21-1233

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

AMERICAN CIVIL LIBERTIES UNION IMMIGRANTS' RIGHTS PROJECT,

PLAINTIFF-APPELLANT,

V.

UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT,

DEFENDANT-APPELLEE.

On Appeal from the United States District Court
for the Southern District of New York
Case No. 1:19-cv-07058-GBD
The Honorable George B. Daniels, United States District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

DAVID GREENE
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
davidg@eff.org
(415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Dated: August 27, 2021

By: /s/ David Greene
David Greene

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

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 Freedom of Information Act ("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).

EFF also has a specific interest here because the case implicates two values central to its mission: individual privacy and government transparency. EFF harmonizes these values by advocating for interpretations of FOIA and other public records laws that maximize public access to government data in ways that avoid disproportionate invasions of individuals' privacy. *See Ctr. for Investigative Reporting v. DOJ*, 982 F.3d 668 (9th Cir. 2020) (serving as *amicus curiae*); *Sander*

[1] No counsel for a party authored this brief in whole or in part, and no person other than amicus or their counsel has made any monetary contributions intended to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

v. Superior Court, 237 Cal. Rptr. 3d 276 (Ct. App. 2018) (same).

INTRODUCTION

Redacting private information from government data while preserving its digital links to other information is a vital—and sometimes the only—way to protect legitimate privacy concerns while ensuring that FOIA remains a robust tool for transparency and accountability. Because the government continues to collect massive amounts of personally identifying information about the public, implicating both privacy and free speech rights, the public's right to access such non-exempt information through FOIA is essential to ensure government accountability and to expose impropriety. As explained below, there are countless examples of government data collection that pose acute risks to individual privacy and free expression.

ACLU's FOIA request harmonized these competing concerns by asking that U.S. Immigration and Customs Enforcement ("ICE") replace identifying Alien Numbers with unique identifiers that would allow ACLU to track the agency's enforcement proceedings. In holding that this redaction procedure was prohibited by FOIA because it amounted to the creation of a new record, the district court frustrated ACLU's oversight efforts. More broadly, the holding threatens to undermine the public's ability to use FOIA to obtain de-identified data that can reveal abuse or otherwise serve as the starting point for further oversight.

The district court's opinion is out of step with the realities of government data storage, and it fails to follow FOIA's command to broadly interpret its statutory disclosure requirements to further the public's right of access.

Moreover, the district court's opinion applied FOIA as if it were a rigid statute incapable of applying to digital data. That view of FOIA is doubly wrong. First, Congress explicitly amended FOIA to ensure access to government data as agencies adopt and expand their use of digital records. Second, FOIA's flexible segregability standard provides agencies and courts with tools to provide disclosure solutions just like the one ACLU proposed here.

Congress has repeatedly affirmed that the public should have access to de-identified data precisely because of FOIA's salutary purpose: exposing government use and abuse of the data it collects. In the 1996 Electronic FOIA Amendments (E-FOIA Amendments), Congress explicitly updated FOIA to require the government to "use new technology to enhance public access to agency records and information." Pub. L. No. 104-231, § 2(a)(6), 110 Stat. 3048 (1996). And in 2018, Congress required federal agencies to make much of digital government data open, usable, and machine-readable by default. Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, tit. II, 132 Stat. 5529, 5534-44 (2019) (Open, Public, Electronic, and Necessary Government Data Act) ("OPEN Data Act").

This Court should reverse and require ICE to use ACLU's replacement procedure to segregate the identifying information from the data while keeping the relational information contained in the data intact. Replacing A-numbers with unique values does not amount to the creation of new records. Further, the Court should clarify that FOIA requires agencies to explore reasonable steps, such as those ACLU proposed, to ensure the broadest public disclosure permitted by law. That outcome would ensure that FOIA can help the public understand the scope of the government's actions without intruding on the privacy of individuals whose data is found in government records systems.

ARGUMENT

I. FOIA Must Allow the Public to Monitor Massive Government Databases While Protecting Individuals' Privacy

Government agencies increasingly collect, generate, and use vast oceans of digital data that reflect both their activities and the lives of the people whom they serve. Government agencies' transition to storing peoples' records digitally thus mirrors society's broader digital transition. As a result, agencies have created massive government databases and have quickly grown pre-existing databases. Additionally, government agencies use data and data-driven algorithms to carry out their missions, meaning that agencies are relying on digital tools to make decisions affecting members of the public.

