ORAL ARGUMENT NOT YET SCHEDULED

No. 21-5276

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

CITIZENS FOR RESPONSIBILITY AND ETHICS IN WASHINGTON
Plaintiff-Appellant,

v.

DEPARTMENT OF JUSTICE,
Defendant-Appellee.

On Appeal from the United States District Court
for the District of Columbia
No. 4:19-cv-3626 (DLF)
The Honorable Dabney L. Friedrich, District Court Judge

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AND THE ELECTRONIC FRONTIER FOUNDATION AS *AMICI CURIAE* IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

John Davisson
Megan Iorio
Enid Zhou
Ben Winters
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

Attorneys for Amici Curiae

March 29, 2022

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), *amici curiae* certify that:

A. Parties, Intervenors, and Amici

Except for the following, all parties, intervenors, and *amici* appearing before the district court and in this Court are listed in the Brief for the Appellant: the Electronic Privacy Information Center, Electronic Frontier Foundation, and American Oversight.

B. Ruling Under Review

References to the rulings at issue appear in the Brief for the Appellant.

C. Related Cases

This case has not previously been before this Court. Counsel is unaware of any related cases within the meaning of D.C. Circuit Rule 28(a)(1)(C).

STATEMENT REGARDING SEPARATE BRIEFING, CONSENT TO FILE, AUTHORSHIP, AND MONETARY CONTRIBUTIONS

A single joint amicus brief is not practicable in this case because the other planned amicus brief does not address the unique perspectives of the Electronic Privacy Information Center ("EPIC") and the Electronic Frontier Foundation ("EFF"). EPIC and EFF focus on the intersection of rights and technology. We are particularly concerned with unaccountable government use of new technologies for decision-making and surveillance. EPIC's and EFF's brief explains why revealing technology contractors' identities is necessary to shed light on government decision-making and surveillance activities. The amicus brief led by American Oversight will take a broader approach to the issue in this case and focus more on the general FOIA practitioner's perspective. Covering both perspectives in one brief would have been impossible due to word count limits and the disparate interests of the *amici.*

The parties consent to the filing of this amicus brief. No party's counsel authored this brief in whole or in part, and no party or party's counsel contributed money intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(a)(4)(E).

/s/ John Davisson
JOHN DAVISSON

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *Amici Curiae* the Electronic Privacy Information Center and the Electronic Frontier Foundation state that they have no parent corporations and that no publicly held corporation owns 10% or more of either of their stock.

/s/ John Davisson
JOHN DAVISSON

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Patrick Andriesen, *IDES Report Detailing Scope of Illinois Unemployment Fraud Remains Unpublished One Year Later*, Illinois Pol'y (Feb. 14, 2022) 21

Rashida Richardson, Jason Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 15 (2019) 8

Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, Berkeley Tech. L. J. 101 (2021) 9

Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016) 8

Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 Harv. J. L. & Tech. 1 (2014) 13

Stephanie Wykstra, *Government's Use of Algorithm Serves Up False Fraud Charges*, Undark (June 1, 2020) 22

TechWire, *Pondera Playing Key Role in EDD's Fight Against Fraud*, TechWire (Apr. 12, 2021) 6

Tom Maxwell, *No One in the U.S. Wants to Sell Phone-Tracking Tech to Cops Anymore*, Input Magazine (Oct. 23, 2020) 14

Tonya Riley, *Feds' Spending on Facial Recognition Tech Expands, Despite Privacy Concerns*, CyberScoop (Jan. 10, 2022) 17

U.S. Gov't Accountability Office, Facial Recognition Technology: Current and Planned Uses by Federal Agencies (2021) 7

U.S. Gov't Accountability Office, *Facial Recognition Technology: Examining Its Use by Law Enforcement, Hearing Before H. Judiciary Subcomm. on Crime, Terrorism, and Homeland Sec.*, 117th Congress (2021) 7

Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2019) 6

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., that focuses public attention on emerging privacy and civil liberties issues. EPIC routinely uses the Freedom of Information Act ("FOIA") and other open-records requests to shed light on government use of technology and litigates withholdings under Exemption 4. *See, e.g.*, Compl., *EPIC v. Immigrations and Customs Enforcement*, No. 20-3071 (D.D.C. filed Oct. 26, 2020); Compl., *EPIC v. Customs and Border Protection*, No. 19-cv-00689 (D.D.C. filed Mar. 12, 2019); Compl., *EPIC v. Department of Homeland Security*, No. 18-1268 (D.D.C. filed May 30, 2018); Compl., *EPIC v. Federal Trade Commission*, No. 18-cv-00942 (D.D.C. filed Apr. 20, 2018); Pl's Memo. Opposing Def's Mot. for Summary Judgment and Supporting Pl's Cross-Motion for Summary Judgment, *EPIC v. Department of Homeland Security*, No. 12-cv-00333 (D.D.C. filed Sep. 27, 2013). EPIC also participates as *amicus curiae* in cases concerning FOIA and the scope of exemptions. *See, e.g.*, Br. for EPIC as *Amicus Curiae* Supporting Respondent, *U.S. Fish & Wildlife Service v. Sierra Club*, 141 S. Ct. 777 (2021) (No. 19-547); Br. for EPIC et al. as *Amici Curiae* Supporting Respondent, *Food Marketing Institute v. Argus Leader Media*, 139 S. Ct. 2356 (2019) (No. 18-481);

---

[1] EPIC law fellow Tom McBrien contributed to this brief.

