No. 18-481

In The Supreme Court of the United States

FOOD MARKETING INSTITUTE,

Petitioner,

v.

ARGUS LEADER MEDIA, DBA ARGUS LEADER,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Eighth Circuit

BRIEF FOR THE AI NOW INSTITUTE, AMERICAN CIVIL LIBERTIES UNION, ELECTRONIC FRONTIER FOUNDATION, CENTER ON RACE, INEQUALITY, AND THE LAW, AND KNIGHT FIRST AMENDMENT INSTITUTE AS *AMICI CURIAE* SUPPORTING THE RESPONDENT

JASON M. SCHULTZ
NYU TECHNOLOGY LAW AND POLICY CLINIC
NYU SCHOOL OF LAW
245 Sullivan Street
New York, NY 10012

Counsel for AI Now Institute

JONATHAN M. MANES
LUCINDA M. FINLEY
Counsel of Record
CIVIL LIBERTIES AND TRANSPARENCY CLINIC
UNIVERSITY AT BUFFALO SCHOOL OF LAW
507 O'Brian Hall
Buffalo, NY 14260
(716) 645-6222
law-cltc@buffalo.edu

Counsel for Amici Curiae

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

DAVID D. COLE
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, N.W.
Washington, DC 20005

VERA EIDELMAN
BRETT MAX KAUFMAN
NATHAN FREED WESSLER
PATRICK TOOMEY
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

Counsel for American Civil Liberties Union

ANTHONY C. THOMPSON
DEBORAH N. ARCHER
VINCENT M. SOUTHERLAND CENTER ON RACE, INEQUALITY, AND THE LAW AT NEW YORK UNIVERSITY SCHOOL OF LAW
139 MacDougal Street
New York, NY 10012

Counsel for Center on Race, Inequality, and the Law

DAVID L. SOBEL
ELECTRONIC FRONTIER FOUNDATION
5335 Wisconsin Avenue, N.W.
Suite 640
Washington, DC 20015

AARON MACKEY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94101

Counsel for Electronic Frontier Foundation

ALEX ABDO
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115

Counsel for Knight First Amendment Institute

TABLE OF CONTENTS

Page

TABLE OF CONTENTS i

TABLE OF AUTHORITIES iii

INTEREST OF *AMICI CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT 6

I. The scope of Exemption 4 bears directly on the public's ability to learn about core government activities that rely on private companies 6

II. Because the government relies on private companies for key technologies, an expansive interpretation of Exemption 4 would shroud many important government activities in secrecy 9

A. Privately developed artificial intelligence and automated decisionmaking systems perform a growing number of core governmental functions 11

B. Private companies supply technology that enables location tracking and other previously impossible forms of surveillance 22

C. Private companies operate some of the federal government's most sensitive information infrastructure, including hosting cloud storage and providing official government credentials for veterans 29

TABLE OF CONTENTS—Continued

Page

III. Exemption 4 should be interpreted narrowly to ensure that the public can obtain critical information when the government relies on private companies 32

A. FMI's interpretation would render many carefully tailored confidentiality statutes superfluous, vastly expanding the secrecy of privatized governmental functions 34

B. FMI's interpretation would establish a subjective standard for secrecy and would result in haphazard, unpredictable, and unprincipled disclosure when government operations happen to involve private companies 36

C. Exemption 4 should be interpreted to include only records actually "obtained from" a private company, and not records that merely concern a private company 37

CONCLUSION 40

APPENDIX 1a

TABLE OF AUTHORITIES

Page

CASES

ACLU of Northern California v. United States Department of Justice, 880 F.3d 473 (9th Cir. 2018) 25, 26

Africa Fund v. Mosbacher, No. 92-cv-289, 1993 U.S. Dist. LEXIS 7044 (S.D.N.Y. May 26, 1993) 35

Argus Leader Media v. USDA, 740 F.3d 1172 (8th Cir. 2014) 35

Ark. Dep't of Human Servs. v. Ledgerwood, 530 S.W.3d 336 (Ark. 2017) 19

Bd. of Trade v. Commodity Futures Trading Comm'n, 627 F.2d 392 (D.C. Cir. 1980) 38

Bloomberg L.P. v. Bd. of Governors of the Fed. Reserve Sys., 601 F.3d 143 (2d Cir. 2010) 38, 39, 40

Carpenter v. United States, 138 S. Ct. 2206 (2018) 23, 28

Council for a Liveable World Educ. Fund v. Dep't of State, No. 96-cv-1807, 1998 U.S. Dist. LEXIS 23642 (D.D.C. Jan. 22, 1998) 35

Dep't of the Air Force v. Rose, 425 U.S. 352 (1976) 7, 33

Det. Watch Network v. United States Immig. & Customs Enforcement, 215 F. Supp. 3d 256 (S.D.N.Y. 2016) 9

Durrani v. United States Dep't of Justice, 607 F. Supp. 2d 77 (D.D.C. 2009) 35

EPA v. Mink, 410 U.S. 73 (1973) 7

TABLE OF AUTHORITIES—Continued

Page

FBI v. Abramson, 456 U.S. 615 (1982).....7, 33

Fisher v. Renegotiation Board, 355 F. Supp. 1171 (D.D.C. 1973) 39

Hodai v. City of Tucson, 365 P.3d 959 (Ariz. Ct. App. 2016).....25

Hodes v. Dep't of the Treasury, 967 F. Supp. 2d 369 (D.D.C. 2013) 35

Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017).....18, 19

Judicial Watch, Inc. v. FDA, 449 F.3d 141 (D.C. Cir. 2006) 38

K.W. ex rel. D.W. v. Armstrong, 180 F. Supp. 3d 703 (D. Idaho 2016).....19, 20

Kentucky v. King, 563 U.S. 452 (2011).....37

Kyllo v. United States, 533 U.S. 27 (2001).....28

Michael T. v. Bowling, No. 15-cv-09655, 2016 U.S. Dist. LEXIS 123749 (S.D. W. Va. Sept. 13, 2016) 19

Millions March NYC v. N.Y. City Police Dep't, No. 100690/2017 (Sup. Ct. Jan. 11, 2019), https://perma.cc/K7DR-M6XS 25

Milner v. Dep't of the Navy, 562 U.S. 562 (2011) 7, 33

Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974) 6

TABLE OF AUTHORITIES—Continued

Page

N.Y. Civil Liberties Union v. Erie Cty. Sheriff's Office, No. 000206/2014, 15 N.Y.S.3d 713 (Sup. Ct. Mar. 17, 2015) 25

Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157 (2003) 7

NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978) 7

Soghoian v. United States Department of Justice, 885 F. Supp. 2d 62 (D.D.C. 2012).....26

State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).....24

State v. Loomis, 881 N.W.2d 749 (Wis. 2016) 15

United States Dep't of Justice v. Julian, 486 U.S. 1 (1988).....33

United States Dep't of Justice v. Landano, 508 U.S. 165 (1993) 33

United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989).....7

United States Dep't of Justice v. Tax Analysts, 492 U.S. 136 (1989) 2, 7

United States v. Muni, 668 F.2d 87 (2d Cir. 1981).....37

United States v. Wymer, 654 Fed. Appx. 735 (6th Cir. 2016) 37

Williams v. Taylor, 529 U.S. 362 (2000).....34

TABLE OF AUTHORITIES—Continued

Page

STATUTES

5 U.S.C. § 552(a)(8)(A)(i)(I) 36, 37

5 U.S.C. § 552(b)(3) 35

5 U.S.C. § 552(b)(4) 8, 34, 37

5 U.S.C. § 552(b)(7)(E) 26

7 U.S.C. § 2018(c) 35

10 U.S.C. § 130 34

10 U.S.C. § 2305(g) 34

13 U.S.C. § 301(g) 34

15 U.S.C. § 1314(g) 34

19 U.S.C. § 1677(f) 34

22 U.S.C. § 2778(e) 35

41 U.S.C. § 4702 35

FOIA Improvement Act of 2016, Pub. L. No. 114-185 ..... 8, 36

Veterans Identification Card Act of 2015, Pub. L. No. 114-31 31

OTHER AUTHORITIES

120 Cong. Rec. H1787-H1803 (1974) 8

120 Cong. Rec. S9310-S9343 (1974) 8

120 Cong. Rec. H10864-H10875 (1974) 8

120 Cong. Rec. S19806-S19823 (1974) 8

TABLE OF AUTHORITIES—Continued

Page

Am. Civil Liberties Union, *You Are Being Tracked* (2013), https://perma.cc/B2R8-WYJN 23

