

ORAL ARGUMENT NOT YET SCHEDULED

No. 26-1049

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ANTHROPIC PBC,

Petitioner,

v.

U.S. DEPARTMENT OF WAR,

PETER B. HEGSETH, in his official capacity as Secretary of War,

Respondents.

*On Petition for Judicial Review of
Department of War 41 U.S.C. § 4713 Notice*

**UNOPPOSED MOTION OF THE AMERICAN CIVIL LIBERTIES
UNION AND THE CENTER FOR DEMOCRACY AND TECHNOLOGY
FOR LEAVE TO FILE BRIEF AS AMICI CURIAE IN SUPPORT OF
PRELIMINARY RELIEF**

The American Civil Liberties Union Foundation (“ACLU”) and the Center for Democracy and Technology (“CDT”) respectfully move this Court for leave to file the attached brief as amici curiae in support of preliminary relief. Counsel for proposed amici curiae conferred with parties’ counsel regarding this motion. Petitioner consents to the filing of the proposed brief and Respondents take no position.

Proposed amici seek to address the importance of Anthropic’s advocacy for guardrails related to the use of artificial intelligence (“AI”) to conduct domestic surveillance. The brief describes the breadth of data collection by the Department of War and other agencies; the dangers posed by AI tools when applied to these immense datasets containing sensitive information—including how these tools can invade privacy, chill speech, and facilitate discriminatory profiling; why existing law is inadequate to protect people in the United States from this surveillance; and why, as a result, Anthropic’s advocacy for strict limitations on the government’s use of AI is critical. The attached brief is substantially different from any other brief submitted by the parties or other known amici, and it would assist the Court in evaluating Anthropic’s motion for preliminary relief by contextualizing the speech at issue.

This Court should exercise its broad discretion to permit proposed amici to appear given their unique expertise and interest in this matter. The ACLU is a nationwide, nonprofit, nonpartisan organization with more than 1.5 million members dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. CDT is a nonpartisan nonprofit organization that shapes technology policy, governance, and design with a focus on equity and democratic values. The ACLU and CDT share a longstanding commitment to protecting civil liberties in the digital age. Proposed amici have

appeared before federal courts in numerous cases implicating civil liberties, national security, and mass domestic surveillance, including as counsel in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), *Wikimedia Foundation v. National Security Agency*, 857 F.3d 193 (4th Cir. 2017), and as amicus in *United States v. Chatrue*, 136 F.4th 100 (4th Cir. 2025), *cert. granted in part*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).

All the requirements for the filing of an amici curiae brief are satisfied. No party will be prejudiced by this filing and it is filed within the time limits set by Federal Rule of Appellate Procedure 29(a)(6). No party's counsel authored this brief in whole or in part, and no person other than amici curiae, their members, or their counsel made a monetary contribution to its preparation or submission.

Proposed amici respectfully request this Court's leave to appear as amici curiae and to deem the accompanying proposed brief filed.

Dated: March 16, 2026

Samir Jain
Jake Laperruque
Greg Nojeim
CENTER FOR DEMOCRACY &
TECHNOLOGY
1401 K Street, NW, Suite 200

Respectfully submitted,

/s/ Ashley Gorski
Ashley Gorski
Patrick Toomey
Charlie Hogle
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004

Washington, DC 20005
sjain@cdt.org

Tel.: (212) 549-2500
Fax: (332) 234-9528
agorski@aclu.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
425 California Street, Suite 700
San Francisco, CA 94104
jgranick@aclu.org

Counsel for Amici Curiae

ADDENDUM**CERTIFICATE OF PARTIES, RULINGS, AND RELATED CASES**

Pursuant to Circuit Rule 27(a)(4), undersigned counsel certifies the following:

Parties and Amici. Undersigned counsel are not aware of any other parties, intervenors, or amici appearing before this Court other than those listed in Addendum A to the Petitioner's Emergency Motion for Stay Pending Review, or those disclosed by other amici to date.

Rulings Under Review. References to the rulings at issue appear in Addendum A to the Petitioner's Emergency Motion for Stay Pending Review.

Related Cases. Undersigned counsel are unaware of any other related cases within the meaning of Circuit Rule 28(a)(1)(C).

DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the undersigned states that no party to the proposed brief of amici curiae is a publicly held corporation, issues stock, or has a parent corporation.

Dated: March 16, 2026

/s/ Ashley Gorski

Ashley Gorski

Counsel for Proposed Amici Curiae

CERTIFICATES OF COMPLIANCE AND SERVICE

1. This motion complies with the length limits and type-face and type-style requirements of Federal Rules of Appellate Procedure 27(d) and 32(a)(5)–(6) as it contains 461 words and was prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

2. On March 16, 2026, I filed this motion and the attached proposed brief with the Clerk of this Court via the CM/ECF system. All participants in the case are registered CM/ECF users, and service will be accomplished through that system.

Dated: March 16, 2026

/s/ Ashley Gorski

Ashley Gorski

Counsel for Proposed Amici Curiae

ORAL ARGUMENT NOT YET SCHEDULED

No. 26-1049

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ANTHROPIC PBC,

Petitioner,

v.

U.S. DEPARTMENT OF WAR,
PETER B. HEGSETH, in his official capacity as Secretary of War,*Respondents.*

*On Petition for Judicial Review of
Department of War 41 U.S.C. § 4713 Notice*

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION
AND CENTER FOR DEMOCRACY AND TECHNOLOGY
IN SUPPORT OF PRELIMINARY RELIEF**

Samir Jain
Jake Laperruque
Greg Nojeim
CENTER FOR DEMOCRACY &
TECHNOLOGY
1401 K Street, NW, Suite 200
Washington, DC 20005
sjain@cdt.org

Ashley Gorski
Patrick Toomey
Charlie Hogle
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
Fax: (332) 234-9528
agorski@aclu.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

425 California Street, Suite 700
San Francisco, CA 94104
jgranick@aclu.org

Counsel for Amici Curiae

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to Federal Rule of Appellate Procedure 26.1(a) and Circuit Rule 28(a)(1), undersigned counsel certifies the following:

Parties and Amici. Undersigned counsel are not aware of any other parties, intervenors, or amici appearing before this Court other than those listed in Addendum A to the Petitioner's Emergency Motion for Stay Pending Review, or those disclosed by other amici to date.

Rulings Under Review. References to the rulings at issue appear in Addendum A to the Petitioner's Emergency Motion for Stay Pending Review.

Related Cases. Undersigned counsel are unaware of any other related cases within the meaning of Circuit Rule 28(a)(1)(C).

Dated: March 16, 2026

/s/ Ashley Gorski

Ashley Gorski

Counsel for Amici Curiae

**STATEMENT REGARDING CONSENT TO FILE AND CERTIFICATE
REGARDING SEPARATE BRIEFING**

Pursuant to Circuit Rule 29(b), counsel of record for all parties have been notified of amici's intent to file this brief. Petitioner consents and Respondents take no position.¹

Pursuant to Circuit Rule 29(d), undersigned counsel certifies that a separate brief is necessary. Amici are nonprofit, nonpartisan organizations with expertise on U.S. privacy law, government surveillance, and the development and deployment of AI technologies. Their brief addresses the dangers to privacy and civil liberties posed by AI tools when applied to datasets containing Americans' sensitive information; why U.S. law does not adequately address the use of AI for surveillance; and why, as a result, Anthropic's advocacy for AI guardrails is critical to protecting the public's privacy interests. This brief is substantially different from any other brief submitted by Petitioner or other known amici.