Br. for EPIC et al. as *Amici Curiae* Supporting Petitioner, *McBurney v. Young*, 569 U.S. 221 (2013) (No. 12-17); Br. for EPIC et al. as *Amici Curiae* Supporting Appellants, *New York Times v. U.S. Department of Justice*, 756 F.3d 100 (2d Cir. 2014) (No. 13-422).

The Electronic Frontier Foundation ("EFF") is a San Francisco-based, member-supported, nonprofit civil liberties organization that has worked for more than 30 years to protect free speech, privacy, security, and innovation in the digital world. With more than 35,000 members, EFF represents the interests of technology users in court cases and policy debates regarding the application of law to the internet and other technologies. In support of its mission, EFF frequently litigates FOIA requests to scrutinize government's use of digital technology in ways that threaten individuals' privacy and free expression. *See EFF v. DHS*, No. 19-cv-07431 (N.D. Cal. Nov. 12, 2019) (seeking details about the government's use of Rapid DNA analyzers at the border to verify familial relationships); *EFF v. Dep't of Commerce*, No. 17-cv-2567 (D.D.C. Nov. 30, 2017) (disclosing records regarding an in-development automated tattoo recognition program); *EFF v. DOJ*, No. 17-cv-1039 (D.D.C. May 31, 2017) (disclosing records reflecting the FBI's efforts to recruit Best Buy employees to serve as paid informants).

SUMMARY OF ARGUMENT

The federal government is increasingly outsourcing key functions to private technology companies. Federal agencies delegate decisions about individuals' education, welfare benefits, eligibility for parole, and level of health care to private companies by buying and using off-the-shelf automated decision-making tools and artificial intelligence ("AI") systems. Vendors sell powerful, cutting-edge surveillance technologies to law enforcement agencies, giving the agencies unprecedented power to identify and track individuals. Agencies also contract with private companies to verify the identities of applicants for public services using technologies that have known faults.

Decision-making, surveillance, and identity verification are quintessential government activities that impact individuals' fundamental rights. The government's decision to carry out these activities using technologies developed by private companies does not render the activities, or information about them, "commercial." Who develops and supplies the technology used for government activities is often the most basic—and vital—information needed to understand the government's activities. This is precisely the type of information that the FOIA was meant to make available to the public. It is not commercial information. The government should not be able to contract around the FOIA when it outsources its decision-making, surveillance, and identity verification activities.

A contractor's identity is often the key piece of information that allows organizations like EPIC and EFF to track the government's use of a specific type of technology and to vindicate rights impacted by this use. Because different jurisdictions may use the same company to supply a particular type of technology, a contractor's identity links information across jurisdictions. The name of the contractor also allows journalists and civil society organizations to discover information about the technology through the company's website and other sources. Knowing how and when a certain company's products are being used for government activities allows journalists and civil society organizations to warn people of risks to their rights, inform the government of pitfalls in different companies' technologies, and spur lawmakers into action.

ARGUMENT

I. The government is increasingly using automated systems created by private companies to make decisions about individuals.

The federal government is increasingly using artificial intelligence and automated decision-making systems in ways that implicate fundamental rights, including in education, child welfare, law enforcement, public benefits, and public health settings. As with any decision-making process, the design of an AI or automated tool involves numerous value-laden choices that affect how the system determines outcomes. But instead of developing these tools on their own, government agencies often purchase automated systems from private technology

vendors. By buying and relying on off-the-shelf commercial AI systems, the government essentially adopts the decision-making frameworks of its private contractors. The government should not be able to avoid scrutiny of its decision-making processes merely because it employs a private company to make or assist in those decisions. At minimum, the public has a right to know who these contractors are. Withholding this information would allow harmful AI tools from disreputable companies to proliferate throughout government without meaningful public awareness or scrutiny.

AI and automated decision-making systems analyze data to aid or replace human decision-making. These tools can take a variety of forms, from simple score sheets to complex machine-learning algorithms. AI and automated systems produce determinations such as risk scores, eligibility statuses, and identifications of individuals. The method or process that an AI or automated system uses to make a decision is called an algorithm. The design of AI and automated decision-making systems is largely unregulated and opaque, giving private companies wide discretion to design these tools as they please. Some vendors that develop these tools for the government operate in the shadows, marketing their services to government clients with little or no public scrutiny. Others have poor track records of inaccuracy and bias arising in their technology.

Privately developed AI and automated decision-making tools have far-reaching effects. For example, within the criminal justice system, judges and law enforcement officials rely on third-party developed predictive risk assessment tools to make decisions about pretrial detention, bail, sentencing, and parole.[2] Government agencies use automated decision-making tools for public benefits administration, including calculating Medicaid benefits and detecting unemployment benefits fraud.[3] Child protective services deploy AI algorithms to identify children at risk of neglect, abuse, or fatality.[4] Law enforcement agencies deploy facial recognition technology such as Clearview AI's controversial facial

---

[2] *See* Danielle Kehl, Priscilla Guo, & Samuel Kessler, *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*, Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School (2017), https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf

[3] *See, e.g.*, Arkansas Dep't of Human Services, *ARChoices in Homecare* (2022), https://humanservices.arkansas.gov/divisions-shared-services/aging-adult-behavioral-health-services/find-home-community-based-services-for-adults-seniors/archoices-in-homecare/; TechWire, *Pondera Playing Key Role in EDD's Fight Against Fraud*, TechWire (Apr. 12, 2021), https://www.techwire.net/news/pondera-playing-key-role-in-edds-fight-against-fraud.html.