Amy Bushatz, *Some Veterans Still Can't Apply for New ID Card*, Military.com (Apr. 2, 2018), https://perma.cc/BL8R-NFBM.....31, 32

Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085 (2018).....13

Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 Duke L. J. 1045 (2019) 14

Bernard E. Harcourt, *Risk as a Proxy for Race*, 27 Fed. Sent'g Rep. 237 (2015).....15

Brent Skorup, *Cops Scan Social Media to Help Assess Your 'Threat Rating'*, Reuters, Dec. 12, 2014, https://perma.cc/7BYY-WXXM.....23

Bryce Clayton Newell, *Local Law Enforcement Jumps on The Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 Me. L. Rev. 397 (2014) 27

Christopher Slobogin, *Principles of Risk Assessment: Sentencing and Policing*, 15 Ohio St. J. Crim. L. 583 (2018) 14

Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (2016), https://www.perpetuallineup.org 16, 23

TABLE OF AUTHORITIES—Continued

Page

Cody Benway, *You Can Run, But You Can't Hide: Law Enforcement's Use Of "Stingray" Cell Phone Trackers and The Fourth Amendment*, 42 S. Ill. U. L.J. 261 (2018) 24

Complaint, *Elec. Frontier Found. v. Dep't of Commerce*, No. 17-cv-2567 (D.D.C. Nov. 30, 2017).....18

Complaint, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Sup. Ct. Mar. 3, 2014), https://perma.cc/LE99-CPTE.....25

Council of the Inspectors General on Integrity and Efficiency, *Cloud Computing Initiative* (Sept. 2014).....30

Dan Hurley, *Can an Algorithm Tell When Kids Are in Danger?*, N.Y. Times Mag. (Jan. 2, 2018), https://perma.cc/6YF6-QTZJ 21

Danielle Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008).....13

Dave Maass & Jeremy Gillula, *What You Can Learn From Oakland's Raw ALPR Data*, EFF Deeplinks (Jan. 21, 2015), https://perma.cc/N9Z7-5NLA 28

Dep't of Veterans Affairs, *Press Release* (Dec. 7, 2016), https://perma.cc/L68Z-8Y5E 31

Elec. Frontier Found., *Automated License Plate Readers*, https://perma.cc/A797-Y6RV 23

TABLE OF AUTHORITIES—Continued

Page

Elizabeth Dwoskin, *Amazon Is Selling Facial Recognition to Law Enforcement—For a Fistful of Dollars*, Wash. Post (May 22, 2018), https://perma.cc/B5ST-C73B 17

Emily Manna & Jesse Franzblau, *Government Inc.: Amazon, Government Security & Secrecy*, Open the Government (2019), https://perma.cc/T3KS-TDE4 .....10, 29

Erin Harbison, *Understanding 'Risk Assessment' Tools*, Bench & B. Minn. (Aug. 3, 2018), https://perma.cc/7W7N-75CX 14

FedRAMP, *Marketplace*, https://perma.cc/W7F5-YBMD 29

Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Association for the Advancement of Artificial Intelligence (2019), https://perma.cc/7XJ7-L77L 17

Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 1 (2018) 17

Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, ProPublica (May 23, 2016), https://perma.cc/92WP-EXDJ 15

TABLE OF AUTHORITIES—Continued

Page

Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014) 13

Kevin McGillivray, *FedRAMP, Contracts, and the U.S. Federal Government's Move to Cloud Computing*, 17 Colum. Sci. & Tech. L. Rev. 336 (2016) 29, 30

Megan T. Stevenson & Christopher Slobogin, *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, 96 Wash. U. L. Rev. 681 (2018) 14

Mohammad A. Tayebi & Uwe Glässer, Social Network Analysis in Predictive Policing (2016) 23

N.Y. State Div. of Criminal Justice Servs., *License Plate Reader Suggested Guidelines* (Jan. 2011), https://perma.cc/EDL8-KPRF 26

Natalie Ram, *Innovating Criminal Justice*, 112 Nw. U. L. Rev. 659 (2018) 14

Neil Gordon, *Contractors and the True Size of Government* (Oct. 5, 2017) https://perma.cc/8X38-ZRYJ 9

Privacy Int'l, *Government Hacking and Surveillance: 10 Necessary Safeguards* (2018), http://bit.ly/2Y8AYlv 23

Robert Brauneis & Ellen Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018) 13

TABLE OF AUTHORITIES—Continued

Page

Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016) 13

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) 22, 24

Thomas Cormen et al., Introduction to Algorithms (3d ed. 2009) 11

U.S. Gov't Accountability Office, GAO-15-621, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* (2015).....16

Vera Eidelman, *The First Amendment Case for Public Access to Secret Algorithms Used In Criminal Trials*, 34 Ga. St. U. L. Rev. 915 (2018).....12

Vigilant Solutions, *About*, https://perma.cc/Z8G8-67RA 27

Vigilant Solutions, *Car Detector—Mobile Hit Hunter*, https://perma.cc/ZT9B-LUY7 27

Vigilant Solutions, *Software Program State and Local Law Enforcement Agency Agreement*, http://bit.ly/2W7QBb4 28

Virginia Eubanks, *A Child Abuse Prediction Model Fails Poor Families*, WIRED (Jan. 16, 2018), https://perma.cc/J75FBDUY.....21

TABLE OF AUTHORITIES—Continued

Page

Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2019) 20

Vivek Kundra, *White House Federal Cloud Computing Strategy* (Feb. 8, 2011).....29

INTEREST OF *AMICI CURIAE*

Amici AI Now Institute at New York University, American Civil Liberties Union, Electronic Frontier Foundation, Center on Race, Inequality, and the Law at NYU School of Law, and Knight First Amendment Institute at Columbia University, are public interest organizations, each committed to public accountability in government. *Amici* rely on the Freedom of Information Act ("FOIA") to understand a broad variety of government activities, including those the government accomplishes by relying on private companies.[1]

Amici are concerned that an interpretation of Exemption 4 that allows companies to self-designate any document as "confidential" will significantly undermine public accountability and transparency of government. *Amici* fear that such a broad and subjective construction of Exemption 4 will severely hinder citizens' ability to understand how the government is operating whenever it carries out public functions with the aid of a contractor, vendor, or other private company. Individual organizational statements are contained in the Appendix following this brief.

[1] No counsel for any party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. The parties' letters consenting to the filing of *amicus* briefs are on file with the clerk. All parties have consented to the filing of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case directly implicates FOIA's central purpose "to open agency action to the light of public scrutiny" in order to "help ensure an informed citizenry, vital to the functioning of a democratic society." *United States Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 142 (1989) (quotations omitted). Because the government so often relies on private vendors or contractors to carry out core governmental functions, it is impossible to adopt an expansive interpretation of Exemption 4 without doing violence to FOIA's core purpose.

Exemption 4 is concerned with certain "commercial or financial information" but Petitioner Food Marketing Institute's ("FMI") proposed interpretation would do far more than exclude corporate information of purely private concern. In practice, it would exclude crucially important information about how the *government* operates, whenever those operations depend on private companies to support governmental functions. On FMI's interpretation, any government contractor or vendor that performs core governmental functions could simply decide that any record that pertains to it should be withheld, without any showing of competitive harm, simply because the record has not been made public and the company prefers to keep it that way.

If Exemption 4 means what FMI says it does, the public interest at the heart of the statute would be displaced by private interests in secrecy. The disclosure inquiry under FOIA would end at whether a contractor

or vendor would prefer something be deemed confidential. FOIA's longstanding presumption of disclosure would be replaced by a presumption of secrecy in every area where the government relies on private companies—which is nearly every part of the federal government. Agencies and their vendors would have incentives to hide information inside company documents that could then be ubiquitously withheld. This type of secrecy would frustrate democratic public accountability of government—precisely what FOIA was enacted to guarantee.

