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

E: info@policingproject.org
W: policingproject.org

December 9, 2024

Office of Management and Budget
725 17th St NW
Washington, DC 20503

Submitted electronically at www.regulations.gov

Re: Request for Information: Executive Branch Agency Handling of Commercially Available Information Containing Personally Identifiable Information

The Policing Project at New York University School of Law submits the following comments in response to the Office of Management and Budget's ("OMB") Request for Information regarding executive branch agency handling of commercially available information ("CAI") containing personally identifiable information ("PII") published on October 16, 2024, at 89 Fed. Reg. 83517 ("CAI RFI").

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 CAI RFI, but are especially relevant to the questions set forth in Sections 1 ("How does AI potentially exacerbate privacy risks associated with agency handling of CAI containing PII?"), 1(a) ("What are the key privacy risks associated with agencies' handling of CAI containing PII that OMB should consider and why?") and 14 ("What else should OMB consider when evaluating potential guidance to agencies on ways to mitigate privacy risks from agencies' activities related to CAI containing PII?").

I. Increasingly, policing agencies are using commercial surveillance and CAI 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, including federal 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 intimate activities.[2] One company, Venntel, 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] Federal law enforcement agencies have been shown to engage in similar practices, for example using a tool called Dataminr to surveil protests related to the Israel-Hamas war[8]

---

[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.

[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; Dell Cameron, *The FBI Just Admitted It Bought US Location Data*, WIRED (Mar. 8, 2023), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/.

[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* Jason Leopold, *Federal Surveillance Targeted Israel-Hamas War Protests*, BLOOMBERG (May 3, 2024), https://www.bloomberg.com/news/newsletters/2024-05-03/israel-hamas-war-protesters-targeted-by-dhs-surveillance.

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.[9] Clearview AI's facial recognition software enables police and federal law enforcement to identify individuals by searching against a database of billions of images scraped from websites such as Facebook, YouTube, and Venmo.[10] LexisNexis has assembled over 283 million "dossiers" with information including work history, outstanding debts, purchases, and driving records.[11] And SpyCloud offers police access to data stolen from websites in data breaches, including user passwords and IP addresses.[12] 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.[13] Numerous federal law enforcement agencies including the FBI, ICE, DEA, and TSA routinely purchase CAI containing PII from data brokers.[14]

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 federal law enforcement, for a price.

II. The exploitation of our personal data by federal law enforcement poses grave risks that are exacerbated by AI. 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

[9] *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

[10] *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. Federal law enforcement agencies have purchased contracts to use facial recognition technology as well. *See* Tonya Riley, *Feds' spending on facial recognition tech expands, despite privacy concerns*, CYBERSCOOP (Jan. 10, 2022), https://cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns/.

[11] *See* Hill, *id.*

[12] *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

[13] *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.

[14] *See* Cameron, *supra* note 2; Tewari & Walter-Johnson, *supra* note 3; Sara Morrison, *A surprising number of government agencies buy cellphone location data. Lawmakers want to know why*, VOX (Dec. 2, 2020), https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; *Government Report Shows TSA Violated Privacy Act with Screening Program; Used Passengers' Private Records Without Telling Congress or the Public*, ACLU (July 22, 2005), https://www.aclu.org/press-releases/government-report-shows-tsa-violated-privacy-act-screening-program-used-passengers.

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.

But, in truth, the concerns about privacy go well beyond specific concerns regarding exercises of essential rights. The fact is that very few of us want our entire life to be available to any entity that pays the price for full admission. Yet, that is fast becoming a possibility.

All this is of even greater concern when law enforcement agencies purchase the data. The Supreme Court cautioned quite clearly about the risks of a "too permeating surveillance" that would reveal the "privacies of life."[15] The proliferation of data about our movements, activities, beliefs, and more — available to any government agency with the funds to procure them — presents just such a risk. Police use of CAI, moreover, 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.[16] 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.[17] The notion of consent here is ephemeral at best, and should not be taken seriously.

The glut of data available to police enables them to employ a variety of powerful AI tools that pose significant risks to privacy and other civil rights and liberties. AI tools, powered by CAI and other data, can be used to identify individuals and track their movements and even their associations with others. Though the use of such tools may offer some benefits in the way of public safety, they also pose real risks, including inaccuracy, incursions upon privacy, equity and bias concerns, and misuse.[18]

Despite these issues, there are few guardrails in place concerning the collection and use of CAI. Federal legislation to address police use of commercial surveillance has been introduced but has

[15] *Carpenter v. United States*, 585 U.S. 296, 302 (2018).
[16] *See* Burke & Dearen, *supra* note 5.
[17] *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.").
[18] *See* Policing Project, *Understanding AI Risk*, https://www.policingproject.org/ai-explained-articles/ai-explained/understanding-ai-risk (last visited Nov. 20, 2024).

not been enacted.[19] A handful of states have passed comprehensive data privacy laws, but the vast majority have not.[20]

Moreover, 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, even though the Office of the Director of National Intelligence itself has called this reasoning into question.[21] Agencies often contend that they do not need a warrant to access data they have lawfully purchased. But this conflates two distinct issues: whether police have lawfully *collected* data and whether they may *query* it. The better view is that when sensitive personal data is involved, police should be required to obtain a warrant regardless of how that data ended up in law enforcement hands. After all, tracking a person through their location data is no less intrusive because that data was purchased from a data broker as opposed to subpoenaed from a telecom company.

Indeed, as the Federal Trade Commission said in its official statement accompanying its enforcement action against the data broker Venntel, the data that law enforcement sought to obtain in *Carpenter*, and what it has routinely obtained from data brokers is "basically the same data. In some ways, [Venntel's] data is more invasive."[22] And yet, "*Carpenter* said that to get this data, you need a warrant; Venntel lets them get it without a warrant."[23] The FTC's action is an important step, but it only targets one company; a vast data broker industry continues to offer sensitive personal data on millions of Americans to federal agencies. The present misapplication of Fourth Amendment principles to CAI makes the regulation of this data all the more urgent.

Agency action is sorely needed to protect Americans from the excesses of the commercial surveillance industry. By setting common-sense rules around the sale of sensitive personal data to law enforcement and other government agencies, OMB could do much to protect privacy and safeguard our civil rights and liberties.

---

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

[20] *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).

[21] *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; OFF. OF THE DIR. OF NAT'L INTEL., SENIOR ADVISORY GRP., PANEL ON COMMERCIALLY AVAILABLE INFO., REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE 2 (2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf.

[22] Statement of Comm'r Alvaro M. Bedoya, Joined by Chair Lina M. Khan & Comm'r Rebecca Kelly Slaughter in Full & Comm'r Melissa Holyoak in Part I, *In re Gravy Analytics, Inc. & Venntel, Inc.* at 4, (Dec. 2, 2024), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-commissioner-alvaro-m-bedoya-joined-chair-lina-m-khan-commissioner-rebecca-kelly-slaughter-3.

[23] *Id.* at 5.

Sincerely,

Max Isaacs
Director of Technology Law & Policy
Policing Project at New York University School of Law

Jesse Woo
AI/Tech Policy Counsel
Policing Project at New York University School of Law