[4] *See* Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2019).

recognition tool to surveil communities, match suspects in criminal investigations, identify travelers at border crossings, and for other purposes.[5]

The government's reliance on off-the-shelf automated decision-making systems has increased throughout the years. A February 2020 report commissioned by the Administrative Conference of the United States ("ACUS") found that nearly half of the 142 federal agencies studied had "experimented with AI and related machine learning tools."[6] In a 2021 Government Accountability Report, 18 agencies reported using facial recognition technology; ten of those agencies plan to expand the use of this technology in 2023.[7] Since the ACUS report, substantial federal funding to develop and procure AI tools has ballooned, with few proactive

---

[5] *Facial Recognition Technology: Examining Its Use by Law Enforcement, Hearing Before H. Judiciary Subcomm. on Crime, Terrorism, and Homeland Sec.*, 117th Congress 8–10 (2021) (statement of Gretta L. Goodwin, Dir., Homeland Sec. and Justice, U.S. Gov't Accountability Office), https://www.congress.gov/117/meeting/house/113906/witnesses/HMTG-117-JU08-Wstate-GoodwinG-20210713.PDF.

[6] David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey & Mariano-Florentino Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies* (2020), *available at* https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.

[7] U.S. Gov't Accountability Office, Facial Recognition Technology: Current and Planned Uses by Federal Agencies (2021), https://www.gao.gov/assets/gao-21-526.pdf.

transparency or accountability requirements in place.[8] The FOIA is often the only way for watchdog organizations to track and analyze the government's use of AI tools.

The choices and assumptions of third-party contractors are built into government AI systems. These choices and assumptions often reinforce historic biases and inequalities. Companies designing AI systems often rely on limited data sets to train algorithms to make predictions. [9] Data sets that lack diversity or are otherwise inaccurate, skewed, or systemically biased can train algorithms to make bad predictions.[10] These limited data sets, as well as the company's data mining practices, may have a history of discrimination baked into them.[11] Companies designing these predictive algorithms also embed their values and biases into the

---

[8] *See, e.g.*, *National Defense Authorization Act for Fiscal Year 2022*, https://www.armed-services.senate.gov/imo/media/doc/FY22%20NDAA%20Executive%20Summary.pdf; National Security Commission on Artificial Intelligence, *Final Report* (Mar. 1, 2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[9] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671, 671 (2016), *available at* https://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf.

[10] *See* Rashida Richardson, Jason Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 15, 18–19 (2019), https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson_etal-FIN.pdf.

[11] Barocas & Selbst, supra note 9 at 674.

system.[12] System designers set the parameters of how to collect, code, and source training data. Designers can encode conscious and unconscious assumptions about race, gender, or other biases into their predictive models when assigning weights to different factors or creating decision trees.[13] The enduring and pervasive history of racial discrimination influences all aspects of the technology development process.[14]

Automated systems may also not be able to accurately perform in ways that government agencies would like them to. Documents disclosed to EFF in response to a FOIA suit showed that private vendors building automated tattoo recognition systems could not accurately identify similar tattoos on different people or link them to images in other media.[15] Although companies' automated tools could accurately match images of the same tattoo with one another, they were not able to accurately do much else. For example, the algorithm used by one company to try to

---

[12] *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 4 (2014).
[13] *Id*. at 14.
[14] *See* Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, Berkeley Tech. L. J. 101, 120 (2021).
[15] *See* Aaron Mackey, Dave Maas, and Shirin Mori, *5 Ways Will Use Tattoo Recognition Technology*, EFF Deeplinks (June 2, 2016), https://www.eff.org/deeplinks/2016/05/5-ways-law-enforcement-will-use-tattoo-recognition-technology.

match a tattoo with an identical image found in another medium, such as on television or billboard, reported an accuracy rate of 36.5 percent.[16] The algorithms fared even worse when trying to match similar tattoos on different people: one company reported an accuracy rate of 14.9 percent.[17] The documents showed that technology is often not able to accurately perform complex tasks, raising concerns that agencies deploying them are using faulty products with potentially dangerous consequences to innocent individuals.

Effective oversight of government decision-making requires disclosing the identities of companies developing and selling these systems to the government. Withholding this information makes it impossible for the public to hold the government accountable for inaccurate or biased decision-making by off-the-shelf AI and automated decision-making systems.

EPIC has used contractors' identities to link information about AI and automated decision-making systems across jurisdictions and to advocate against harmful uses of these systems. For example, in *Rodriguez v. Massachusetts Parole Board*, a case currently before the Massachusetts Supreme Judicial Court, EPIC criticized the state's use of a risk assessment tool to deny the plaintiff parole based

---

[16] *Id*.
[17] *Id*.

on information EPIC obtained about the tool in Idaho. [18] The Parole Board's decision was based in part on a risk score produced by the Levels of Service/Case Management Inventory tool ("LS/CMI") developed and sold by MHS, Inc.[19] The Massachusetts Parole Board and MHS refused to provide Mr. Rodriguez and the public with meaningful information about how the tool made determinations about hopeful parolees.