An expansion of Exemption 4 would be particularly devastating for the public's ability to understand government programs that increasingly depend on emerging and complex technology developed by private companies. The government relies extensively on the private sector to provide technology that is central to all manner of government activities—from "big data" algorithmic decisionmaking systems, to powerful surveillance technology, to the government's core information infrastructures—and this reliance is sure to increase going forward. It is critical to cabin Exemption 4's reach so that the public is not left without the ability to understand core governmental activities by accessing records about the private sector technologies on which those activities depend.

For example, the government is increasingly relying on private-sector artificial intelligence ("AI") and algorithmic systems to make decisions that directly affect people's rights and opportunities including setting pre-trial detention, bail, criminal sentences, and parole

eligibility; charging an individual with a crime; removing a child from a home; and determining Medicaid benefits. All such technologies can easily encode biases—racial, or otherwise—and programming errors that lead to inaccurate or unfair results. As a result, when deployed by government, these private-sector algorithms can systemically deprive individuals of rights and opportunities that the government is charged with protecting.

The government also relies on the private sector for increasingly powerful surveillance technology including extremely precise location tracking, interception of network traffic, surreptitious computer hacking, and even automated physical surveillance using video cameras.

And private companies provide the government's data infrastructure, which handles the most sensitive information about individuals, including, in at least one instance, the quintessentially governmental task of verifying identity and providing a "government-issued" identification card.

These and other private-sector technologies increasingly define how government programs operate, how they affect individuals, and whether they may infringe on constitutional rights and liberties. But in most of these domains, the purchasing agency will not have detailed knowledge of how a particular technology works. That expertise is provided by the private company. In order to understand how government functions, it is essential for the public to be able to see documents provided to the government by private companies.

This Court should interpret Exemption 4 with these concerns firmly in mind. The statute's protection for "confidential" commercial information "obtained from a person" should not be interpreted to shroud vast swathes of governmental activity in secrecy solely because a private company has some private, subjective interest in secrecy.

There are strong reasons to reject the expansive and subjective definition of "confidential" commercial information proposed by FMI. That definition would fly in the face of decades of judicial precedent holding that FOIA exemptions must be narrowly interpreted. It would render the rest of Exemption 4's text, regarding "trade secrets," superfluous. It would also make a hash of Congress' painstaking work over decades to enact an array of narrowly targeted commercial secrecy exemptions. An expansive interpretation of Exemption 4 would thus risk overriding Congress' careful balancing of interests in disclosure and nondisclosure. FMI's proposed reading would also create a haphazard, unpredictable, and disorderly situation in which the scope of governmental secrecy depends not on any objective test or shared notion of confidentiality, but rather on each contractor or vendor's subjective preference for secrecy.

In addition, FMI's test—as applied in this case—would obliterate the exemption's textual limitation to information "obtained from a person." It would instead allow a private entity to prevent disclosure of information that is created by the government and which

belongs to the government, on the theory that a private company can object to any record that happens to include information about it that it prefers not to make public.

The Court should reject FMI's invitation to gut Exemption 4's crucial limits. *Amici* respectfully ask this Court to maintain the *National Parks* standard that has applied for over forty years to determine whether information in a FOIA document is "confidential," or to adopt a similar test that imposes an objective standard to determine whether disclosure of information would cause competitive harm or undermine another legitimate public interest. *See Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765 (D.C. Cir. 1974). The Court should also clarify that the exemption is strictly limited to records actually "obtained from" a private party. These tests provide a framework by which Exemption 4 can serve its legitimate but narrow goal, while preserving FOIA's core purpose of allowing the public to understand what its government is doing.

ARGUMENT

I. The scope of Exemption 4 bears directly on the public's ability to learn about core government activities that rely on private companies.

Passed in 1966 and strengthened several times since, FOIA "is often explained as a means for citizens

to know what the Government is up to." *Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 171 (2003) (quotation marks omitted). As this Court has noted, the statute's "central purpose is to ensure that the Government's activities be opened to the sharp eye of public scrutiny." *United States Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 779 (1989). This purpose serves "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). These interests are implicated whenever governmental functions are involved, no less so when the government has contracted with private entities to assist in these functions.

Consistent with this purpose, "FOIA . . . mandates that an agency disclose records on request, unless they fall within one of nine exemptions, [which] are 'explicitly made exclusive,' and must be 'narrowly construed,'" *Milner v. Dep't of the Navy*, 562 U.S. 562, 565 (2011) (quoting *EPA v. Mink*, 410 U.S. 73, 79 (1973) and *FBI v. Abramson*, 456 U.S. 615, 630 (1982)). This statutory structure permits the public "to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." *Dep't of the Air Force v. Rose*, 425 U.S. 352, 361 (1976) (quotation marks omitted); *Tax Analysts*, 492 U.S. at 142.

The transparency guaranteed by FOIA is a "structural necessity in a real democracy." *Nat'l Archives*, 541 U.S. at 172. Congress has repeatedly recognized FOIA

as central to our system of democratic accountability. The original 1966 bill passed by an overwhelming margin in both chambers of Congress. 120 Cong. Rec. H1787-H1803 (1974); 120 Cong. Rec. S9310-S9343 (1974). Congress strengthened FOIA in 1974, overriding a presidential veto to do so. 120 Cong. Rec. H10864-H10875 (1974); 120 Cong. Rec. S19806-S19823 (1974). FOIA has been amended repeatedly since then, most recently in 2016, in order to reinforce and further expand its reach. *See* FOIA Improvement Act of 2016, Pub. L. No. 114-185.

FOIA's unequivocal statutory purpose to open up government to public scrutiny remains fully engaged when the government chooses to enlist the aid of private companies to do government work. The public has an especially strong interest in being able to understand and oversee how private entities carry out public functions. The limits of Exemption 4, which exempts "commercial or financial information obtained from a person [that is] privileged or confidential," 5 U.S.C. § 552(b)(4), therefore directly implicates FOIA's core statutory purpose. If the exemption is defined so broadly that it can exempt essentially any records provided to the government and designated as confidential by private companies, it threatens to undermine the central objective of FOIA in every domain where the government relies on private companies.

II. Because the government relies on private companies for key technologies, an expansive interpretation of Exemption 4 would shroud many important government activities in secrecy.

The government frequently acts with the assistance of private companies. As of 2015, over forty percent of the federal workforce was employed by contractors. *See* Neil Gordon, *Contractors and the True Size of Government* (Oct. 5, 2017), https://perma.cc/8X38-ZRYJ. The government relies on private parties to do government work in many familiar contexts, like operating prisons and detention facilities. Exemption 4 has already been used in attempts to limit the public's understanding of that exercise of quintessentially governmental power. *See*, *e.g.*, *Det. Watch Network v. United States Immig. & Customs Enforcement*, 215 F. Supp. 3d 256 (S.D.N.Y. 2016).

The danger that Exemption 4 will be used to shield government work from the public eye is only increasing as the government turns to the private sector for technology to help carry out central functions in an enormous variety of domains. The government deploys artificial intelligence and algorithmic systems to inform decisions that affect fundamental liberty and property interests. It has purchased powerful surveillance technology that empowers law enforcement to engage in precise, pervasive location tracking and other intrusive surveillance that was previously impossible. It relies on private companies to provide the bedrock information infrastructure of the government.

Companies that contract with the government are already afforded significantly more privacy in carrying out their work than federal offices doing the same jobs. Private companies are, of course, not directly subject to FOIA, even when operating as contractors. In the tech sector, in particular, the intricacies of complex systems and programming serve to diminish oversight—policymakers and government officials often lack the expertise to identify problems. Engineers, in turn, may not be fully informed about what they are creating for the government, or all of the ways their technology will be used by agencies. *See* Emily Manna & Jesse Franzblau, *Government Inc.: Amazon, Government Security & Secrecy*, Open the Government, at 16-17 (2019), https://perma.cc/T3KS-TDE4.

