Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

October 25, 2022

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Submitted electronically at www.regulations.gov

Re: Advance Notice of Proposed Rulemaking Regarding Commercial Surveillance

We, the undersigned scholars of privacy and technology law, in conjunction with the Policing Project at New York University School of Law, submit the following comments in response to the Federal Trade Commission's ("FTC") Advance Notice of Proposed Rulemaking regarding commercial surveillance and data security published on August 22, 2022, at 87 Fed. Reg. 51273 ("Commercial Surveillance ANPR").

The Policing Project is a non-partisan center at New York University School of Law dedicated to promoting public safety through transparency, equity, and democratic engagement. Much of our work focuses on the use of emerging technologies by law enforcement and how this impacts civil rights, civil liberties, and racial justice.

Our comments below address several of the issues raised in the Commercial Surveillance ANPR, but are especially relevant to the questions set forth in Sections IV(a)(4) ("How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?") and IV(a)(5) ("Are there some harms that consumers may not easily discern or identify? Which are they?").

I. Increasingly, policing agencies are using commercial surveillance to monitor individuals.

Unbeknownst to many, a growing number of private companies are amassing vast quantities of data related to individuals' movements, associations, and activities. The use of this data by private entities such as advertisers and retailers has received significant attention in recent years.[1] But another aspect of the commercial surveillance industry has received far less scrutiny: the use of personal data by policing agencies seeking to expand their surveillance capabilities.

Policing agencies are purchasing location data derived from the everyday apps we install on our cellphones, including weather, map, dating, and prayer apps — even apps relating to our most

[1] *See, e.g.*, Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

intimate activities.[2] One company, Ventell, boasts that it collects over 15 billion location points *daily* from individuals' cell phones and other mobile devices.[3] Through this data, the company claims, police can determine an individual's "frequented locations," "known associates," and "pattern of life."[4] Another company, Fog Data Science, offers location data sourced from apps such as Starbucks and Waze for as little as $7,500 per year.[5]

Other commercial surveillance firms analyze data from popular social media websites such as Twitter, Facebook, and Instagram. A service called Geofeedia was used by policing agencies in multiple cities to surveil protests against police abuses.[6] Another service, Digital Stakeout, was used by the Oregon Department of Justice to surveil individuals using the "#BlackLivesMatter" hashtag on social media.[7]

And these examples are just the tip of the iceberg — a vast array of personal data is available to police in this sprawling and largely unregulated market. Motorola offers a database of vehicle location data from automated license plate readers (devices which capture and store license plate information from passing vehicles) comprising over 35 billion records.[8] Clearview AI's facial recognition software enables police to identify individuals by searching against a database of billions of images scraped from websites such as Facebook, YouTube, and Venmo.[9] LexisNexis has assembled over 283 million "dossiers" with information including work history, outstanding debts, purchases, and driving records.[10] And SpyCloud offers police access to data stolen from websites in data breaches, including user passwords and IP addresses.[11] Some are now raising alarms about the prospect of fertility and period-tracking apps sharing data with law enforcement in states that have criminalized abortion.[12]

---

[2] *See* Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, Vice (Dec. 3, 2020), https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps.

[3] *See* Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.

[4] *See id.*

[5] *See* Garance Burke & Jason Dearen, *How An Obscure Cellphone Tracking Tool Provides Police 'Mass Surveillance on a Budget'*, PBS (Sept. 1, 2022), https://www.pbs.org/newshour/politics/how-an-obscure-cellphone-tracking-tool-provides-police-mass-surveillance-on-a-budget.

[6] *See* Sam Levin, *ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protesters*, Guardian (Oct. 11, 2016), https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter; *US Start-up Geofeedia 'Allowed Police to Track Protesters'*, BBC (Oct. 12, 2016), https://www.bbc.com/news/world-us-canada-37627086.

[7] *See* Conrad Wilson, *Oregon Orders a Stop to Surveillance of Black Lives Matter Supporters*, NPR (Nov. 13, 2015), https://www.npr.org/2015/11/13/455862583/oregon-orders-a-stop-to-surveillance-of-black-lives-matter-supporters.

[8] *See* DO MORE THAN JUST DETECT: BUILD YOUR LICENSE PLATE RECOGNITION PROGRAM WITH PURPOSE-BUILT CAMERAS & ADVANCED SOFTWARE, MOTOROLA SOLUTIONS, https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/lpr_brochure.pdf

[9] *See* Kashmir Hill, *The Secretive Company That Might End Privacy As We Know It*, N.Y. TIMES (Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[10] *See id.*

[11] *See* Joseph Cox, *Police Are Buying Access to Hacked Website Data*, VICE (July 8, 2020), https://www.vice.com/en/article/3azvey/police-buying-hacked-data-spycloud

[12] *See* Vittoria Elliot, *Fertility and Period Apps Can Be Weaponized in a Post-Roe World*, WIRED (June 7, 2022), https://www.wired.com/story/fertility-data-weaponized.