EPIC was able to provide the Supreme Judicial Court with information about the MHS tool by linking information obtained about MHS from other sources. Through an open records request to the Idaho Department of Corrections, EPIC had obtained a checklist of factors considered by a related MHS risk assessment tool called the LSI-R.[20] Notably, EPIC did not know what system Idaho used at the

---

[18] *See* Br. for EPIC as *Amicus Curiae* Supporting Appellant 23–25, *Rodriguez v. Massachusetts Parole Board*, No. SJC-13197 (Mass. Sup. Jud. Ct. filed Feb. 14, 2022), *available at* https://epic.org/documents/rodriguez-v-massachusetts-parole-board/.

[19] *Id.* at 20.

[20] EPIC, *Documents Obtained by EPIC Show Idaho's Use of Subjective Categories in Calculating Risk* (Dec. 11, 2019), https://epic.org/documents-obtained-by-epic-show-idahos-use-of-subjective-categories-in-calculating-risk/.

time of the request,[21] but Idaho's production revealed that MHS supplied the tool.[22] Additional research confirmed that the systems used in Idaho and Massachusetts considered many of the same factors.[23] This allowed EPIC to explain to the Massachusetts Supreme Judicial Court that the tool the Massachusetts Parole Board used to determine Mr. Rodriguez's recidivism risk did not make reliable determinations for juvenile lifers like Mr. Rodriguez.

The information EPIC presented in its brief caught the attention of at least one justice on the court, who questioned the Parole Board's attorney about the tool's appropriateness for juvenile lifers.[24] The Parole Board's attorney conceded that the tool was not designed for use on juvenile lifers and was "not perfect."[25]

---

[21] Idaho Public Records Act Request Submitted By EPIC to the Idaho Dep't of Corrections (Nov. 21, 2019), https://archive.epic.org/EPIC-19-11-21-ID-FOIA-20191121-Request.pdf.

[22] EPIC, *Documents Obtained by EPIC Show Idaho's Use of Subjective Categories in Calculating Risk* (Dec. 11, 2019), https://epic.org/documents-obtained-by-epic-show-idahos-use-of-subjective-categories-in-calculating-risk/.

[23] Pamela M. Casey *et al.*, *Offender Risk & Needs Assessment Instruments: A Primer for the Courts* A-32 – A-34 (2014), *available at* https://www.ncsc.org/__data/assets/pdf_file/0018/26226/bja-rna-final-report_combined-files-8-22-14.pdf.

[24] Oral Argument at 26:01, *Rodriguez v. Massachusetts Parole Board*, No. SJC-13197 (argued Mar. 7, 2022), *available at* https://boston.suffolk.edu/sjc/archive.php.

[25] Oral Argument at 28:59, *Rodriguez v. Massachusetts Parole Board*, No. SJC-13197 (argued Mar. 7, 2022), *available at* https://boston.suffolk.edu/sjc/archive.php.

The name of the contractor was the crucial link allowing EPIC to apply the information learned from Idaho to Mr. Rodriguez's case in Massachusetts. This information was integral in the fight to vindicate Mr. Rodriguez's and other hopeful parolee's fundamental rights. If the government could withhold contractor identities, similar work would be impossible.

II. Government agencies conduct increasingly invasive surveillance using technologies purchased from private companies.

Government surveillance programs are typically powered by technology developed by and purchased from private vendors. The public cannot track the spread of surveillance technologies within the government and monitor the scope of government surveillance without knowing the identities of these private vendors.

Privately developed surveillance technologies enable the government to identify, track, and profile individuals. For example, the government uses technology like cell site simulators,[26] automatic license plate readers ("ALPRs"),[27]

---

[26] *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy*, 28 Harv. J. L. & Tech. 1 (2014).

[27] EFF, *Automated License Plate Readers* (Aug. 28, 2017), https://www.eff.org/pages/automated-license-plate-readers-alpr; ACLU, *You Are Being Tracked* (2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

and camera networks equipped with various identification and analysis tools, like facial recognition,[28] to track peoples' real-time and historic locations. The government analyzes the contents of cell phones and other electronic devices using powerful forensic tools.[29] The government also uses data mining tools to collect, analyze, and categorize large volumes of online speech.[30]

A limited number of vendors, many with controversial reputations, supply or have supplied these surveillance tools, such as L3Harris for cell site simulators,[31]

---

[28] EFF, *Face Recognition* (Oct. 24, 2017), https://www.eff.org/pages/face-recognition.

[29] *See* Logan Koepke, Emma Weil, Urmila Janardan, Tinuola Dada & Harlan Yu, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 20, 2020), https://www.upturn.org/work/mass-extraction/.

[30] *See, e.g.*, Mohammad A. Tayebi & Uwe Glässer, *Social Network Analysis in Predictive Policing* 7–14 (2016); Brent Skorup, *Cops Scan Social Media to Help Assess Your 'Threat Rating*,*'* Reuters (Dec. 12, 2014), https://www.reuters.com/article/idUS384038468220141212.