Expanding Exemption 4 would thus prevent the public from answering important questions across a variety of domains where technology is transforming the powers and processes of government. It could render the public unable to determine whether technology is accurate, systemically biased, infringing individual rights, or even doing the job it is intended to do. The Court should not give private companies the power to prevent the public from investigating these questions using FOIA.

A. Privately developed artificial intelligence and automated decisionmaking systems perform a growing number of core governmental functions.

Automated decisionmaking and AI systems are transforming governmental administration across numerous domains, including health, education, criminal justice, parental rights, and public benefits. These systems are typically developed by private companies on behalf of the government. If Exemption 4 is expanded to include any records these private companies designate as "confidential," it will become effectively impossible to use FOIA as it was meant to be used—to understand how the government is making decisions in an ever-growing number of contexts.

AI and other automated systems aid (and sometimes replace) human decisionmaking by processing a variety of inputs through algorithms designed to produce results optimized according to some predetermined criteria. At the most basic level, an algorithm is just a computational procedure—a series of steps—that transforms inputs into an output. *See* Thomas Cormen et al., Introduction to Algorithms 5 (3d ed. 2009). It is like a manual or a recipe: a set of instructions for how to build something from raw materials.

Some contemporary algorithmic systems used in government simply attempt to take particular processes or rules and automate them in software. Increasingly, however, the government is relying on

private companies to develop statistical "machine learning" systems, which analyze large datasets to identify how various features in the data are correlated with a particular desired outcome. The system "learns" which features are most predictive of the desired result, and produces a model that can be applied to new cases to generate predictions. If a simple algorithm is akin to a recipe, machine learning systems analyze data to generate their own recipes, which can then be put to use.

Contrary to popular mythology, these types of computer systems are not infallible or objective in any meaningful sense. They are complex software systems the design of which involves innumerable decisions by human beings—engineers, data scientists, and coders. Those decisions can and do introduce bias, error, and hidden assumptions. *See* Vera Eidelman, *The First Amendment Case for Public Access to Secret Algorithms Used In Criminal Trials*, 34 Ga. St. U. L. Rev. 915, 923-32 (2018).

Even "simple" rules-based algorithmic systems can easily be infected by human coding errors, which can go unidentified for years. Problems are even more difficult to identify with respect to predictive systems built on "big data" machine learning techniques. Among other difficulties, these systems reflect and potentially amplify any biases and inadequacies in the datasets that they are trained on, potentially producing a model that makes systemically flawed predictions. Moreover, even if a model is well-tuned to one application, it may produce misleading results when

deployed in circumstances that differ from those for which it was originally designed.

These errors can produce flatly inaccurate results, or results that are systemically biased. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Cal. L. Rev. 671 (2016). Moreover, it is often difficult to understand why an algorithmic system produces a particular result. The algorithm's workings are typically inscrutable to the government officials who rely on them and to members of the public who are subject to their decisions. *See* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085 (2018); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. Rev. 93 (2014); Danielle Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008). The algorithmic system typically does not "show its work" or explain its reasoning—it simply issues a result.

The government already relies on algorithmic systems for a diverse array of decisions. *See* Robert Brauneis & Ellen Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018). In the future, these tools could transform nearly every domain of public administration. Allowing vendors to keep all documentation about these systems hidden from the public under Exemption 4 would be a catastrophe for the public's ability to understand governmental decisionmaking in the digital age.

a. At all levels of the criminal legal system, judges and other state actors are relying directly on algorithmic tools to make decisions about pretrial detention, bail, sentencing, and parole. Erin Harbison, *Understanding 'Risk Assessment' Tools*, Bench & B. Minn. (Aug. 3, 2018), https://perma.cc/7W7N-75CX. These tools purport to predict the risk that an individual will require rehabilitative resources while on parole, commit another offense after conviction, pose a threat to public safety, or fail to appear in court. *See* Christopher Slobogin, *Principles of Risk Assessment: Sentencing and Policing*, 15 Ohio St. J. Crim. L. 583 (2018). They rely on actuarial techniques to make predictions based on analysis of historical data. *See*, *e.g.*, Natalie Ram, *Innovating Criminal Justice*, 112 Nw. U. L. Rev. 659 (2018); Megan T. Stevenson & Christopher Slobogin, *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, 96 Wash. U. L. Rev. 681 (2018). The appeal of risk assessment algorithms lies in their promise to objectively classify the likelihood of recidivism or failure to appear. *See* Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 Duke L. J. 1045, 1047-48 (2019).

While these algorithms may be intended to reduce the possibility of bias on the part of a judge, like all algorithmic systems, they are themselves susceptible to bias. Sources of potential bias range from the disproportionate representation of people of color at all stages of the criminal legal process, to the possibility of bad data being used to teach the algorithm, to coding errors, to reliance on factors that are proxies for race

or other prohibited grounds for decision. *See*, *e.g.*, Bernard E. Harcourt, *Risk as a Proxy for Race*, 27 Fed. Sent'g Rep. 237 (2015). Furthermore, criminal risk assessment algorithms can be flat-out inaccurate. Without sufficient transparency, there is no way for the public to know whether any of these faults exist in a piece of software the government is using. *See State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017) (noting transparency, accuracy, and due process concerns require that "use of a COMPAS risk assessment must be subject to certain cautions").

In 2016, ProPublica released a report which detailed the racially biased results of COMPAS, a widely used risk assessment algorithm. According to ProPublica's data, the algorithm mistakenly labeled black defendants as higher risk twice as frequently as it mistakenly labeled white defendants as such. *See* Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, ProPublica (May 23, 2016), https://perma.cc/92WP-EXDJ.

These types of risk-scoring algorithms are often created by private companies for use by the federal and state courts. *Id.* Developers have resisted efforts to provide sufficient transparency about how their systems are developed and tested. For example, in response to the ProPublica study, Northpointe, which developed the COMPAS tool, refused to share its method of calculating risk scores on the theory that its methods are proprietary. *Id.*

Were it to expand Exemption 4, this Court could license private companies to make even broader secrecy claims regarding all manner of documentation they provide to government about their systems—even in contexts where the fundamental liberty interests of citizens are at stake.

b. Government agencies have begun to use AI-based biometric identification tools, such as facial recognition and tattoo recognition software, across a range of law enforcement applications. These tools raise serious questions about privacy, pervasive surveillance, and the risk of error, including racially disparate error rates.

In 2015, the Government Accountability Office published a report concerning facial recognition technology, which documented several privacy concerns associated with such tools. U.S. Gov't Accountability Office, GAO-15-621, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* (2015). These include the reduction of anonymity and the possibility of misidentification. *Id.* at 13-17. The 2015 report expressed concern that facial recognition might misidentify individuals at a higher rate than other biometric techniques "because facial recognition technology systems are currently less accurate than other biometrics." *Id.* at 17. Indeed, this has proven to be the case. *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (2016), https://www.perpetuallineup.org. A recent study revealed that Rekognition, face recognition

software developed by Amazon, is racially biased and significantly more accurate in recognizing lighter faces than darker faces.[2] Amazon's Rekognition software is in use by the government already; researchers focused on Amazon's system "following the revelation of the active use and promotion of its facial recognition technology in law enforcement[.]" Raji & Buolamwini, *supra*, note 2, at 3; *see also* Elizabeth Dwoskin, *Amazon Is Selling Facial Recognition to Law Enforcement—For a Fistful of Dollars*, Wash. Post (May 22, 2018), https://perma.cc/B5ST-C73B.

The public has a strong interest in accessing information related to which types of facial recognition software the government is using, in what ways it is being used, and the level of accuracy achieved. Expanding Exemption 4 could frustrate these goals by allowing companies to self-designate records as "confidential."