The commercial surveillance industry is arming police with an expansive arsenal of information about our personal lives. Our movements, communications, financial histories — even our faces — are being captured, catalogued, and furnished to law enforcement, for a price.

II. The exploitation of our personal data by law enforcement poses grave risks. Yet there is little transparency about these practices, and few guardrails.

Privacy is essential to our way of life. We may, for good reasons, wish to keep private the medical care we receive or the religious services we attend. We may wish to shield from others our attendance at a support group or our membership in a private organization. Or we may wish to share our political beliefs with friends and neighbors, free from government scrutiny.

Without privacy, we may be deterred from exercising our most essential rights and liberties. That is why the proliferation of commercial surveillance and its exploitation by law enforcement and other government agencies is of such momentous consequence.

Despite these broad implications for society, police use of commercial surveillance currently is shrouded in secrecy. Consumers have little way of telling whether their data has fallen into the hands of law enforcement — indeed, app developers themselves sometimes are unaware of who ultimately receives user data.[13] And, while data brokers often claim that users "consent" to sharing their data through terms of service, the reality is that vanishingly few consumers read these agreements or understand their implications.[14]

More alarming still is the fact that, at present, there are few guardrails in place concerning these practices. Federal legislation to address police use of commercial surveillance has been introduced but has not been enacted.[15] A handful of states have passed comprehensive data privacy laws, but the vast majority have not.[16] And a lack of clarity around the applicability of Fourth Amendment protections to third-party data has led many policing agencies to use such data without obtaining a warrant or court order.[17]

Rulemaking is sorely needed to protect consumers from the excesses of the commercial surveillance industry. For the reasons discussed above, the FTC should be especially attentive to the law enforcement market — indeed, concerns around surveillance are at their apex when governments are surveilling their citizens. By setting common-sense rules around the sale of

---

[13] *See* Burke & Dearen, *supra* note 5.

[14] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U.L. REV. 1498–500 (2019) ("Notions of consent, control, and transparency have dominated data protection discussions for years, and the result is a sea of "I agree" buttons, drop-down menus, and switches that we are unable to navigate. . . . Relying upon consent to justify data practices rests on the dubious assumptions that people understand what they are being told, and we can meaningfully calculate the risk of our choices online and exercise agency through mediated technologies.").

[15] *See* SENATE BILL 1265, 117TH CONGRESS (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/1265.

[16] *See State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGIS., https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (last visited Sept. 30, 2022).

[17] *See* Bennett Cyphers & Aaron Mackey, *Fog Data Science Puts Our Fourth Amendment Rights Up For Sale*, ELECTRONIC FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-data-science-puts-our-fourth-amendment-rights-sale.

sensitive personal data to law enforcement and other government agencies, the FTC could do much to protect consumer privacy and safeguard our civil rights and liberties.

Sincerely,

Kiel Brennan-Marquez
Professor & William T. Golden Scholar
Faculty Director, Center on Community Safety, Policing, and Inequality
University of Connecticut School of Law

Danielle K. Citron
Jefferson Scholars Foundation Schenck Distinguished Professor in Law
Caddell and Chapman Professor of Law
Director, LawTech Center
University of Virginia School of Law

Catherine Crump
Robert Glushko Clinical Professor of Practice in Technology Law
Director, Samuelson Law, Technology and Public Policy Clinic
Co-Director, Berkeley Center for Law & Technology
University of California, Berkeley, School of Law

Andrew Guthrie Ferguson
Professor of Law
American University Washington College of Law

Barry Friedman
Jacob D. Fuchsberg Professor of Law
Affiliated Professor of Politics
Director, Policing Project
New York University School of Law

Woodrow Hartzog
Professor of Law & Class of 1960 Scholar
Boston University School of Law

Maria Ponomarenko
Associate Professor of Law
University of Texas School of Law

Neil Richards
Koch Distinguished Professor in Law
Director, Cordell Institute
Washington University in St. Louis School of Law

Christopher Slobogin
Milton R. Underwood Chair in Law
Director, Criminal Justice Program
Affiliate Professor of Psychiatry
Vanderbilt University Law School

Katherine Jo Strandburg
Alfred B. Engelberg Professor of Law
New York University School of Law

Matthew Tokson
Professor of Law
University of Utah S.J. Quinney College of Law

Ari Ezra Waldman
Professor of Law & Computer Science
Faculty Director, Center for Law, Information and Creativity
Northeastern University