[31] Tom Maxwell, *No One in the U.S. Wants to Sell Phone-Tracking Tech to Cops Anymore*, Input Magazine (Oct. 23, 2020), https://www.inputmag.com/tech/american-cops-are-turning-to-canada-for-phone-tracking-tech-after-stingray-drops; Dell Cameron & Dhruv Mehrotra, *Cops Turn to Canadian Phone-Tracking Firm After Infamous 'Stingrays' Become 'Obsolete*,*'* Gizmodo (Oct. 23, 2020), https://gizmodo.com/american-cops-turns-to-canadian-phone-tracking-firm-aft-1845442778.

Vigilant Solutions and ELSAG for ALPRs,[32] Clearview AI for facial recognition,[33] Cellebrite and Magnet Forensic for digital forensics,[34] and Babel Street for social media monitoring. [35] Journalists, advocates, and even members of Congress have scrutinized these companies for their controversial technology and business practices. For example, lawmakers have urged federal agencies to end the use of Clearview AI's facial recognition technology, stating that this type of technology has "the concerning potential to violate Americans' privacy rights and exacerbate existing injustices."[36] Vigilant Solutions hires contractors to collect ALPR data across the country, which it then shares with "auto recovery (aka '"repo"') companies, banks, credit reporting agencies, and insurance companies" with no

---

[32] EFF, *Automated License Plate Readers* (Aug. 28, 2017), https://www.eff.org/pages/automated-license-plate-readers-alpr.
[33] *See* Paresh Dave & Jeffrey Dastin, *EXCLUSIVE Facial Recognition Company Clearview AI Seeks First Big Deals, Discloses Research Chief*, Reuters (Feb. 22, 2022), https://www.reuters.com/technology/exclusive-facial-recognition-company-clearview-ai-seeks-first-big-deals-2022-02-22/.
[34] Koepke, et al., *supra* note 29.
[35] Brennan Center for Justice, *Third-Party Vendors of Social Media Monitoring Tools for Law Enforcement Agencies* (Nov. 17, 2021), https://www.brennancenter.org/our-work/research-reports/third-party-vendors-social-media-monitoring-tools-law-enforcement.
[36] Letters from Senators Edward J. Markey, Jeffrey A. Merkley, and Representatives Pramila Jayapal, Ayanna Pressley to Alejandro N. Mayorkas, Secretary of Homeland Sec., Dep't of Homeland Sec., et al. (Feb. 9, 2022), https://www.markey.senate.gov/imo/media/doc/letters_-_federal_gov_use_of_clearview_ai.pdf.

retention limits.[37] When EFF investigated Vigilant and California law enforcement data sharing claims related to Vigilant's ALPRs, EFF found that the company's public statements directly contradicted internal communications.[38]

The Supreme Court has recognized that the government's use of new surveillance technologies implicates fundamental constitutional rights. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *Kyllo v. United States*, 533 U.S. 27 (2001). The public has a right to know how these technologies might be impacting their fundamental rights. Knowing the identity of a government contractor is often the only effective way to track which agencies are using a certain technology.

A clear and timely example of this work is the case of Clearview AI. Clearview AI's facial recognition technology scrapes public images from social media without users' consent to make it so that "almost anyone in the world will be

---

[37] EFF, *Automated License Plate Readers*, *supra* note 32.
[38] Dave Maass, *Here's Why You Can't Trust What Cops and Companies Claim About Automated License Plate Readers*, EFF Deeplinks (Mar. 19, 2019), https://www.eff.org/deeplinks/2019/03/heres-why-you-cant-trust-what-cops-and-companies-claim-about-automated-license.

identifiable."[39] Clearview AI's system was constructed without the consent or knowledge of any of the subjects, resulting in widespread controversy.[40] Amidst this controversy, procurement records revealed that the Federal Bureau of Investigation signed a contract with Clearview AI for the company's facial recognition technology.[41] EPIC and other organizations have used the FOIA to track government contracts with Clearview AI and to pressure government agencies to stop using the company's tool.[42]

Contractor identities were also important for EPIC's investigation into and advocacy against federal agencies' use of whole body scanners. In 2010, an EPIC FOIA lawsuit against the Transportation Security Administration ("TSA") revealed

---

[39] Drew Harwell, *Facial Recognition Firm Clearview AI Tells Investors It's Seeking Massive Expansion Beyond Law Enforcement*, Wash. Post (Feb. 12, 2022), https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/.

[40] *See* Alexandra S. Levine, *'Chilling': Facial Recognition Firm Clearview AI Hits Watchdog Groups with Subpoenas*, Politico (Sep. 24, 2021), https://www.politico.com/news/2021/09/24/clearview-ai-subpoena-watchdog-groups-514273.

[41] Tonya Riley, *Feds' Spending on Facial Recognition Tech Expands, Despite Privacy Concerns*, CyberScoop (Jan. 10, 2022), https://www.cyberscoop.com/feds-spending-on-facial-recognition-tech-continues-unmitigated-despite-privacy-concerns/.