In the face of the government's digital shift, the public must still be able to learn what agencies are up to, including by relying on FOIA. *See DOJ v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 772-73 (1989). For FOIA to remain a robust accountability and oversight tool, the public must be able to use it to access electronically stored data while still balancing legitimate concerns for non-disclosure, such as individual privacy. As explained below, redaction of digital records and the substitution of unique identifiers accomplishes this goal.

A. Government Agencies Are Creating and Using Large Databases That Include Peoples' Personal and Expressive Data

Government agencies across the country, big and small, create and use databases. Agencies store data on members of the public, documents submitted for services, operational records, inventory records, and much more. Government databases often raise free expression and privacy concerns.

The Department of Homeland Security, for example, is building a biometric and biographic database called Homeland Advanced Recognition Technology (HART) that already stores large amounts of sensitive and personally identifying information. Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Facial Recognition and Peoples' "Non-Obvious Relationships,"* EFF

Deeplinks Blog (June 7, 2018);[2] U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA* (Feb. 4, 2020) ("HART PIA").[3] HART is collecting information like fingerprints, face and iris scans, and social security and A-numbers on many vulnerable people, such as "millions of applicants and petitioners seeking immigration benefits." *Id*. at 2, 32.

HART shares that and other information between all levels of government in the U.S. and foreign and international government agencies. *Id*. at 4. The government's first Privacy Impact Assessment of the database concedes that it has unmitigated risks "that data quality will not be maintained," that data will not be timely removed in accordance with retention schedules, and that "foreign partners" will violate data governance rules. *Id*. at 24, 29, 32. HART also contains records on "relationship patterns among individuals and organizations," including "non-obvious relationships," *id*. at 28, potentially impinging on associational privacy rights under the First Amendment. *See, e.g.*, *NAACP v. Alabama*, 357 U.S. 449, 466 (1958). This includes information that purports to identify "gang affiliations," HART PIA at 4, even though such data is unreliable. *See* Mick Dumke, *Chicago's*

[2] Available at https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.
[3] Available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

Gang Database Is Full of Errors—And Records We Have Prove It, ProPublica (Apr. 19, 2018).[4]

DHS also collects data to monitor immigrants' social media. Drew Harwell & Nick Miroff, *ICE Just Abandoned its Dream of 'Extreme Vetting' Software That Could Predict Whether a Foreign Visitor Would Become a Terrorist*, Wash. Post (May 17, 2018) (ICE will "hire a contractor that can provide training, management and human personnel").[5] DHS has paid more than $42 million to a contractor for what has now been rebranded as the "Visa Lifecycle Vetting" program. *Id*.[6] The program ostensibly targets visa applicants (foreign nationals), but it inevitably also collects data on the many U.S. persons who are connected to them through social media. And those Americans are disproportionately people of color and immigrants themselves. The program may be, in effect, targeting individuals for surveillance of online speech based on a protected class, such as their race, religion, or national origin, or the content of their speech.

[4] Available at https://www.propublica.org/article/politic-il-insider-chicago-gang-database.
[5] Available at https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist.
[6] *See Blanket Purchase Agreement 70CMSD18A00000003*, USASpending.gov, available at https://www.usaspending.gov/award/68975297 (accessed on Aug. 24, 2021).

And for nearly three years, DHS and the Department of Health and Human Services (HHS) tracked and shared sensitive data on the sponsors of unaccompanied immigrant children and the children themselves. In April 2018, the agencies agreed to collect and process fingerprints of potential sponsors of unaccompanied immigrant children, including their household members. Memorandum of Agreement Among ORR-HHS, ICE & CBP Regarding Consultation & Information Sharing in Unaccompanied Alien Children Matters 4–5 (Apr. 13, 2018) (rescinded by Memorandum of Agreement Among ORR-HHS, ICE & CBP Regarding Consultation & Information Sharing in Matters Relating to Unaccompanied Children (Mar. 11, 2021). The stated purpose was to determine sponsorship eligibility and to ensure the welfare of the children, *see id.*, but the federal register notice, which appears to still be active, allows ICE to use this information for enforcement and deportation purposes. Privacy Act of 1974``; System of Records, 83 Fed. Reg. 20,844 (May 8, 2018); *System of Records Notices (SORNs)*, U.S. Dep't of Homeland Sec.[7]