Amicus Electronic Frontier Foundation ("EFF") has already encountered such efforts to use Exemption 4 to impede basic transparency regarding biometric identification software that raises significant privacy and free expression concerns. In 2016 and 2017, EFF sought FBI and National Institute of Standards and Technology's ("NIST") records related to the agencies'

---

[2] Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Association for the Advancement of Artificial Intelligence (2019), https://perma.cc/7XJ7-L77L; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings of Machine Learning Research 1 (2018).

development of automated tattoo recognition technology. *See* Complaint, *Elec. Frontier Found. v. Dep't of Commerce*, No. 17-cv-2567 (D.D.C. Nov. 30, 2017). NIST researchers created a thirteen-page presentation summarizing an early phase of their research. The FBI released the title page, but it withheld the remaining twelve pages under Exemption 4. The presentation, which was ultimately disclosed, contained information on NIST's goals for tattoo recognition technology, testing protocols, and information on the origin of its dataset. If Exemption 4 had been defined as broadly as FMI wishes, EFF's would probably not have been successful and the report would have remained secret. Expanding Exemption 4 could thus leave the public in the dark about how the government develops biometric identification technologies and the accuracy of its systems.

c. Governments are also implementing automated decisionmaking systems to evaluate the performance of employees including, for example, public school teachers. A school district in Texas implemented one such "data driven" teacher evaluation model through privately developed software that purported to compare the results of a teacher's students to classroom statistics across the state and within the teacher's prior performance record. Teachers sued the district, arguing that the software was fundamentally inscrutable and that there was no way for teachers to know whether the software was accurately assessing their job performance. *See Houston Fed'n of Teachers, Local 2415 v. Houston Indep. Sch. Dist.*, 251 F. Supp. 3d

1168, 1171 (S.D. Tex. 2017). The court agreed, holding that the "teachers have no meaningful way to ensure correct calculation of their [evaluation] scores, and as a result are unfairly subject to mistaken deprivation of constitutionally protected property interests in their jobs." *Id.* at 1180. Similar systems purporting to measure the efficacy of government employees are likely to proliferate. Without meaningful transparency, these systems will raise serious concerns about fairness and accuracy.

d. Government agencies are using algorithmic tools to make decisions about how to ration federally-funded medical benefits, including essential medical services that severely disabled people receive from Medicaid. *See Ark. Dep't of Human Servs. v. Ledgerwood*, 530 S.W.3d 336 (Ark. 2017) (upholding an order enjoining the state from using its algorithm-based assessment tool to calculate attendant care hours, and finding irreparable harm to profoundly disabled beneficiaries); *K.W. ex rel. D.W. v. Armstrong*, 180 F. Supp. 3d 703 (D. Idaho 2016) (finding that algorithmic system used to calculate Medicaid benefits violated Due Process); *Michael T. v. Bowling*, No. 15-cv-09655, 2016 U.S. Dist. LEXIS 123749 (S.D. W. Va. Sept. 13, 2016).

These algorithms purport to make the state's allocation of scarce resources more efficient, but they are easily infected with grave defects. In one case, a court found that the state's automated Medicaid budgeting system was so unreliable that it "arbitrarily deprive[d] participants of their property rights and hence violate[d] due process." *K.W. ex rel. D.W.*, 180 F. Supp. 3d

at 718. In the same case, the court found that the ability of patients to appeal was frustrated by the state's refusal to provide a manual for a disability scoring tool furnished by a private company. *Id.* at 717. In the absence of basic transparency—which an expanded interpretation of Exemption 4 would frustrate—it will be impossible to audit the reliability and fairness of similar automated systems.

e. Child protective services ("CPS") agencies are also using automated decisionmaking systems to identify children at risk of abuse, neglect, or fatality. *See* Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (2019). These agencies have deployed predictive algorithms in an attempt to more efficiently utilize CPS resources. But, as with other predictive systems, they are susceptible to error and bias latent in the datasets they are built upon and the factors used to predict risk. For example, because these systems are based on datasets derived from a variety of government agency sources with which lower-income families are more likely to interact, there is a risk that they will have disproportionately negative effects on lower-income families. Information about low-income families is more abundant and more accessible to CPS than that of families that have resources to access private services that are not visible to CPS, like mental health care. This can amplify disparate outcomes, particularly in jurisdictions with a high prevalence of neglect cases, because most neglect cases are related to poverty (e.g., inadequate provisions of food). In such circumstances, these

predictive systems are likely to find correlations between low-income status and child neglect and then to disproportionately target CPS interventions at low-income families—in effect, because of their lack of resources. *See* Virginia Eubanks, *A Child Abuse Prediction Model Fails Poor Families*, WIRED (Jan. 16, 2018), https://perma.cc/J75FBDUY; Dan Hurley, *Can an Algorithm Tell When Kids Are in Danger?*, N.Y. Times Mag. (Jan. 2, 2018), https://perma.cc/6YF6-QTZJ.

For the public to understand how government is operating through private-sector algorithmic systems—and whether such systems are infected by bias or inaccuracy—the public, and particularly researchers, need access to basic information that private companies provide to government. This will typically include:

- documents that reflect that an automated system has been acquired and is being used;
- documents that reflect the objectives, purposes, and design choices made by the company;
- documents that reflect how the autonomous system is embedded into a governmental decisional context;
- documents that describe how the autonomous system processes inputs to produce outputs; and

- validation studies and other reports reflecting efforts to audit a system's accuracy, fairness, and suitability for its proposed purpose.

Under the broad reading of Exemption 4 FMI seeks, private software developers could object to disclosure of all of these types of documents. This degree of secrecy could pave the way toward an era of automated governmental decisionmaking that is largely inscrutable and unaccountable: errors will go unfixed, bias undetected, and individuals will be unable to understand or challenge the processes to which they are subject.

B. Private companies supply technology that enables location tracking and other previously impossible forms of surveillance.

The government relies on private companies to provide powerful, cutting-edge investigative technology. Government agencies now have access to a growing variety of private surveillance technologies. For example, cell site simulators can pinpoint the location of cell phones, log calls, and sometimes even intercept the content of conversations. *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). Computer hacking and surveillance software allows agencies to hijack and search computers, cell

phones, and myriad other internet-connected devices. *See* Privacy Int'l, *Government Hacking and Surveillance: 10 Necessary Safeguards* (2018), http://bit.ly/2Y8AYlv. Automated license plate readers track vehicle locations over months or years, creating a rich database of people's movements. *See* Elec. Frontier Found., *Automated License Plate Readers*, https://perma.cc/A797-Y6RV; Am. Civil Liberties Union, *You Are Being Tracked* (2013), https://perma.cc/B2R8-WYJN. Facial-recognition algorithms promise to automatically identify individuals in photos or videos, allowing police to track people in real time or to mine stored footage captured by CCTV cameras, and police body-worn cameras. *See*, *e.g.*, Garvie, *supra*. Social media data-mining tools allow government to amass, analyze, and assess large volumes of online speech and association from social networks. *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://perma.cc/7BYY-WXXM.

These invasive technologies enable surveillance that has never before been possible and allow police access to "information otherwise unknowable." *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018). Sometimes these technologies are so complicated, very few at the government even fully understand their operation. Often the only way to learn about these technologies is through the information the vendor itself has provided to the government. That information could be sealed away from the public indefinitely if

FMI's subjective and essentially limitless reading of "confidential" is adopted.

a. One example of this powerful, private-sector surveillance technology are cell site simulators, also known as "Stingray" devices or "IMSI-catchers." *See State v. Andrews*, 134 A.3d 324 (Md. Ct. Spec. App. 2016); Cody Benway, *You Can Run, But You Can't Hide: Law Enforcement's Use Of "Stingray" Cell Phone Trackers and The Fourth Amendment*, 42 S. Ill. U. L.J. 261, 264 (2018); Pell & Soghoian, *supra.* These devices mimic cell-phone towers, forcing phones nearby to connect with them. Benway, *supra*, at 265. This allows for highly intrusive forms of surveillance. Stingrays sweep up data not just about a target's cell phone, but also bystanders' phones in the area. *Id.* Stingrays can triangulate and track the location of cell phones, determine all of the cell phones located within a specific area, and even track all of the connections that a cell phone makes with a network—collecting the numbers dialed and the data accessed. *Id.* at 265-66. Some versions of the technology are also capable of intercepting the actual content transmitted through a cell phone. *Id.* The technology is extremely accurate and sensitive, able to pin users within a few meters of their actual location. *Id.* at 266.

