy General Counsel wrote to the LAPD.[176] Austin wrote that the LAPD must stop any fake accounts, impersonation, or data collection for surveillance purposes because they violated Meta's terms of service.[177] Austin added that since developers are prohibited from using data obtained on the platform for surveillance, Meta would take action against prohibited third-party vendor conduct.[178] A Twitter spokesperson, responding to revelations about LAPD's use of a different vendor to monitor Twitter, reiterated publicly that the platform prohibits the use of developer services for surveillance purposes and represented that it "proactively enforce[s] our policies to ensure customers are in compliance."[179]

**Today: Multiple X Policies Prohibit Surveillance.**

X's *Ads Products and Services Agreement* states:

> "Compan[ies in Ads API Program] will not [] knowingly allow or assist any government entities, law enforcement, or other organizations to conduct surveillance on the Twitter Service or the Twitter Materials or obtain information on Twitter's users or their Tweets that would require a subpoena, court order, or other valid legal process, or that would otherwise have the potential to be inconsistent with Twitter's users' reasonable expectations of privacy."[180]

X's *Developer Agreement* states:

---

[175] *LAPD Social Media Monitoring Documents*, BRENNAN CENTER FOR JUSTICE (Sep. 8, 2021; updated Dec. 15, 2021), https://www.brennancenter.org/our-work/research-reports/lapd-social-media-monitoring-documents.

[176] Letter from Roy L. Austin, Jr., Meta Vice President and Deputy General Counsel, to Michael R. Moore, Los Angeles Police Department Chief (Nov. 11, 2021), https://about.fb.com/wp-content/uploads/2021/11/LAPD-Letter.pdf.

[177] *Id.* at 1 ("To the extent these practices are 1 ongoing they violate our terms of service. While the legitimacy of such policies may be up to the LAPD, officers must abide by Facebook's policies when creating accounts on our services. The Police Department should cease all activities on Facebook that involve the use of fake accounts, impersonation of others, and collection of data for surveillance purposes.")

[178] *Id.* at 2–3 ("It has also come to our attention that the LAPD has used a third-party vendor to collect data on our platforms regarding our users. Under our policies, developers are prohibited from using data obtained on our platforms for surveillance, including the processing of platform data about people, groups, or events for law enforcement or national security purposes (https://developers.facebook.com/terms/#control). We regard the above activity as a breach of Facebook's terms and policies, and as such, we will disable any fake accounts that we identify and take action against third-party vendor conduct that violates our terms..")

[179] Sam Levin & Johana Bhuiyan, *Revealed: LAPD Used 'Strategic Communications' Firm to Track 'Defund the Police' Online*, THE GUARDIAN (Dec. 15, 2021), https://www.theguardian.com/us-news/2021/dec/15/revealed-los-angeles-police-social-media-surveillance-technology.

[180] *Ads API Agreement § 15.2: User Protection*, TWITTER, https://developer.twitter.com/en/developer-terms/ads-api-agreement.

> "Unless explicitly approved otherwise by Twitter in writing, you 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, segmenting, or profiling individuals based on sensitive personal information, including their health (e.g., pregnancy), negative financial status or condition, political affiliation or beliefs, racial or ethnic origin, religious or philosophical affiliation or beliefs, sex life or sexual orientation, trade union membership, Twitter Content relating to any alleged or actual commission of a crime, or any other sensitive categories of personal information prohibited by law."[181]

In an elaboration of the *Developer Agreement*, X provides additional detail on surveillance policies:

> "[W]e prohibit 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.
>
> We describe prohibited uses of our data and developer products in the Developer Agreement, including prohibitions on investigating or tracking Twitter users or their content, as well as tracking, alerting, or monitoring sensitive events (such as protests, rallies, or community organizing meetings).
>
> Other categories of activities prohibited under these terms include (but are not limited to):
>
> - Investigating or tracking sensitive groups and organizations, such as unions or activist groups
> - Background checks or any form of extreme vetting
> - Credit or insurance risk analyses
> - Individual profiling or psychographic segmentation
> - Facial recognition

[181] *Developer Agreement § XII.B. User Protection*, TWITTER, https://developer.twitter.com/en/developer-terms/agreement.

> These policies apply to all users of our APIs. Any misuse of the Twitter APIs for these purposes will be subject to enforcement action, which can include suspension and termination of access."[182]

X's *Guidelines for Law Enforcement* explains policies for law enforcement personnel directly seeking information about X users, which do not discuss surveillance.[183]

**Today: Meta Platform Terms Prohibit Surveillance.**

> Meta's *Platform Terms* state:
>
> "a. Prohibited Practices. You will not perform, or facilitate or support others in performing, any of the following prohibited practices (collectively, "Prohibited Practices"): . . .
>
> > iii. Processing Platform Data to perform, facilitate, or provide tools for surveillance. Surveillance includes the Processing of Platform Data about people, groups, or events for law enforcement or national security purposes."[184]

[182] *More about restricted uses of the Twitter APIs*, TWITTER, https://developer.twitter.com/en/developer-terms/more-on-restricted-use-cases.

[183] *Guidelines for law enforcement*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support.

[184] *Meta Platform Terms § 3.a.iii*, META, https://developers.facebook.com/terms/.