[42] EPIC, *LAPD Bans Use of Clearview AI Facial Recognition* (Nov. 19, 2020), https://epic.org/lapd-bans-use-of-clearview-ai-facial-recognition/.

contracts with two companies: Rapiscan and L-3 Communications.[43] Both sets of scanners created revealing, almost naked images of subjects, but the two companies used different scanning technology to accomplish this task: Rapiscan used low dose X-rays, which expose the subject to radiation, while L-3 Communications used radio waves, which do not.[44] EPIC used this information to seek further records about the Rapiscan machines and their potential health effects.[45] EPIC also tracked other agencies' uses of the Rapiscan machines using publicly available records and the FOIA[46] and sued the TSA's parent agency, the Department of Homeland Security, to suspend the whole body scanner program.[47]

---

[43] Marc Rotenberg, John Verdi & Ginger McCall, *Preliminary Analysis: Documents Obtained from Department of Homeland Security Concerning Body Scanners* 2, EPIC (Jan. 11, 2010), http://epic.org/privacy/body_scanners/EPIC_WBI_Memo_Final_Edit.pdf.
[44] Joe Sharkey, *A Farewell to 'Nudity' at Airport Checkpoints*, N.Y. Times (Jan. 21, 2013), https://www.nytimes.com/2013/01/22/business/a-farewell-to-nudity-at-airport-checkpoints.html.
[45] *See* EPIC, *EPIC v. Department of Homeland Security (Full Body Scanner Radiation Risks)* (2013), https://epic.org/documents/epic-v-department-of-homeland-security-full-body-scanner-radiation-risks/.
[46] *See, e.g.,* Freedom of Information Act Request Submitted by EPIC to Latita Payne, U.S. Secret Service (Apr. 20, 2012), at 2–3, https://archive.epic.org/foia/dhs/usss/Secret-Service-FOIA-Request.pdf.
[47] *See* EPIC, *EPIC v. DHS (Suspension of Body Scanner Program)* (2017), https://epic.org/documents/epic-v-dhs-suspension-of-body-scanner-program/.

Meanwhile, Congress imposed a deadline for both companies to retrofit their scanners with software that would create less revealing images of subjects.[48] Rapiscan came under suspicion of manipulating the tests of this privacy software.[49] Ultimately, L-3 met its deadline to develop the software, but Rapiscan did not, leading the TSA to cancel its contract with Rapiscan and to remove its machines from airports.[50]

The government has increasingly turned to private data brokers to acquire the information it once collected itself, an effort some agencies argue allows them to avoid constitutional safeguards such as obtaining a warrant for private data.[51] For instance, instead of using surveillance tools or government agents to track individuals' movements, some government agencies have purchased bulk location data from data brokers. One such broker, X-Mode, was mired in controversy after a journalist exposed how the company purchased location data from cell phone

---

[48] David Kravets, *TSA Pulls Plug on Airport Nude Body Scanners*, Wired (Jan. 18, 2013), https://www.wired.com/2013/01/tsa-abandons-nude-scanners/.
[49] Kim Zetter, *Maker of Airport Body Scanners Suspected of Falsifying Software Tests*, Wired (Nov. 15, 2012), https://www.wired.com/2012/11/rapiscan-fraudulent-tests/.
[50] David Kravets, *supra*, note 48.
[51] *See* Charlie Savage, *Intelligence Analysts Use Smartphone Location Data Without Warrants, Memo Says*, The N.Y. Times (Jan. 22, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

apps that cater to Muslims.[52] Government contracts subsequently revealed that several federal agencies purchased location data from X-Mode and other location data brokers such as Venntel.[53] Public watchdogs and members of Congress have used this information to pressure the agencies to end their use of these data broker products.[54]

III. Government agencies purchase identity verification technologies and others from private companies.

Verifying the identity of a person applying for public benefits, accessing public records, or applying for an identity card is a core government function, but agencies are increasingly turning to private companies to perform sensitive identity

---

[52] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[53] Lee Fang, *IRS, Department of Homeland Security Contracted Firm That Sells Location Data Harvested from Dating Apps*, Intercept (Feb. 18, 2022), https://theintercept.com/2022/02/18/location-data-tracking-irs-dhs-digital-envoy/.

[54] Letter from Senators Elizabeth Warren and Ron Wyden and Representatives Carolyn B. Maloney and Mark DeSaulnier to Mr. Chris Gildea, President, Venntel, Inc. (Jun. 24, 2020), *available at* https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-06-24.CBM%20Warren%20Wyden%20DeSaulnie%20to%20Venntel%20re%20Mobile%20Phone%20Location%20Data.pdf; Fourth Amendment Is Not For Sale Act, S. 1265, 117th Congress (2021), *available at* https://www.congress.gov/bill/117th-congress/senate-bill/1265/text?r=73&s=1; EPIC, *Location Tracking* (2022), https://epic.org/issues/data-protection/location-tracking/; EPIC, *EPIC Sues ICE for Records on Social Media and Location Surveillance* (Mar. 18, 2022), https://epic.org/epic-sues-ice-for-records-on-social-media-and-location-surveillance/.

verification tasks. Some of these private companies use facial recognition and other surveillance systems to identify individuals.[55] These programs are spreading quickly. For example, the Department of Veteran Affairs turned to a private contractor to control access to the website that allows veterans to access medical records, lab results, and applications for benefits.[56] And after instances of fraud in the Pandemic Unemployment Assistance program, state unemployment agencies have faced public pressure to procure systems that promise to use identity verification to avoid and detect fraud.[57]

Outsourcing identity verification raises serious privacy, equity, and efficacy concerns. When companies collect highly sensitive data like social security

---

[55] *See, e.g.*, Irina Ivanova, *IRS Is Exploring Alternatives to Selfie Verification with ID.me*, CBS News (Jan. 31, 2022), https://www.cbsnews.com/news/irs-id-me-tax-return-alternatives/.