Dated: March 16, 2026

/s/ Ashley Gorski

Ashley Gorski

Counsel for Amici Curiae

¹ No party or party's counsel authored this brief in whole or in part, and no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief. No person other than amicus or his counsel contributed money that was intended to fund the preparation or submission of this brief.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, amici state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

Dated: March 16, 2026

/s/ Ashley Gorski

Ashley Gorski

Counsel for Amici Curiae

TABLE OF CONTENTS

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES	i
STATEMENT REGARDING CONSENT TO FILE AND CERTIFICATE REGARDING SEPARATE BRIEFING	ii
CORPORATE DISCLOSURE STATEMENT	iii
TABLE OF AUTHORITIES	vi
GLOSSARY	xi
IDENTITIES AND INTERESTS OF AMICI CURIAE	1
INTRODUCTION AND SUMMARY OF ARGUMENT	2
ARGUMENT	3
I. AI tools, especially when applied to bulk data, enable extraordinarily intrusive surveillance.	3
A. The government acquires Americans’ sensitive data in vast quantities.	4
1. Government agencies buy Americans’ sensitive data from commercial brokers.	4
2. Government agencies engage in other forms of sweeping surveillance and data collection.	9
B. AI tools promise to make this surveillance even more intrusive by allowing the government to track Americans’ movements, monitor their speech, and profile individuals at scale.	11
II. Existing legal frameworks for surveillance fail to provide Americans with adequate privacy protection.	15
A. U.S. statutory law does not prohibit government agencies from purchasing data about Americans that would otherwise require a warrant or court order to obtain.	16

B. Intelligence agencies take a narrow view of constitutional protections for publicly available data and data shared with third parties.....18

C. The government regularly seeks to exploit loopholes in U.S. privacy laws to justify sweeping surveillance.21

D. Enforcement mechanisms for existing legal protections are also weak and susceptible to abuse.25

III. Anthropic’s advocacy for surveillance guardrails around AI addresses a matter of immense public concern.28

CONCLUSION30

TABLE OF AUTHORITIES

Cases

<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	16, 19, 20
<i>Clapper v. Amnesty Int’l USA</i> , 568 U.S. 398 (2013).....	27
<i>Leaders of a Beautiful Struggle v. Balt. Police Dep’t</i> , 2 F.4th 330 (4th Cir. 2021)	7
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	6, 19
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	19
<i>United States v. Jones</i> , 565 U.S. 400 (2012).....	7
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	19
<i>Wikimedia Found. v. NSA</i> , 14 F.4th 276 (4th Cir. 2021)	27

Statutes

18 U.S.C. §§ 2701-13.....	17
50 U.S.C. § 1801	17, 24
50 U.S.C. § 1862.....	22
50 U.S.C. § 1881a.....	23

Other Authorities

ACLU, PCLOB Comment Regarding Surveillance Activities Governed by EO 12333 (Jan. 13, 2016)	25
Amicus Br. of Congressman F. James Sensenbrenner, Jr., <i>ACLU v. Clapper</i> , No. 13-cv-03994 (S.D.N.Y. Sept. 4, 2013) (ECF No. 46-1)	22
Amodei, Dario, <i>The Adolescence of Technology: Confronting and Overcoming the Risks of Powerful AI</i> (Jan. 2026).....	15
Ball, James, <i>NSA collects millions of text messages daily in ‘untargeted’ global sweep</i> , <i>The Guardian</i> (Jan. 16, 2014)	11
Caputo, Marc, <i>Scoop: State Dept. to Use AI to Revoke Visas of Foreign Students Who Appear “Pro-Hamas,”</i> <i>Axios</i> (Mar. 6, 2025)	14
Cox, Joseph, <i>Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees</i> , <i>VICE</i> (May 17, 2023)	13
Cox, Joseph, <i>How the U.S. Military Buys Location Data from Ordinary Apps</i> , <i>VICE</i> (Nov. 16, 2020).....	6
Cox, Joseph, <i>ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day</i> , <i>404Media</i> (Sep. 30, 2025)	5
Cox, Joseph, <i>Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics</i> , <i>404Media</i> (Oct. 23, 2024).....	6
Cyphers, Bennett, <i>How the Federal Government Buys Our Cell Phone Location Data</i> , <i>Electronic Frontier Foundation</i> (June 13, 2022)	6
Devereaux, Ryan et al., <i>The NSA Is Recording Every Cell Phone Call in the Bahamas</i> , <i>The Intercept</i> (May 19, 2014)	11
DHS, <i>2020-2021 Data Mining Report</i> (Aug. 2022)	13
DHS, <i>Artificial Use Case Inventory—Customs and Border Protection: Port of Entry Risk Assessments</i>	13

DIA, <i>Clarification of Information Briefed During DIA’s 1 December Briefing on CTD</i> (Jan. 15, 2021)	5, 20
DoD Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities (2016)	17, 24
DOJ, <i>Attachment B—Statement of Work, FBI Directorate of Intelligence Social Media Exploitation Tool</i> (Jan. 21, 2022)	10
Frenkel, Sheera et al., <i>How Talks Between Anthropic and the Defense Dept. Fell Apart</i> , N.Y. Times (Mar. 1, 2026)	24
Gellman, Barton & Ashkan Soltani, <i>NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say</i> , Wash. Post (Oct. 30, 2013)	11
Gellman, Barton & Ashkan Soltani, <i>NSA tracking cellphone locations worldwide, Snowden documents show</i> , Wash. Post (Dec. 4, 2013)	10
Hendrix, Justin, <i>DHS AI Surveillance Arsenal Grows as Agency Defies Courts</i> , Tech Policy Press (Feb. 1, 2026)	14
ICE, <i>AI Use Cases: Enhanced Lead Identification and Targeting</i> (2025)	13
Jaffer, Jameel & Brett Max Kaufman, <i>How to Decode the True Meaning of What NSA Officials Say</i> , Slate (July 31, 2013)	21
Letter from Gen. Paul M. Nakasone to Sen. Ron Wyden (Dec. 11, 2023)	8
Letter from Sen. Ron Wyden to Avril Haines, Dir. of Nat’l Intelligence (Jan. 25, 2024)	6
Letter from Under Sec. of Def. Ronald S. Moultrie to Sen. Ron Wyden (Dec. 11, 2023)	5, 20
MacMillan, Douglas et al., <i>Arrested by AI: Police ignore standards after facial recognition matches</i> , Wash. Post (Jan. 13, 2025)	15