Companies have already sought to shroud even the most basic information about Stingrays under Exemption 4 and similar exemptions at the state level. In Arizona, the Harris Corporation, which manufactures many versions of these devices, asked the police to withhold even its pricing data about cell site simulator

equipment under Exemption 4, although that exemption was not ultimately litigated. *Hodai v. City of Tucson*, 365 P.3d 959 (Ariz. Ct. App. 2016); Complaint, Ex. B, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Sup. Ct. Mar. 3, 2014), https://perma.cc/LE99-CPTE. Similarly, the Erie County Sheriff's Office in New York invoked trade secrets to withhold information about Stingrays. *See N.Y. Civil Liberties Union v. Erie Cty. Sheriff's Office*, No. 000206/2014, 15 N.Y.S.3d 713 (Sup. Ct. Mar. 17, 2015). Another New York court recently rejected the NYPD's argument that prices and features of its surveillance technology are trade secrets because there was no allegation of competitive harm or substantial injury from disclosure. *Millions March NYC v. N.Y. City Police Dep't*, No. 100690/2017 (Sup. Ct. Jan. 11, 2019), https://perma.cc/K7DR-M6XS.

Thus far, these efforts to withhold information about Stingrays under exemptions for commercial confidences have met only limited success—and have not had to be litigated—because the exemptions in question do not sweep nearly as broadly as FMI would like. But if FMI's broad and subjective standard prevails, what is now obviously subject to disclosure would become contested territory.

Indeed, FMI's definition of "confidential" would likely transform many successful FOIA requests about novel surveillance technologies into Exemption 4 denials. For example, in *ACLU of Northern California v. United States Department of Justice*, the government invoked a variety of FOIA exemptions, including the exemption for law enforcement techniques, to try to

prevent disclosure of information regarding cell phone based location tracking. 880 F.3d 473, 484 (9th Cir. 2018). In *Soghoian v. United States Department of Justice*, the government similarly resisted disclosure of certain information about internet and cell phone surveillance. 885 F. Supp. 2d 62, 65 (D.D.C. 2012). These cases have been litigated under exemptions that are more precisely tailored to the public interests actually at stake in such disputes, such as Exemption 7(E) for law enforcement "techniques and procedures." 5 U.S.C. § 552(b)(7)(E). But if Exemption 4 were expanded, the government could easily withhold all such information based solely on a company's private interests, so long as the records in question pertained to the company selling the equipment.

b. Automated License Plate Readers ("ALPR") are another example of powerful surveillance technology developed by private contractors before being sold or licensed to the government. ALPRs are camera systems which are generally mounted over roadways or attached to police squad cars. N.Y. State Div. of Criminal Justice Servs., *License Plate Reader Suggested Guidelines*, at 6 (Jan. 2011), https://perma.cc/EDL8-KPRF. From its perch above the road, an ALPR camera collects all of the license plate numbers it views, along with data on the location, date, and time, as well as photographs taken by the camera. *Id.* All of this information is uploaded to a central server. *Id.* at 7. In the aggregate, ALPR data can paint an intimate portrait of a driver's life, potentially identifying drivers who visit sensitive places such as health centers,

immigration clinics, gun shops, union halls, protests, or centers of religious worship. *See* Bryce Clayton Newell, *Local Law Enforcement Jumps on The Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 Me. L. Rev. 397, 403-04, 413 (2014). Private companies do not simply supply ALPR hardware, they also sell government agencies access to massive databases that aggregate billions of individual location points from commercial and government ALPR devices. *See* Vigilant Solutions, *About*, https://perma.cc/Z8G8-67RA. Law enforcement can use this aggregated data to determine a vehicle's frequent destinations, its travel patterns, associated vehicles, and where the vehicle has been recorded in the past. Vigilant Solutions, *Car Detector—Mobile Hit Hunter*, https://perma.cc/ZT9B-LUY7.

As with other surveillance technologies, transparency is essential in order for the public to understand the government's capabilities and engage in meaningful democratic oversight. In Chicago, for example, a public records request about ALPRs successfully led to the disclosure of police training materials that provided basic instructions on using the ALPR and an outline of its powerful capabilities—including being able to "stake out" certain license plates and map out the vehicle's "frequent locations." Under FMI's subjective definition of "confidential," all such material could potentially be withheld at the whim of the vendor because it contains information about the capabilities of the technology it provides.

This is not idle speculation. The largest ALPR contractor, Vigilant Solutions, already includes language in its contracts prohibiting disclosure of "confidential information," which the company defines to include the data collected and generated by its ALPR readers. *See* Vigilant Solutions, *Software Program State and Local Law Enforcement Agency Agreement*, at 1, http://bit.ly/2W7QBb4. These contracts' broad terms could be interpreted to restrict disclosure of all kinds of information, including aggregated data showing just how invasive ALPRs can be. *See* Dave Maass & Jeremy Gillula, *What You Can Learn From Oakland's Raw ALPR Data*, EFF Deeplinks (Jan. 21, 2015), https://perma.cc/N9Z7-5NLA.

* * *

In other contexts, this Court has properly adopted legal interpretations that take into consideration the rapid development of technology. In a recent Fourth Amendment case, when considering cell phone location tracking technology, the Court was careful to " 'take account of more sophisticated systems that are already in use or in development.' " *Carpenter*, 138 S. Ct. at 2218-19 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)). Similar concerns favor a narrow interpretation of FOIA Exemption 4. In order to understand the capabilities of government surveillance technology and parameters within which it operates, the public must have access to basic documents, which will often be provided by or pertain to private vendors.

C. Private companies operate some of the federal government's most sensitive information infrastructure, including hosting cloud storage and providing official government credentials for veterans.

a. Private companies store and process a massive amount of federal data. Since 2011, when the White House instituted its "Cloud First" policy encouraging the use of cloud computing, private cloud storage has proliferated across the government. *See* Vivek Kundra, *White House Federal Cloud Computing Strategy*, 1-2 (Feb. 8, 2011). Microsoft, Google, IBM, Cisco, Blackberry, Adobe, Oracle, and Amazon Web Services, along with dozens of other companies, all supply cloud services to the federal government. FedRAMP, *Marketplace*, https://perma.cc/W7F5-YBMD. Amazon will likely also soon become the Department of Defense's sole cloud provider with one of the largest government IT contracts in history. Manna, *supra*, at 5.

Cloud computing provides remote access to shared file storage space, software applications, and systems processing on demand. Data is stored on servers all over the world. This can be much cheaper than traditional network or storage systems. The trade-off is that "data stored on cloud computing infrastructures is done outside of the control of the data owner—requiring a great deal of reliance on the Cloud Service Provider." Kevin McGillivray, *FedRAMP, Contracts, and the U.S. Federal Government's Move to Cloud Computing*, 17 Colum. Sci. & Tech. L. Rev. 336, 339 (2016).

The loss of control over data creates serious privacy concerns for government and governed alike. Significant aspects of cloud services are performed by third-party subcontractors, invisible to the contracting agency. *Id.* at 374. These third-parties are sometimes excluded from the terms of the contract between an agency and its prime contractor, leaving no service agreement in place and therefore no real control over data. *Id.* at 367. Such was the case with an EPA cloud contract in which the NDA did not flow from the prime to the subcontractor for lack of privity. *Id.* This rendered the agency unable to audit or seek damages from the subcontractor, leaving the EPA on the hook for $2.3 million in noncompliant or non-delivered services. *Id.* at 377-78.

Data stored in the cloud by other agencies may be vulnerable too. An audit by the Council of Inspectors General on Integrity and Efficiency concluded that the participating agencies had "not fully considered and implemented existing guidelines" and that "all [participant] contracts lack[ed] the detailed specifications recommended in Federal cloud computing guidelines." Council of the Inspectors General on Integrity and Efficiency, *Cloud Computing Initiative*, at 1 (Sept. 2014). The study found "none of the 19 participating agencies had adequate controls in place to manage its cloud service providers and the data that reside within its cloud." *Id.* at 2.