[56] *See* Dep't of Veterans Affairs, Press Release (Dec. 7, 2016), https://www.va.gov/opa/pressrel/pressrelease.cfm?id=2838.

[57] *E.g.*, Patrick Andriesen, *IDES Report Detailing Scope of Illinois Unemployment Fraud Remains Unpublished One Year Later*, Illinois Pol'y (Feb. 14, 2022), https://www.illinoispolicy.org/ides-report-detailing-scope-of-illinois-unemployment-fraud-remains-unpublished-one-year-later/; Greg Iacurci, *More Than $87 Billion in Federal Benefits Siphoned from Unemployment System, Says Labor Department*, CNBC (Dec. 20, 2021), https://www.cnbc.com/2021/12/02/over-87-billion-in-federal-benefits-siphoned-from-unemployment-system.html; Ally Schweitzer & Martin Austermuhle, *D.C.'s Department of Employment Services Enabled Widespread Identity Theft, Victims Allege*, DCist.com (Sept. 29, 2021), https://dcist.com/story/21/09/29/dc-unemployment-office-enabled-widespread-identity-theft-fraud-victims-allege/.

numbers on behalf of the government, that data may be protected only by a company's ordinary privacy policy and data practices—not federal law binding government actors.[58] In those instances, it is vital to know the identity of the contractor to understand the privacy and security risks of using a government service. The outsourcing process also blurs the distinction between governmental functions and private commercial interests, obscuring who is truly making the decisions. This is especially problematic when these systems fail. For example, a system used in Michigan falsely accused thousands of innocent people of fraud.[59] A lack of accountability can also harm those subject to biased outcomes that are harder to audit when the evidence is under the control of a private company.

Perhaps the most notorious of the identity verification system vendors is ID.me. EPIC, EFF, and their coalition partners successfully pressured the Internal Revenue Service ("IRS") to stop using ID.me to verify the identities of people

---

[58] *See* Johana Bhuiyan, *A US Surveillance Program Tracks Nearly 200,000 Immigrants. What Happens to Their Data?*, Guardian (Mar. 14, 2022), https://www.theguardian.com/us-news/2022/mar/14/us-immigration-surveillance-isap.

[59] *See* Stephanie Wykstra, *Government's Use of Algorithm Serves Up False Fraud Charges*, Undark (June 1, 2020), https://undark.org/2020/06/01/michigan-unemployment-fraud-algorithm/.

accessing tax documents online.[60] Under the program, taxpayers would have to take "video selfies" that would be assessed by ID.me's facial recognition system.[61] Given facial recognition's privacy and bias issues,[62] requiring taxpayers to comply with this system represented a serious threat to privacy rights across the country. ID.me's biometric privacy policy also would have put millions of Americans' biometric identifiers at risk of misuse by a private company simply because they wished to access a government service.[63]

---

[60] EPIC, EFF, *et al.*, *A Call to Federal and State Agencies to End the Use of ID.me and Other Facial Recognition Identity Verification Services* (Feb. 14, 2022), https://epic.org/wp-content/uploads/2022/02/Coalition-Letter-ID.me-and-Face-Verification-Feb2022.pdf.

[61] Alan Rappeport & Kashmir Hill, *I.R.S. to End Use of Facial Recognition for Identity Verification*, N.Y. Times (Feb. 7, 2022), https://www.nytimes.com/2022/02/07/us/politics/irs-idme-facial-recognition.html.

[62] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat'l Inst. of Standards and Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 2018 Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research 81:1–15 (2018), *available at* http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Adam Schwartz, *Resisting the Menace of Face Recognition*, EFF Deeplinks (Oct. 26, 2021), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition.

[63] *See* ID.me, *Consent for ID.me to Collect Biometric Data: Biometric Information Privacy Statement* (Mar. 14, 2022), https://www.id.me/biometric.

The ability to raise concerns specific to ID.me was crucial for the campaign's success. In coalition members' public articles,[64] interviews,[65] and letters from members of Congress,[66] advocates referenced ID.me's specific failures and factual inconsistencies to explain why the program impermissibly risked Americans' privacy rights. In a letter to IRS Commissioner Charles Rettig, four members of Congress noted that ID.me's CEO and press relations department had issued conflicting statements about key aspects of the technology's capabilities.[67] The members of Congress also cited to specific instances of ID.me failing in the past, and they noted ID.me's general lack of transparency. A different pair of Senators also urging the program's suspension noted that "ID.me has a history of user complaints when its technology was used by state unemployment agencies,"

---

[64] Joy Buolamwini, *The IRS Should Stop Using Facial Recognition*, Atlantic (Jan. 27, 2022), https://www.theatlantic.com/ideas/archive/2022/01/irs-should-stop-using-facial-recognition/621386/.

[65] MSNBC Interview with Jeramie Scott, Senior Counsel, EPIC (Feb. 6, 2022), *available at* https://www.msn.com/en-us/news/politics/take-a-selfie-view-your-tax-records/vi-AATxb2e.