National Security Commission on Artificial Intelligence, Final Report (2021).....	13
Off. of the Dir. of Nat'l Intel., Intelligence Community Policy Framework for Commercially Available Information (2024).....	18
Off. of the Dir. of Nat'l Intel., Senior Advisory Group, Panel on Commercially Available Information (Jan. 27, 2022).....	8, 9, 20
Off. of C.L., Priv., and Transparency, <i>Annual Statistical Transparency Report</i> , Off. of the Dir. of Nat'l Intel. (2024).....	23
Press Release, Sen. Ron Wyden, <i>Government Watchdogs Must Investigate Warrantless Purchases of Americans' Internet Browsing Data by Federal Agencies</i> (Sept. 21, 2022)	7
<i>Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act</i> , Privacy and Civil Liberties Oversight Board (July 2, 2014)	23
<i>Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act</i> , Privacy and Civil Liberties Oversight Board (Jan. 23, 2014).....	22
Savage, Charlie, <i>Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants</i> , Memo Says, N.Y. Times (Jan. 22, 2021)	25
Savage, Charlie, <i>Power Wars: Inside Obama's Post-9/11 Presidency</i> (2011).....	26
Shiffman, John & Kristina Cooke, <i>U.S. Directs Agents to Cover Up Program Used to Investigate Americans</i> , Reuters (Aug. 5, 2013).....	27
<i>Statement from Dario Amodei on our discussions with the Department of War</i> , News, Anthropic.com (Feb. 26, 2026)	21, 28, 29
Taitz, Sarah & Patrick Toomey, <i>Concealing Surveillance: The Government's Disappearing Section 702 Notices</i> , Just Security (Sept. 27, 2023).....	27

Tau, Byron & Garance Burke, *Border Patrol is Monitoring US drivers and Detaining Those with ‘Suspicious’ Travel Patterns*, Associated Press (Nov. 20, 2025)13

Tau, Byron, *U.S. Spy Agencies Know Your Secrets. They Bought Them.*, Wall St. J. (Mar. 8, 2024)5, 8

Venkatesh, Anika & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026).....8

Wang, Nina et al., *American Dragnet: Data-Driven Deportation in the 21st Century*, Geo. L. Ctr. on Priv. & Tech. (May 10, 2022).....8

GLOSSARY

AI.....Artificial Intelligence

CBP Customs and Border Protection

CIA..... Central Intelligence Agency

DHS Department of Homeland Security

DIA..... Defense Intelligence Agency

DoD Department of Defense

DoW Department of War

FBI.....Federal Bureau of Investigation

FISA Foreign Intelligence Surveillance Act

ICE Immigration and Customs Enforcement

NSA National Security Agency

ODNI.....Office of the Director of National Intelligence

PCLOB Privacy and Civil Liberties Oversight Board

SCA Stored Communications Act

IDENTITIES AND INTERESTS OF AMICI CURIAE

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with more than 1.5 million members dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The ACLU has a longstanding commitment to protecting civil liberties in the digital age, and it has appeared before federal courts in numerous cases implicating civil liberties and mass domestic surveillance, including as counsel in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), *American Civil Liberties Union v. Clapper*, 785 F.3d 787 (2d Cir. 2015), and *Wikimedia Foundation v. National Security Agency*, 857 F.3d 193 (4th Cir. 2017).

The Center for Democracy and Technology (“CDT”) is a nonprofit, nonpartisan, public interest organization that, for over 30 years, has worked to promote the constitutional and democratic values of privacy, equality, free expression, and individual liberty in the digital age. CDT regularly advocates before the courts, legislatures, and regulatory agencies for laws and policies that protect against invasive and unwarranted government surveillance.

INTRODUCTION AND SUMMARY OF ARGUMENT

Anthropic has been an outspoken advocate for AI guardrails, including limits on the use of its own AI tools for mass domestic surveillance and fully autonomous lethal weapons. Anthropic's constitutionally protected advocacy highlights vital societal questions about the government's adoption of AI tools for surveillance and warfare. Amici write to underscore three issues related to this advocacy and the government's response: (1) the privacy-invading dangers posed by AI tools when applied to bulk datasets containing Americans' sensitive information; (2) why U.S. law is inadequate to protect Americans from this surveillance; and (3) why, as a result, Anthropic's push for strict limitations on the government's use of AI is critical to protecting the public's privacy interests. Given the dangers of AI-enabled surveillance, Anthropic's public commitment to AI guardrails is laudable. Yet the Department of War ("DoW"), in response, has not merely declined to sign a deal with the company, but has punished Anthropic for its stance.¹

AI tools, especially when applied to the immense quantities of sensitive data purchased or otherwise collected by government agencies, can enable

¹ For brevity, this brief uses "Americans" to refer to people in the United States and U.S. persons abroad. Although Anthropic's advocacy related to fully autonomous weapons is a matter of significant public importance, that issue is beyond the scope of this brief.

extraordinarily intrusive surveillance. These tools have the potential to map the intimate details of every American’s life in ways never before possible—shattering expectations of privacy, limiting freedom of association, facilitating discrimination, and rending the social fabric of this country in the process.

Although DoW insists that it seeks to deploy AI tools only for “lawful” uses, that is cold comfort. Privacy laws in the United States lag decades behind the technology and leave enormous gaps in protection. DoW and other government agencies “lawfully” collect Americans’ data in bulk, including through commercial data purchases and surveillance that operate outside of any statutory framework or court oversight. Against this backdrop, Anthropic and other AI companies have every reason and every right to speak out about the dangers of using AI to conduct mass surveillance.

ARGUMENT

I. AI tools, especially when applied to bulk data, enable extraordinarily intrusive surveillance.

The government, including DoW, buys and collects immense quantities of Americans’ sensitive data. Even before the adoption of AI tools, the government’s collection and use of this data resulted in significant privacy harms. But AI promises to make these privacy intrusions far worse: these systems can integrate disparate types of structured and unstructured data, automate searches across ever-larger datasets, and distill the privacies of life from that data—at a speed and scale

that human analysts never could match. AI can enable surveillance that is not merely a degree more efficient, but is orders of magnitude more comprehensive, more detailed, and more intrusive than ever before. Statutory law does not provide meaningful protection from this surveillance, and constitutional decisions have yet to catch up to technological realities.

A. The government acquires Americans' sensitive data in vast quantities.

1. Government agencies buy Americans' sensitive data from commercial brokers.

Government agencies, including DoW, buy Americans' sensitive data in bulk. Generally speaking, the process works as follows: When we carry smartphones, use apps, and otherwise access the internet, we create data. That data can reveal exceedingly personal information about us—our locations over time, our race, ethnicity, gender, income, sexual proclivities, reproductive health, religious practice, political affiliations, and more. Commercial brokers compile this data from apps, websites, credit bureaus, public records, and other sources. They use it to create detailed individual profiles, which they then sell.