The public has a strong interest in understanding the government's reliance on private cloud providers. There are serious questions about the limits on the

collection and use of data by private companies; the vulnerability of sensitive data to hackers; safeguards in place to prevent misuse; and potential impacts on vulnerable populations. FOIA is the principal mechanism by which the public can make such inquiries. An expanded reading of Exemption 4 would inhibit or outright prevent this oversight.

b. Government agencies have also begun to entrust private companies with sensitive identity-verification and credentialing functions. For example, the Department of Veterans Affairs ("VA") has enlisted a private contractor to control access to a website, www.VA.gov, that allows veterans electronic access to medical records, lab results, and applications for disability and educational benefits, among other services. Veterans seeking to access their records through this government website are encouraged or required to register an account with a private company, ID.me, in order to gain access. *See* Dep't of Veterans Affairs, *Press Release* (Dec. 7, 2016), https://perma.cc/L68Z-8Y5E.

The government is also relying on the same private company to provide government-backed identification cards. In 2015, Congress required the VA to issue official ID cards proving veteran status. Veterans Identification Card Act of 2015, Pub. L. No. 114-31. VA has delegated the task of verifying identity to the private company. *See* Amy Bushatz, *Some Veterans Still Can't Apply for New ID Card*, Military.com (Apr. 2, 2018), https://perma.cc/BL8R-NFBM. Identity-verification is a core governmental function; outsourcing it to a private entity raises significant questions

about accuracy and fairness: could the private system inadvertently exclude individuals who are eligible, or improperly grant credentials to those who are not eligible? *Id.*

Outsourcing such functions also raises serious potential privacy concerns by blurring the distinction between governmental functions and private commercial interests. Highly sensitive data like social security numbers that are collected by private companies on behalf of the government may become subject to a company's ordinary privacy policy and data practices. Information provided in order to obtain government services may thus end up protected only by laws regulating the private sector.

Many of these concerns can only be addressed by reference to documents exchanged between private companies and government. If FOIA's Exemption 4 is given FMI's broad reading, citizens might be prevented from meaningfully overseeing systems that affect their daily lives and contain their most sensitive data.

III. Exemption 4 should be interpreted narrowly to ensure that the public can obtain critical information when the government relies on private companies.

FMI's interpretation of Exemption 4 would swallow up more precisely tailored laws meant to protect legitimate commercial interests. It would create disorder, broadening the exemption's scope to an unpredictable extent, depending on the whims of each vendor or

contractor. In so doing, it would shroud in secrecy core governmental functions aided by private companies, negating FOIA's core purpose.

The Court should thus maintain a strict, narrow interpretation of Exemption 4. Like other FOIA exemptions, Exemption 4 "must be narrowly construed." *Rose*, 425 U.S. at 361; *see also Milner*, 562 U.S. at 571; *United States Dep't of Justice v. Julian*, 486 U.S. 1, 8 (1988) (interpreting Exemption 5 in accordance with "obligation to construe FOIA exemptions narrowly in favor of disclosure"); *FBI v. Abramson*, 456 U.S. at 630 (reaching a "result [that] is consistent with the oft-repeated caveat that FOIA exemptions are to be narrowly construed"); *United States Dep't of Justice v. Landano*, 508 U.S. 165, 181 (1993) (construing Exemption 7(D) "narrowly in favor of disclosure").

At a minimum, the Court should maintain a definition of "confidential" that requires a showing of competitive harm. The Court should also clarify that the exemption's requirement that information be "obtained from a person" means the exemption cannot cover information that the government itself develops or produces, simply because it concerns a private company. These interpretations would maintain appropriate limits on Exemption 4's scope.

A. FMI's interpretation would render many carefully tailored confidentiality statutes superfluous, vastly expanding the secrecy of privatized governmental functions.

Exemption 4 should not be interpreted to render other statutory text redundant. It is a core principle of statutory interpretation that "every word and every provision is to be given effect." *Williams v. Taylor*, 529 U.S. 362, 404 (2000). Yet FMI's interpretation would render the portion of Exemption 4 concerned with "trade secrets" superfluous, because private companies could self-designate *any* information as "confidential," whether or not they constituted a "trade secret" within the meaning of the Act. 5 U.S.C. § 552(b)(4).

Likewise, Exemption 4 should be interpreted in a way that does not make other statutes enacted by Congress redundant. FMI's interpretation of the exemption would make superfluous a whole host of targeted commercial privacy rules that Congress has enacted to protect specific commercial secrecy interests in particular domains. *See*, *e.g.*, 10 U.S.C. § 130 (restricting disclosure of certain technical contractor data with military or space applications); 10 U.S.C. § 2305(g) (protecting military contractor proposals unless incorporated into contracts); 13 U.S.C. § 301(g) (prohibiting disclosure of shippers' export declarations); 15 U.S.C. § 1314(g) (prohibiting disclosure of answers and documentary materials given in antitrust investigations); 19 U.S.C. § 1677(f) (prohibiting disclosure of certain information submitted to the International Trade

Commission); 22 U.S.C. § 2778(e) (prohibiting disclosure of certain information submitted by export license applicants); 41 U.S.C. § 4702 (protecting non-military, executive-agency procurement proposals).

These statutes demonstrate that Congress did not understand Exemption 4 to sweep as broadly as FMI argues. And in a number of cases, courts have indeed made fine-grained rulings about whether particular information submitted by a private company falls within one of these statutes and is therefore exempt from FOIA under Exemption 3, 5 U.S.C. § 552(b)(3), which allows agencies to withhold information under certain confidentiality statutes. *See Hodes v. Dep't of the Treasury*, 967 F. Supp. 2d 369 (D.D.C. 2013) (finding some information not exempt under 41 U.S.C. § 4702); *Durrani v. United States Dep't of Justice*, 607 F. Supp. 2d 77 (D.D.C. 2009) (finding some information not exempt under 22 U.S.C. § 2778(e)); *Africa Fund v. Mosbacher*, No. 92-cv-289, 1993 U.S. Dist. LEXIS 7044 (S.D.N.Y. May 26, 1993) (same); *Council for a Liveable World Educ. Fund v. Dep't of State*, No. 96-cv-1807, 1998 U.S. Dist. LEXIS 23642 (D.D.C. Jan. 22, 1998) (construing 22 U.S.C. § 2778(e) narrowly).

Even in the specific context of this case, which concerns financial information regarding retailers and wholesalers who participate in SNAP, Congress has passed a specific statute protecting certain specific information against disclosure. 7 U.S.C. § 2018(c); *see Argus Leader Media v. USDA*, 740 F.3d 1172 (8th Cir. 2014).

All of these statutes would be rendered superfluous and irrelevant if Exemption 4 were interpreted to encompass anything a private company has not made public and prefers not to disclose. By enacting this panoply of context-specific confidentiality statutes, Congress demonstrated that it did not understand or intend Exemption 4 to sweep nearly that far.

B. FMI's interpretation would establish a subjective standard for secrecy and would result in haphazard, unpredictable, and unprincipled disclosure when government operations happen to involve private companies.

FMI's reading expands Exemption 4 to an unknowable and necessarily subjective extent. Under FMI's proposed test, each company would decide for itself what should be regarded as confidential. This kind of subjective test would leave the public unaware of what is happening in certain parts of our government, and unsure of what types of records, if any, are accessible.

Congress recently amended FOIA to make clear that exemptions must be given an objective, predictable scope. The FOIA Improvement Act of 2016 added language confirming that tests for exemptions should be objective, not subjective: "An agency shall withhold information under this section only if the agency *reasonably foresees* that disclosure would harm an interest protected by an exemption." 5 U.S.C.