[66] Letter from Representatives Ted Lieu, Yvette Clarke, Pramila Jayapal & Anna Eshoo to IRS Commissioner Charles Rettig (Feb. 7, 2022), *available at* https://lieu.house.gov/sites/lieu.house.gov/files/Letter%20to%20the%20IRS%20on%20Facial%20Recognition%20%28Final%29%202.4.22.pdf.

[67] *Id.*

among other issues.[68] This underscored the hasty and opaque method by which the IRS chose ID.me and rolled out the program.

Eventually, the IRS and the Department of Treasury agreed to suspend the program.[69] But 27 states and multiple federal agencies still have contracts with ID.me. EPIC and its partners will continue to track and apply pressure to federal and state agencies to stop using this harmful facial recognition technology.[70] Tracking ID.me and the growing governmental use of biometrics will require the ability to know when ID.me is hired for the work.

IV. Knowing contractors' identities enables EPIC and EFF to submit properly scoped FOIA requests.

Knowing specific contractors' identities enables EPIC and EFF to submit targeted open records requests that are not unduly burdensome to the agency. EPIC and EFF regularly submit open records requests to inform the public about crucial developments in privacy and civil liberties. When requesters are able to reference specific contractor names in their requests, rather than relying on broad,

---

[68] Letter from Senators Jeffrey Merkley & Roy Blunt to IRS Commissioner Charles Rettig (Feb. 3, 2022), *available at* https://www.merkley.senate.gov/imo/media/doc/22.02.03%20Merkley-Blunt%20Letter%20to%20IRS%20on%20Facial%20Recognition%20Technology%20(002).pdf.

[69] *See* EPIC, EFF, et al., *supra* note 60.

[70] *Id.*

generalized requests for an entire category of information, agencies can efficiently and effectively search for relevant materials.[71] Moreover, by knowing the name of a contractor, requesters like EPIC and EFF can look up specific contract numbers and specify documents within their FOIA request, providing agencies with a path to locate and release responsive records.

By submitting requests that mention specific contractors, EPIC and EFF are able to obtain information about important developments in civil liberties and technology. For example, EPIC and others have tracked the abusive surveillance company Clearview AI as it quietly spread without democratic oversight.[72] EPIC uncovered information about a Department of Defense partnership with Raytheon to test "surveillance blimps" in the United States.[73] And EPIC shed light on an Immigrations and Customs Enforcement program that relied on the private vendor

---

[71] *See, e.g.*, Freedom of Information Act Request Submitted by EPIC to Robert Warren, D.C. Dep't of Human Services (June 25, 2021), *available at* https://epic.org/wp-content/uploads/foia/dc/dhs/screening-scoring/EPIC-21-06-25-DC-DHS-FOIA-20210625-Request.pdf.

[72] *See, e.g.,* EPIC, *EPIC Seeks Documents About ICE's Use of Clearview Other Facial Recognition Services* (Oct. 26, 2020), https://epic.org/epic-seeks-documents-about-ices-use-of-clearview-other-facial-recognition-services/

[73] *See* EPIC, *EPIC v. Army (Surveillance Blimps)* (2015), https://epic.org/documents/epic-v-army-surveillance-blimps/.

Cellebrite for mobile phone forensics technology, a program that was not well understood at the time.[74]

News and civil society organizations have used contractor identities to track new mass surveillance systems,[75] shed light on widespread bias in risk assessment algorithms,[76] reveal otherwise secret law enforcement use of new surveillance technologies,[77] provide informed comments to public agencies about novel privacy risks,[78] and track bad actors.[79] Without the ability to identify and track specific vendors, it would have been much more difficult for the public to understand these entities' controversial activities.

---

[74] *See* EPIC, *EPIC v. ICE (Mobile Forensics)* (2019), https://epic.org/documents/epic-v-ice-mobile-forensics/.
[75] *See* Jay Stanley, *Fast-Growing Company flock is Building a New AI-Driven Mass-Surveillance System*, ACLU.org (Mar. 3, 2022), https://www.aclu.org/report/fast-growing-company-flock-building-new-ai-driven-mass-surveillance-system.
[76] *See* Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[77] *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.
[78] Comments of EPIC *et al.* Regarding the Public and Private Sector Uses of Biometric Technologies (Jan. 15, 2022), https://epic.org/documents/epic-comments-to-ostp-on-public-and-private-sector-uses-of-biometric-technologies/.
[79] EPIC, *EPIC v. ICE (Palantir Databases)* (2020), https://epic.org/documents/epic-v-ice-palantir-databases/.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to reverse the district court's partial grant of summary judgment for Defendant.

Date: March 29, 2022

/s/ John Davisson
John Davisson
Megan Iorio
Enid Zhou
Ben Winters
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amici Curiae
Electronic Privacy Information Center &
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 5298 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and Circuit Rule 32(e)(1); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font in Times New Roman font.

Signature: *<u>/s/ John Davisson</u>* **Date:** March 29, 2022

CERTIFICATE OF SERVICE

I certify that on March 29, 2022, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the D.C. Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: March 29, 2022

/s/ John Davisson
John Davisson
Megan Iorio
Enid Zhou
Ben Winters
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amici Curiae
Electronic Privacy Information Center &
Electronic Frontier Foundation