The U.S. government is a major customer. While agencies' contracts with data brokers are not always public or advertised, reporting shows that they spend millions of dollars for access to enormous repositories of individuals' sensitive

data.² To quote Michael Morell, former deputy director of the CIA, “The information that is available commercially would kind of knock your socks off.”³ “If we collected it using traditional intelligence methods, it would be top secret sensitive. And you wouldn’t put it in a database, you’d keep it in a safe.” *Id.*

DoW is no exception. Take one component, the Defense Intelligence Agency (“DIA”). In a now-unclassified memorandum, DIA acknowledged that it had been purchasing U.S. smartphone location data for two-and-a-half years.⁴ The agency explained that it identifies “U.S. location data points” and stores them in a dedicated database.⁵ To “query” the U.S. location database, DIA policy requires only internal approval from agency officials.⁶

DIA is no outlier—other DoW components also purchase and use location data harvested from domestic smartphones. For instance, U.S. Special Operations

² See, e.g., Joseph Cox, *ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day*, 404Media (Sep. 30, 2025), <https://perma.cc/2SPS-TZGY>.

³ Byron Tau, *U.S. Spy Agencies Know Your Secrets. They Bought Them.*, Wall St. J. (Mar. 8, 2024), <https://perma.cc/3X7V-DBQG>.

⁴ DIA, *Clarification of Information Briefed During DIA’s 1 December Briefing on CTD*, at 1 (Jan. 15, 2021), <https://perma.cc/BR4Z-8GYH> (“DIA Memo”).

⁵ *Id.*

⁶ *Id.*; see also Letter from Under Sec. of Def. Ronald S. Moultrie to Sen. Ron Wyden (Dec. 11, 2023), at 4 (confirming that “Defense Intelligence Components” purchase “location data from phones located in the United States”), <https://perma.cc/PF8E-Z5DS> (“Moultrie Letter”).

Command bought access to a product known as “Locate X” which gathers location data, including from U.S. smartphones. Locate X enables users to “draw a shape on a map, see all [tracked] devices [] in that location, and then follow a specific device around to see where else it has been.”⁷

The military has also acquired Americans’ smartphone location data from “X-Mode.” X-Mode developed a package of code and paid developers to embed it in their smartphone apps.⁸ When apps with this code collected location data, including on U.S. users, they sent it directly to X-Mode.⁹ X-Mode then sold the data from these apps—which included a weather app and popular Muslim prayer and dating apps—to “U.S. military customers.”¹⁰

A person’s location data is extraordinarily sensitive. It can reflect “a wealth of detail about her familial, political, professional, religious, and sexual associations.” *Riley v. California*, 573 U.S. 373, 396 (2014) (quoting *United States*

⁷ Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), <https://perma.cc/4VBR-7T6N> (“*Ordinary Apps*”); Joseph Cox, *Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics*, 404Media (Oct. 23, 2024), <https://perma.cc/JKL8-38AX>.

⁸ Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, Electronic Frontier Foundation (June 13, 2022), <https://perma.cc/S99L-LN6W>.

⁹ *Id.*

¹⁰ Letter from Sen. Ron Wyden to Avril Haines, Dir. of Nat’l Intelligence (Jan. 25, 2024), at 2, <https://perma.cc/KAE2-U5P3>.

v. Jones 565 U.S. 400, 415 (Sotomayor, J., concurring)). Location tracking may expose the visit to “the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.” *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). “[E]ven just a few points of . . . location history” can reveal a person’s “unique and habitual” movements, so much so that “it is almost always possible to identify people by observing even just a few points of their location history.” *Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 2 F.4th 330, 343-44 (4th Cir. 2021) (en banc) (citing study showing that “identity is easy to deduce from just a few random points of an individual’s movements,” and explaining that “common sense and ample authority over the last decade corroborates this conclusion”).

But location data is only part of the story. Components of the Department of War—DIA, the National Security Agency (“NSA”), U.S. Cyber Command, the Naval Criminal Investigative Services, and the Defense Counterintelligence and Security Agency—have also purchased access to Americans’ “netflow” records, which can reveal a person’s web-browsing activity.¹¹ And the Office of the

¹¹ Press Release, Sen. Ron Wyden, *Government Watchdogs Must Investigate Warrantless Purchases of Americans’ Internet Browsing Data by Federal Agencies* (Sept. 21, 2022), <https://perma.cc/UTK6-P4DX>; see Letter from Gen. Paul M.

Director of National Intelligence (“ODNI”) has described how commercial data can be obtained from “cookies and other methods . . . that track end users as they browse the Internet.”¹²

Purchasing mountains of Americans’ sensitive data from commercial brokers is hardly unique to the U.S. military: other government agencies do the same, including the Department of Homeland Security (“DHS”), the Internal Revenue Service, the Drug Enforcement Agency, and the Federal Bureau of Investigation.¹³ Immigration and Customs Enforcement (“ICE”) and Customs and Border Protection (“CBP”), for instance, have purchased Americans’ smartphone location data en masse from commercial brokers.¹⁴ In the same vein, ICE has also used state, local, and commercial databases to profile millions of U.S. residents using their utility records, driver’s licenses, and license plates.¹⁵

Nakasone to Sen. Ron Wyden (Dec. 11, 2023), at 1-2, <https://perma.cc/ZN9F-MTNT>.

¹² ODNI, Senior Advisory Group, Panel on Commercially Available Information at 5 (Jan. 27, 2022), <https://bit.ly/4lxJ9Tx> (“ODNI Report”).

¹³ See, e.g., Tau, *U.S. Spy Agencies Know Your Secrets. They Bought Them.*, *supra* n.3.

¹⁴ See, e.g., Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), <https://perma.cc/N9EB-XX9J>.

¹⁵ See, e.g., Nina Wang et al., *American Dragnet*, Geo. L. Ctr. on Priv. & Tech., at 1-2 (May 10, 2022), <https://perma.cc/SL8L-YPRH>.

Taken together, these massive commercial datasets allow agencies across the government to intrude into the most intimate details of people’s lives, and to do so absent any independent authorization or oversight. Even ODNI has recognized that commercial data “increases [the government’s] power,” “implicates civil liberties,” and “can be misused to pry into private lives.”¹⁶ As ODNI observed, “[t]he government would never have been permitted to compel billions of people to carry location tracking devices on their persons at all times, to log and track most of their social interactions, or to keep flawless records of all their reading habits. Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect[.]”¹⁷

2. Government agencies engage in other forms of sweeping surveillance and data collection.

In addition to data purchases, government agencies conduct still other types of large-scale data collection. For example, they surveil information that Americans and others post on the public internet, including on social media. The FBI, DHS, and CBP have each purchased access to a social media monitoring platform that can “pair keyword searches with geospatial capabilities to view all social media postings for a specific area,” “monitor feeds on an active and

¹⁶ ODNI Report, *supra* n.12, at 11, 13.