§ 552(a)(8)(A)(i)(I) (emphasis added). Reasonable foreseeability is classic objective language and its use indicates that a subjective test is inconsistent with the statute itself. *See*, *e.g.*, *Kentucky v. King*, 563 U.S. 452 (2011) ("Legal tests based on reasonableness are generally objective."); *United States v. Wymer*, 654 Fed. Appx. 735, 754 (6th Cir. 2016) ("[R]easonable foreseeability is an objective test."); *United States v. Muni*, 668 F.2d 87, 90 (2d Cir. 1981).

The subjective reading FMI urges would swallow up FOIA whole where the government relies on contractors to deliver services or where private technology and equipment is central to government programs. If private companies are free to deem as secret information about their services that they have already shared with the government, the public will frequently be left in the dark about government activities.

C. Exemption 4 should be interpreted to include only records actually "obtained from" a private company, and not records that merely concern a private company.

Exemption 4's protection for commercial information is limited to information that is both "confidential" and, importantly, "obtained from a person." 5 U.S.C. § 552(b)(4). The Court should clarify that the latter phrase, too, imposes a meaningful limit on the scope of the exemption. In particular, the Court should clarify that the exemption covers only information that

a private contractor provides directly to the government, and does not cover the government's own records or information that the government itself develops, even if it concerns the private company or would reveal information about the company's operations, products, or services. This interpretation would make clear that any information the government itself generates about its contractors and vendors—for example, audits, assessments, evaluations, financial summaries, records of payments, purchase prices, contracts, etc.—would remain subject to disclosure unless covered by another, more precisely-tailored exemption.

The Second Circuit has examined the "obtained from a person" requirement carefully and persuasively in *Bloomberg L.P. v. Board of Governors of the Federal Reserve System*, 601 F.3d 143 (2d Cir. 2010). In that case, the court considered a FOIA request for details about loans granted by the Federal Reserve to commercial banks in the aftermath of the financial crisis. *Id*. at 145-46. The court distinguished between completed bank loan applications (which would be records "obtained from" the borrower) and the terms of the loans actually awarded by the Federal Reserve (which were the agency's own information generated upon the decision to grant a loan). *Id.* at 148.

The court observed, more generally, that records generated by the government or within the agency cannot be subject to Exemption 4. *Id.* (citing *Bd. of Trade v. Commodity Futures Trading Comm'n*, 627 F.2d 392, 403-04 (D.C. Cir. 1980) and *Judicial Watch, Inc. v. FDA*, 449 F.3d 141, 148 (D.C. Cir. 2006)). This is true, the

court explained, even when information created by the agency could disclose information about the private entity: "The fact that information *about* an individual can sometimes be inferred from information *generated within an agency* does not mean that such information was *obtained from* that person within the meaning of FOIA." *Id.* (emphases in original).[3]

The records sought by Argus Leader in this case illustrate the danger of ignoring the phrase "obtained from a person" in the exemption. Argus Leader seeks records about private companies—grocery stores—that are an integral part of delivering an important governmental service, namely food aid. But Argus Leader does not seek any proprietary information that the grocery stores themselves provided to the government, or which the government demanded from them. Instead, Argus Leader seeks records that *the government itself* has created in order to administer the program. Like the loan amounts at issue in *Bloomberg L.P.*, records showing the amount of money paid out to grocery stores by the government are not records "obtained from a person" but instead generated by the government.

---

[3] This line of reasoning has surfaced periodically nearly since FOIA's inception. For example, in *Fisher v. Renegotiation Board*, 355 F. Supp. 1171 (D.D.C. 1973), the court held that Exemption 4 did not cover records from a federal board charged with eliminating excessive profits on defense contracts. *Id.* at 1173. The court found that records showing the amounts of excess profits were the board's own calculations and thus not "obtained from a person," even though they were based directly on figures obtained from the contractors. *Id.* at 1174.

In particular, the records requested by Argus Leader reside in the USDA's own Food and Nutrition Services Store Tracking Redemption System database. Br. of Resp. at 4. These are the government's own records. The fact that they *concern* a private company does not mean that they were "obtained from" that company. *Cf. Bloomberg L.P.*, 601 F.3d at 148. Indeed, arguing that such figures belong to the grocery stores and are not the government's own data is akin to arguing that one's own checkbook register is not one's own data but rather information "obtained from" the stores with which one has transacted. Just as one's own record of payments cannot be said to be a private company's records simply because they reveal information about that company, information developed by the government cannot be said to be "obtained from" a private company simply because it would reveal something about the private company.

The Court should thus clarify that the phrase, "obtained from a person," means that the exemption covers only records that the government actually receives directly from a person or company. Consistent with the Court's unbroken line of cases requiring that exemptions be construed narrowly, the exemption cannot be read to cover records that the government creates itself, even if they concern the company.

CONCLUSION

Amici urge the Court to reject FMI's broad and subjective interpretation of Exemption 4. Instead, the

Court should give Exemption 4 a narrow construction, holding that information is covered only if the records in question were actually "obtained from" a private company and disclosure would actually cause competitive harm, such that the records can properly be considered "confidential" in nature.

Respectfully submitted,

JASON M. SCHULTZ
NYU TECHNOLOGY LAW AND POLICY CLINIC
NYU SCHOOL OF LAW
245 Sullivan Street
New York, NY 10012

Counsel for AI Now Institute

DAVID D. COLE
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, N.W.
Washington, DC 20005

VERA EIDELMAN
BRETT MAX KAUFMAN
NATHAN FREED WESSLER
PATRICK TOOMEY
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

Counsel for American Civil Liberties Union

JONATHAN M. MANES
LUCINDA M. FINLEY
Counsel of Record
CIVIL LIBERTIES AND TRANSPARENCY CLINIC
UNIVERSITY AT BUFFALO SCHOOL OF LAW
507 O'Brian Hall
Buffalo, NY 14260
(716) 645-6222
law-cltc@buffalo.edu

Counsel for Amici Curiae
DAVID L. SOBEL
ELECTRONIC FRONTIER FOUNDATION
5335 Wisconsin Avenue, N.W.
Suite 640
Washington, DC 20015

AARON MACKEY
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94101

Counsel for Electronic Frontier Foundation

ANTHONY C. THOMPSON
DEBORAH N. ARCHER
VINCENT M. SOUTHERLAND
CENTER ON RACE, INEQUALITY, AND THE LAW AT NEW YORK UNIVERSITY SCHOOL OF LAW
139 MacDougal Street
New York, NY 10012

Counsel for Center on Race, Inequality, and the Law

ALEX ABDO
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115

Counsel for Knight First Amendment Institute

March 25, 2019

APPENDIX

The AI Now Institute at New York University ("AI Now") is an interdisciplinary research center dedicated to understanding the social implications of artificial intelligence. As artificial intelligence and related technologies are used to make determinations and predictions in high stakes domains such as criminal justice, law enforcement, housing, hiring, and education, they will affect basic rights and liberties in profound ways. AI Now produces original research and acts as a hub for the field focused on these issues. Public records requests comprise an important source of information for AI Now.

The American Civil Liberties Union ("ACLU") is a nationwide, non-partisan, non-profit organization with approximately 2 million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Founded in 1920, the ACLU has appeared before this Court on numerous occasions, both as direct counsel and as *amicus curiae*. Documents obtained through Freedom of Information Act requests are often critical in shaping the ACLU's response on a range of important civil liberties issues.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect rights in the digital world. With over 36,000 active donors and dues-paying members, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF regularly

files Freedom of Information Act requests with federal agencies to understand government surveillance, including partnerships between law enforcement and private companies.

The Center on Race, Inequality, and the Law at New York University School of Law was created to confront the laws, policies, and practices that lead to the oppression and marginalization of people of color. Accordingly, the Center uses public education, research, advocacy, and litigation to highlight and dismantle structures and institutions that have been infected by racial bias and plagued by inequality. The Center focuses, in part, on the intersection of race, bias, the criminal legal system, and other governmental systems in which technology plays a salient role in shaping the exercise of discretion by institutional actors. Public records requests are critical to the Center's work.

The Knight First Amendment Institute at Columbia University is a non-partisan, not-for-profit organization that works to defend the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. The Institute's aim is to promote a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government. The Institute regularly relies on the Freedom of Information Act to promote government accountability.