¹⁷ *Id.* at 13.

continuous basis,” “view connections between subject/posters, the subject’s network, linked accounts, catalogs of friends, follower lists, and biographical details,” and “provide sentiment analysis, including emotion analysis, using word lists or natural language processing, to be able to determine likely attitudes of the targets.”¹⁸

In addition to domestic collection of social media posts, intelligence agencies collect private communications and data in bulk from abroad, including the communications and data of Americans. Under Executive Order 12,333, the NSA conducts a wide array of warrantless surveillance programs outside of the United States. While much of this collection is ostensibly directed at people abroad, vast quantities of Americans’ communications are nonetheless captured in the process, as Americans’ data is routinely sent, routed, or stored abroad. For example, according to news reports as far back as 2013, the NSA has:

- Collected nearly 5 billion records per day on the locations of cell phones, including those of Americans;¹⁹

¹⁸ Department of Justice, *Attachment B—Statement of Work, FBI Directorate of Intelligence Social Media Exploitation Tool*, at 5-6 (Jan. 21, 2022), <https://perma.cc/2L2Q-VRHP>.

¹⁹ Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, Wash. Post (Dec. 4, 2013), <https://perma.cc/8NFD-LJZD>.

- Collected nearly 200 million text messages daily;²⁰
- Intercepted data from Google and Yahoo user accounts as that information traveled between data centers abroad;²¹
- Recorded and stored every cell phone call in, into, and out of at least two countries, including the Bahamas.²²

While these examples are staggering, they are likely only the tip of the iceberg as the government's data collection has expanded over time, providing the raw material for today's AI-powered surveillance tools.

B. AI tools promise to make this surveillance even more intrusive by allowing the government to track Americans' movements, monitor their speech, and profile individuals at scale.

The government's bulk collection of Americans' sensitive data is itself a privacy intrusion. But the application of AI tools to these datasets could result in far more severe and widespread intrusions—facilitating the monitoring of everyone's movements, speech, and associations; enabling the profiling and watchlisting of individuals with unpopular views; furthering discriminatory

²⁰ James Ball, *NSA collects millions of text messages daily in 'untargeted' global sweep*, The Guardian (Jan. 16, 2014), <https://perma.cc/AMJ4-JDQS>.

²¹ Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, Wash. Post (Oct. 30, 2013), <https://perma.cc/EN4Q-Z3NH>.

²² Ryan Devereaux et al., *The NSA Is Recording Every Cell Phone Call in the Bahamas*, The Intercept (May 19, 2014), <https://perma.cc/3KY6-3GTX>.

investigations and prosecutions of disfavored populations; and completely upending traditional expectations of privacy. These harms are not theoretical. Even today, AI tools can synthesize disparate data streams, analyze that data, and provide comprehensive, detailed outputs at the touch of a button—allowing the government to track people, map contact networks, draw inferences, establish standard patterns and flag any “suspicious” deviations from them, and build dossiers far more efficiently than human analysts ever could.

As the scope of government data collection continues to increase, so too will the threat that AI-powered tools pose to Americans’ privacy. Datasets that previously would have required dozens of analysts weeks or months to pour through can be digested in moments. Large language models and other AI technology can also effectively combine and make sense of distinct data formats, digesting geolocation data, web browsing records, social media posts, and more to create comprehensive pictures of our lives—where we work, where we worship, where our kids go to school, who we associate with, and what we say online.

As just one example of how AI today can accelerate and broaden government surveillance: the government may purchase a large dataset containing the movements of thousands of cellphones, but those trails may not have names or phone numbers assigned to them. AI can connect names with devices faster than

any human, while integrating other categories of information for an even more robust picture of a person's life. And it can do this work at scale.

Indeed, AI tools are already being used by intelligence agencies to analyze the vast volumes of data they acquire. Agencies like the NSA, CIA, and FBI are pursuing “ubiquitous AI integration in each stage of the intelligence cycle.”²³ These agencies are seeking to use AI to help select surveillance targets, identify people whose communications are intercepted, and analyze the vast amounts of data they collect.²⁴ Similarly, DHS and ICE use AI to identify leads for immigration enforcement and select targets for intelligence, risk assessments, and watchlisting.²⁵ And CBP uses a predictive intelligence program to analyze drivers' travel patterns at scale and to flag vehicles deemed “suspicious” for agents to stop and search.²⁶

²³ National Security Commission on Artificial Intelligence, Final Report at 110 (2021), <https://perma.cc/FQ5H-ZGEH>.

²⁴ *Id.* at 108-10, 143-45.

²⁵ *See id.* at 109, 112; Joseph Cox, *Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees*, VICE (May 17, 2023), <https://perma.cc/M6MX-9A4V>; DHS, *Artificial Use Case Inventory—Customs and Border Protection: Port of Entry Risk Assessments*, <https://perma.cc/RCP2-VZWJ>; DHS, *2020-2021 Data Mining Report*, at 26 (Aug. 2022), <https://perma.cc/9K6P-GUHG>; ICE, *AI Use Cases: Enhanced Lead Identification and Targeting* (2025), <https://perma.cc/VF4J-QLCA>.

²⁶ Byron Tau & Garance Burke, *Border Patrol is Monitoring US drivers and Detaining Those with ‘Suspicious’ Travel Patterns*, Associated Press (Nov. 20, 2025), <https://perma.cc/Z4RC-Q6NK>.

Government agencies also use AI tools to hunt for disfavored speech online. For example, the State Department uses AI tools to monitor and review online speech and social media posts, looking for people who express “alleged terrorist sympathies.”²⁷ DHS, in the meantime, is acquiring AI tools that allow it to conduct “fine-grained social media searches” and to find a person’s online accounts and digital identifiers.²⁸ This ability—to make connections across digital domains, building an ever-more-comprehensive picture of a person’s speech and associations—is part of how AI tools are transforming surveillance.

The deployment of AI systems for surveillance, watchlisting, border searches, biometric identification, and immigration vetting will automate and expand some of the government’s most intrusive, damaging, and secretive programs. These activities disproportionately impact U.S. communities that have long faced discrimination, such as immigrants and racial and religious minorities. As in areas like policing and the criminal legal system, the use of AI for “national

²⁷ Marc Caputo, *Scoop: State Dept. to Use AI to Revoke Visas of Foreign Students Who Appear “Pro-Hamas,”* Axios (Mar. 6, 2025), <https://perma.cc/UR78-V3FV>.

²⁸ Justin Hendrix, *DHS AI Surveillance Arsenal Grows as Agency Defies Courts,* Tech Policy Press (Feb. 1, 2026), <https://perma.cc/SE4T-PNC7>.

security” purposes could easily perpetuate racial, ethnic, and religious profiling, while more broadly endangering civil rights and civil liberties.²⁹

At the same time, using AI tools for this kind of analysis and profiling can pose other dangers, as the systems can catastrophically fail. As just one example, widespread use of AI-driven face recognition technology by police has led to grave errors. At least 12 people are now publicly known to have been wrongfully arrested in the United States as a result of police reliance on face recognition technology that misidentified individuals.³⁰ Indeed, Anthropic has said its tools are not suited for the surveillance for which the government wants to use them—underscoring that using AI in domestic surveillance is dangerous not just when the technology works, but also when agencies seek to stretch it beyond its capabilities.

II. Existing legal frameworks for surveillance fail to provide Americans with adequate privacy protection.

Anthropic’s public statements have highlighted just how far U.S. privacy laws lag behind these powerful new technologies, and why the government’s

²⁹ See Dario Amodei, *The Adolescence of Technology: Confronting and Overcoming the Risks of Powerful AI* (Jan. 2026), <https://perma.cc/RVY7-HY98> (noting that “[i]t might be frighteningly plausible to simply generate a complete list of anyone who disagrees with the government on any number of issues” and that AI could “detect pockets of disloyalty forming, and stamp them out before they grow”).

³⁰ See, e.g., Douglas MacMillan et al., *Arrested by AI: Police ignore standards after facial recognition matches*, Wash. Post (Jan. 13, 2025), <https://perma.cc/43AZ-FYQT>.

“lawful” use of AI tools could easily result in mass domestic surveillance, with catastrophic consequences. Amici agree. The first problem is the lack of legal rules regulating the government’s purchases of Americans’ sensitive data—the raw material often fed into AI systems. On top of that, DoW components take an extremely narrow view of constitutional protections, insisting that decisions like *Carpenter v. United States*, 585 U.S. 296 (2018), do not restrict their ability to conduct surveillance that reveals a comprehensive picture of a person’s movements or pattern of life. Finally, existing privacy laws are filled with loopholes that the government has long exploited to justify sweeping surveillance and are notoriously difficult to enforce. For all these reasons, Anthropic’s advocacy for specific AI guardrails is warranted. Existing laws simply do not provide reliable protection against AI-powered mass domestic surveillance.

A. U.S. statutory law does not prohibit government agencies from purchasing data about Americans that would otherwise require a warrant or court order to obtain.

Federal law guarding Americans’ privacy from intrusive government surveillance provides insufficient protection against the purchase of commercially available data. Many of these laws predate the rise of the public-facing internet, commercial surveillance, and the data brokerage industry described above. And this is exactly why a contract permitting “all lawful uses” of AI tools, as the government demands, is inadequate to protect the public’s privacy interests.

Chief among these laws is the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-13, passed in 1986. The SCA limits governmental access to some data by requiring that agencies obtain a warrant, court order, or subpoena to obtain it. *Id.* §§ 2702-2703. Those limitations, however, apply only to demands for certain types of data from providers of “electronic communication services” or “remote computing services”—not data brokers.

DoW maintains that these purchases also fall outside of the scope of the Foreign Intelligence Surveillance Act (“FISA”), which regulates several types of surveillance and physical searches, but not explicitly government purchases from data brokers. *See* 50 U.S.C. § 1801 *et seq.*

Agency policies do not fill the gaps in federal law. Although DoW and intelligence agencies have some policies governing the use of commercially available information, the protections are extremely modest, laden with loopholes, and largely unenforceable. For example, a 2016 DoW policy manual expressly *permits* the intentional collection of “publicly available” “U.S. person information” if the information is “reasonably believed to be necessary” for a Department function.³¹ This is a vague and modest restriction at best, and it is unclear whether

³¹ DoD Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities at 11 (2016), <https://bit.ly/4rugSP1>. In DoW’s interpretation, “publicly available information” includes information “available to the public by subscription or purchase.” *Id.* at 53.

it would even apply to the mine run of DoW’s commercial data purchases. The agency may not consider its purchases of global data—which includes U.S. person data—to constitute “intentional” collection of “U.S. person information.” *See infra* Section II.C. A more recent policy “framework” established by ODNI is similarly weak. The framework requires agencies to limit their collection of sensitive personal information “to the maximum extent feasible”—but no more than is “consistent with” the agency’s “mission or administrative need.”³²

B. Intelligence agencies take a narrow view of constitutional protections for publicly available data and data shared with third parties.

Not only does U.S. statutory law permit the government’s bulk purchases of Americans’ data, but the law more generally fails to account for AI’s capacity to revolutionize the government’s ability to exploit that data. Neither Congress nor the Supreme Court has reckoned with AI’s power to create detailed, comprehensive pictures of Americans’ lives en masse. Because government agencies take the view that constitutional protections do not apply to the purchase *or use* of commercially acquired or “public” data, there are few restraints on the agency’s ability to apply AI tools to dystopian ends.

³² ODNI, Intelligence Community Policy Framework for Commercially Available Information 5 (2024), <https://bit.ly/4uwAYLq>.

Given the statutory vacuum for commercial data purchases and “public” data, the primary protection against the use of AI tools to analyze this data flows from the Fourth Amendment. But this jurisprudence is still in the nascent stages of accounting for how data that is “public” or shared with third parties can nevertheless be assembled by the government to expose the “privacies of life,” *Carpenter*, 585 U.S. at 311 (quoting *Riley v. California*, 573 U.S. 373, 403 (2014)). In a pair of cases from the 1970s, the Supreme Court held that constitutional privacy protections do not apply to some types of records shared with third parties. *See United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979). More recently, the Supreme Court has declined to apply the third-party doctrine in cases involving new technology, but DoW components have interpreted those cases narrowly.

The most significant decision in this area is *Carpenter*. In holding that a request for seven days’ worth of historical cell-site location information was a search requiring a warrant, the Court limited the third-party doctrine and affirmed that Fourth Amendment protection can extend to records reflecting movements in public. The Court’s analysis focused on the government’s power to use cell-site location data to “effortlessly compile[]” highly “detailed” information by leveraging a database that “runs against everyone,” generate “retrospective” data that law enforcement could mine infinitely, and grant the government “access to a

category of information [that is] otherwise unknowable.” *Carpenter*, 585 U.S. at 309, 312.

Despite the relevance of these issues to commercial datasets, DoW components have taken the position that *Carpenter* does not require them to obtain a court order to acquire or use commercial data available to the public.³³ In particular, DIA has claimed that *Carpenter* was a “narrow” decision that does not address data purchases or collection techniques involving “national security.”³⁴ And ODNI has publicly described several theories for limiting *Carpenter*’s application to commercial data purchases: some purchases may involve factors that “bring the acquisition outside the scope of *Carpenter*”; *Carpenter* may not apply to the “special need” of intelligence collection; and the seller of data may consent unilaterally to the sale, at least where the subject is not “present” and objecting to the sale.³⁵

Thus, the problems are two-fold: the significance and reach of Supreme Court decisions is contested by the executive branch; and those decisions have yet to fully account for how data held by third parties can reveal the privacies of life—let alone for AI’s capacity to extract these privacies from bulk datasets.

³³ Moultrie Letter, *supra* n.6, at 1.

³⁴ See DIA Memo, *supra* n.4, at 2.

³⁵ See ODNI Report at 19-20.

C. The government regularly seeks to exploit loopholes in U.S. privacy laws to justify sweeping surveillance.

As Anthropic has explained in its public statements, precisely because U.S. privacy laws are so outdated and incomplete, a contract permitting “all lawful uses” of AI tools does not protect against many applications of AI for mass domestic surveillance.³⁶ But explicit surveillance guardrails are also essential because, even where existing privacy laws might appear to apply, the government has crafted and expanded numerous loopholes in those laws over time, using them to justify sweeping surveillance of people in the United States. It has stretched terms like “relevant” and “targeted” far past their commonsense limits, and it has cloaked broad collection of Americans’ communications behind words like “incidental,” “unintentional,” and “inadvertent.” These interpretive maneuvers heighten the need for clear and comprehensive guardrails when it comes to the use of AI for surveillance.

There are many examples of these legal gymnastics, but a few will suffice.³⁷ One notorious example revealed by Edward Snowden was the NSA’s reliance on the term “relevant” to collect records of virtually every phone call to, from, or

³⁶ See *Statement from Dario Amodei on our discussions with the Department of War*, News, Anthropic.com (Feb. 26, 2026), <https://bit.ly/4sMAaQX>.

³⁷ Numerous examples have been catalogued elsewhere. See Jameel Jaffer & Brett Max Kaufman, *How to Decode the True Meaning of What NSA Officials Say*, Slate (July 31, 2013), <https://bit.ly/4cOER8a>.

within the United States for nearly a decade. To justify this surveillance, the government cited Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1862 (2012): a law that authorized the government to compel businesses to disclose records “relevant” to foreign intelligence investigations. But unbeknownst to the public, the government had interpreted the word “relevant” to encompass essentially all domestic call records—placing hundreds of millions of Americans under surveillance on the theory that some small fraction of the records might become useful to an investigation in the future.³⁸ As one of Section 215’s primary drafters emphasized, although the law was modeled after traditional subpoena authorities, the government’s secret interpretation and the scale of the resulting surveillance bore no relation to what would have been permissible with a grand jury subpoena. Amicus Br. of Congressman F. James Sensenbrenner, Jr., *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Sept. 4, 2013) (ECF No. 46-1), <https://perma.cc/WBX6-J8RT>. One can easily imagine similarly expansive claims with respect to AI-driven surveillance, with the government justifying the collection of vast datasets based on AI’s potential to find hidden patterns within the sea of collected data.

³⁸ See *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act*, 57-60, Privacy and Civil Liberties Oversight Board (“PCLOB”) (Jan. 23, 2014), <https://perma.cc/S82M-CJPK>.

The government has also frequently used the term “targeted” to describe and justify what is in fact broad surveillance of Americans. Section 702 of FISA authorizes the government to “target” foreigners located abroad—an authority officials often insist is narrow and focused. 50 U.S.C. § 1881a.³⁹ But in practice, this surveillance is directed at nearly 300,000 individuals, groups, and organizations overseas, and vacuums up hundreds of millions of communications per year, including those of countless Americans who are in contact with the government’s foreign targets.⁴⁰ Similarly, officials use the term “incidental” to excuse this surveillance, conveying the impression that the collection of Americans’ communications is a *de minimis* or unintended byproduct, common to all forms of surveillance.⁴¹ But the warrantless surveillance of Americans’ communications under Section 702 was both a purpose and the direct result of the statute.⁴² The government retains the communications of Americans for years,

³⁹ See generally *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 57-60, PCLOB (July 2, 2014), <https://perma.cc/ASK4-9WRA> (“PCLOB Report”).

⁴⁰ Off. of C.L., Priv., and Transparency, *Annual Statistical Transparency Report (2024)* at 28, Off. of the Dir. of Nat’l Intel., <https://bit.ly/4lvlMdn>; PCLOB Report, *supra* n.39, at 111.

⁴¹ See, e.g., PCLOB Report, *supra* n.39, at 82, 86-87.

⁴² *Id.*

treating them as an enormous surveillance windfall and encouraging analysts to search through them without a warrant.⁴³

A similar sleight of hand occurs with the government's use of terms like "unintentional" and "inadvertent." A number of surveillance statutes and agency rules limit the "intentional" collection of Americans' private information, *see* 50 U.S.C. § 1801(f); DoD Manual 5240.1, but the government has found ways to sidestep these limitations by acquiring vast amounts of data and communications in bulk. As described above, agencies like DIA or NSA purchase enormous commercial datasets, or siphon communications off the internet backbone en masse, claiming they are seeking the information of foreigners. But the resulting datasets often contain the intermingled data of foreigners and Americans alike. This collection of Americans' private information is entirely foreseeable and expected. But rather than purge Americans' data, the agencies often retain and sift

⁴³ Reporting suggests that Anthropic has not objected to the use of its AI tools on information collected under FISA, which may include information collected under Section 702. Sheera Frenkel et al., *How Talks Between Anthropic and the Defense Dept. Fell Apart*, N.Y. Times (Mar. 1, 2026), <https://perma.cc/93WX-93KR>. While that invites important questions about where Anthropic has drawn its red lines in defining "mass domestic surveillance," it only underscores the need for clear and comprehensive AI guardrails.

through it, claiming it has been unintentionally collected and can be exploited for intelligence purposes.⁴⁴

Together, these and other loopholes mean that AI guardrails cannot be left to existing laws alone, because those laws provide no guarantees against “mass domestic surveillance.”

D. Enforcement mechanisms for existing legal protections are also weak and susceptible to abuse.

Finally, AI guardrails cannot be reduced to “all lawful uses” because the executive branch often secretly defines what is “lawful” in the national security context, giving itself the green light to conduct surveillance. And even when its spying activities become public, the government regularly thwarts efforts to obtain judicial review of surveillance in the courts.

The government has a track record of declaring its actions “lawful” in secret, even those that violate previously sacrosanct legal prohibitions. The NSA’s warrantless wiretapping program StellarWind, launched soon after September 11th, is a case in point. So is the CIA’s torture program. In both instances, lawyers in the Office of Legal Counsel secretly blessed activities that had no credible basis

⁴⁴ Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. Times (Jan. 22, 2021), <https://perma.cc/WW74-MFTD>; ACLU, PCLOB Comment Regarding Surveillance Activities Governed by EO 12333, at 2-7 (Jan. 13, 2016) <https://perma.cc/P887-UFXQ>.

in law and flew in the face of clear legal precedent, embracing novel legal rationales to justify the executive branch's unconstitutional or unlawful actions. *See* Charlie Savage, *Power Wars* 162-223 (2011). In both instances, executive branch lawyers did so in secret—it was only years later that the public saw the legal memoranda that purported to find the NSA's warrantless wiretapping and the CIA's torture "lawful." And only then was the executive branch's legal analysis subjected to meaningful independent scrutiny and widely rejected. If these activities can be unilaterally proclaimed "lawful" within the executive branch, that term alone surely cannot supply the AI guardrails needed to protect Americans from novel forms of mass domestic surveillance. This is particularly true in the national security context, where interpretations of the law are often kept secret, and uses of AI need not be publicly inventoried.

This problem is compounded by the difficulty of obtaining independent judicial review of surveillance conducted for national security purposes. The executive branch has long sought to insulate such activities from adversarial litigation in the courts, using a variety of obfuscatory techniques and legal arguments. The government relies on overbroad classification to withhold even basic information about its surveillance activities from the public, and it often deprives individuals whose privacy has been invaded of any notice of surveillance, including when the government is pursuing a criminal prosecution with the help of

the resulting evidence.⁴⁵ In some cases, the government even engages in a technique called “parallel construction”—a method of sanitizing and recreating an evidentiary trail in order to conceal controversial forms of surveillance.⁴⁶ The purpose and effect of such measures is to prevent individuals from challenging the lawfulness of surveillance in criminal cases. To thwart judicial review in civil cases, the government adopts different strategies, but to the same end: it invariably contests the plaintiffs’ standing, arguing they cannot even plausibly allege they were surveilled; and if plaintiffs surmount that hurdle by relying on public evidence, the government invokes the state secrets privilege, arguing that the case must be dismissed nonetheless. *See, e.g., Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013); *Wikimedia Found. v. NSA*, 14 F.4th 276 (4th Cir. 2021). The result is a legal vacuum of sorts, where the executive branch proclaims the lawfulness of its actions while aggressively seeking to evade or shut down any independent judicial review. It is easy to imagine the same occurring should DoW harness AI to engage in mass domestic surveillance.

⁴⁵ *See, e.g., Sarah Taitz & Patrick Toomey, Concealing Surveillance: The Government’s Disappearing Section 702 Notices*, Just Security (Sept. 27, 2023), <https://perma.cc/37FP-X43Y>.

⁴⁶ *See John Shiffman & Kristina Cooke, U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013), <https://bit.ly/4lr08H2>.

III. Anthropic’s advocacy for guardrails around AI-powered surveillance addresses a matter of immense public concern.

Anthropic’s advocacy for transparency and safety in AI development, and its discussion of the risks of mass domestic surveillance, are critical contributions to the ongoing public debate about the relationship between AI and government power. The U.S. government’s use of AI models for surveillance and the constraints that apply to such uses are matters of enormous importance. Although the public knows relatively little about the government’s current deployment of AI tools, there is no doubt that these tools have already enlarged the government’s surveillance capabilities. Without meaningful safeguards, the application of AI tools to ever-expanding government databases could easily result in the mass domestic surveillance about which Anthropic has raised the alarm.

Anthropic’s February 26 public statement about its discussions with DoW illustrates why the company’s red lines—and its speech about those red lines—are so important. The post explains that, in Anthropic’s view, the application of AI in certain cases “can undermine, rather than defend, democratic values,” and that “AI-driven mass surveillance presents serious, novel risks to our fundamental liberties. To the extent that such surveillance is currently legal, this is only because the law has not yet caught up with the rapidly growing capabilities of AI.”⁴⁷

⁴⁷ *Statement from Dario Amodei, supra* n.36.

DoW, for its part, had stated that it would contract only with AI companies that agree to “any lawful use” of their products.⁴⁸ As amici have explained, given the significant gaps in U.S. privacy law and the government’s broad view of its authority to collect and exploit information about Americans, “any lawful use” of AI tools by the government could quickly lead to dystopian levels of domestic monitoring: reconstructions of our movements, analyses of our web-browsing, and assessments of our religious observance, media preferences, medical conditions, and political leanings. *See supra*.

Anthropic was right to insist on guardrails against mass domestic spying, and to draw attention to this issue through its public statements. AI can enable surveillance that is unprecedented in its detail, scope, and scale—endangering the freedoms upon which our democracy depends. The right to privacy, freedom of speech, and freedom of association are critical to individual flourishing and to a healthy democratic society. These freedoms allow us to explore our interests, to cultivate and express a sense of self, to join or build communities of our choosing, and to seek to shape public and political discourse—to participate in the project of collective self-governance.

⁴⁸ *See id.*

But mass surveillance is corrosive to these freedoms. It can fuel the government's targeting of politically unpopular or vulnerable populations—suppressing dissent, weakening activism, and furthering invidious discrimination. And the chilling effects of this surveillance reach even more broadly. If the government is always watching—collecting data about our movements, associations, and online habits to feed AI analysis—people will inevitably respond by curtailing their speech and conforming their behavior. Mass surveillance makes people less willing to associate with individuals and organizations that may be the subject of government scrutiny, less willing to communicate openly, and less likely to search for, read, and write about sensitive topics online. The implementation of mass surveillance through AI thus poses a mortal threat to the political and social freedoms on which our democracy is founded.

CONCLUSION

Because the government is not permitted to punish Anthropic for its advocacy about the dangers of AI-enabled surveillance, the Court should grant the stay.

Dated: March 16, 2026

Samir Jain
Jake Laperruque
Greg Nojeim
CENTER FOR DEMOCRACY &
TECHNOLOGY

Respectfully submitted,

/s/ Ashley Gorski
Ashley Gorski
Patrick Toomey
Charlie Hogle
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

1401 K Street, NW, Suite 200
Washington, DC 20005
sjain@cdt.org

125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
Fax: (332) 234-9528
agorski@aclu.org

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
425 California Street, Suite 700
San Francisco, CA 94104
jgranick@aclu.org

*Counsel for Amici Curiae*⁴⁹

⁴⁹ Counsel thank law graduate (admission pending) Byul Yoon for her contributions to this brief.

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. 29(a) and 32(a) because it contains 6,486 words.
2. This brief complies with the typeface requirements of Fed. R. App. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced and easy-to-read typeface using Microsoft Word in 14-point size font.

Dated: March 16, 2026

/s/ Ashley Gorski
Ashley Gorski

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on March 16, 2026, I electronically filed the foregoing Certificate with the Clerk for the United States Court of Appeals for the District of Columbia Circuit by using the CM/ECF system. A true and correct copy of this brief has been served via the Court's CM/ECF system on all counsel of record.

Dated: March 16, 2026

/s/ Ashley Gorski
Ashley Gorski

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

333 Constitution Avenue, NW
Washington, DC 20001-2866
Phone: 202-216-7000 | Facsimile: 202-219-8530

Case Caption: Anthropic PBC

v.
U.S. Department of War, et al.

Case No: 26-1049

ENTRY OF APPEARANCE

The Clerk shall enter my appearance as Retained Pro Bono Appointed (CJA/FPD) Gov't counsel
for the Appellant(s)/Petitioner(s) Appellee(s)/Respondent(s) Intervenor(s) Amicus Curiae below:

Party Information

(List each represented party individually - Use an additional blank sheet as necessary)

American Civil Liberties Union

Center for Democracy & Technology

Counsel Information

Lead Counsel: Ashley Gorski

Direct Phone: (212) 284-7305 Fax: (332) 234-9528 Email: agorski@aclu.org

2nd Counsel: Patrick Toomey

Direct Phone: (212) 519-7816 Fax: (332) 234-9528 Email: ptoomey@aclu.org

3rd Counsel:

Direct Phone: (____) _____ Fax: (____) _____ Email: _____

Firm Name: American Civil Liberties Union Foundation

Firm Address: 125 Broad Street, 18th Floor, New York NY 10004

Firm Phone: (212) 549-2500 Fax: (____) _____ - _____ Email: _____

Notes: This form must be submitted by a member of the Bar of the U.S. Court of Appeals for the D.C. Circuit.
Names of non-member attorneys listed above will not be entered on the court's docket. Applications for
admission are available on the court's web site at <http://www.cadc.uscourts.gov/>.