"Fusion centers," which multiple levels of government operate jointly, collect information from across the government and private sector. *Fusion Centers*, Dep't of Homeland Security.[8] Fusion centers' surveillance has also swept up data

[7] Available at https://www.dhs.gov/system-records-notices-sorns (accessed Aug. 24, 2021).
[8] Available at https://www.dhs.gov/fusion-centers (accessed Aug. 24, 2021).

reflecting peoples' expressive activities. Recent reporting shows that Minnesota's fusion center has collected data on the ongoing protests against the construction of a tar sands pipeline. Will Parrish, *Minnesota Law Enforcement Agency Blocks Release of Public Records About Surveilling Pipeline Opponents*, The Intercept (Aug. 7, 2021).[9] Last year, Maine's fusion center shared with local law enforcement a right-wing social media page's disinformation about a Black Lives Matter protest. Matthew Guariglia, *Maine Should Take This Chance to Defund the Local Intelligence Fusion Centers*, EFF Deeplinks Blog (Apr. 2, 2021).[10] And in 2018, the Chicago-area fusion center monitored and reported to DHS on nationwide protests against ICE. *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers*, Open the Government.[11]

Law enforcement agencies are also using body worn cameras to collect video data of the public, including sensitive and expressive details of peoples' interactions with police. Alexandra Ulmer & Julia Harte, *Explainer: How Police Body-Worn Cameras Are Used in the United States*, Reuters (Apr. 30, 2021).[12] U.S. border patrol agents will soon be wearing 7,500 cameras, after the federal

[9] Available at https://theintercept.com/2021/08/07/minnesota-pipeline-line-3-public-records.
[10] Available at https://www.eff.org/deeplinks/2021/03/eff-calls-maine-support-bill-defunds-local-intelligence-fusion-center.
[11] Available at https://www.openthegovernment.org/dhs-fusion-centers-full-report.
[12] Available at https://www.reuters.com/world/us/how-police-body-worn-cameras-are-used-united-states-2021-04-30.

government awarded a $21 million contract to a vendor for the cameras and cloud-based storage. Ted Hesson, *U.S. to Outfit Border Agents with Body Cameras in Major Oversight Move*, Reuters (Aug. 4, 2021).[13] As body cameras began proliferating several years ago, storing the massive amounts of video data they produce became an early problem for police departments, especially bigger ones generating over 10,000 hours of video a week. Josh Sanburn, *Storing Body Cam Data is the Next Big Challenge for Police*, Time (Jan. 25, 2016);[14] Bureau of Just. Assistance, *Body-Worn Camera Frequently Asked Questions*, Dep't of Just., 15 (2015) ("Video data storage is one of the most expensive aspects of body-worn camera (BWC) programs.").[15]

States and federal agencies are sharing another large set of data with each other: driver's license records. Every state's motor vehicle agency stores driver and vehicle data, and may provide it to law and immigration enforcement or sell copies to consumer data brokers and other private companies. Julie Mao, *State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy*, Just Futures Law (Mar. 2020).[16] In recent years, for example, North

[13] Available at https://www.reuters.com/world/us/us-outfit-border-agents-with-body-cameras-major-oversight-move-2021-08-04.
[14] Available at https://time.com/4180889/police-body-cameras-vievu-taser/.
[15] Available at https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/BWC_FAQs.pdf.
[16] Available at https://justfutureslaw.org/wp-content/uploads/2020/04/2020-3-5-State-DMV-Data-Sharing-Just-Futures-Law.pdf.

Carolina collected on average $41 million annually by selling DMV data. Nate Morabito, *'Data is Worth Gold Now': DMVs Sold Driver and Vehicle Records and Made $172M as a Result*, WCNC Charlotte (July 26, 2021).[17] State DMVs are taking pictures of every licensed driver and have some of the country's largest repositories of faceprints—sensitive data on people not accused of any crime or wrongdoing. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, Wash. Post (July 7, 2019).[18]

Even mundane government operations generate and store data that is relevant to public oversight. For example, the City and County of San Francisco lists 463 individual data systems, with approximately half of the systems updated with new data either daily or continuously. *Inventory of Citywide Enterprise Systems of Record*, DataSF.[19] These systems range from "Airport Museum Exhibits" to "Ankle Bracelet Monitoring" of people on probation. And across the country, counties and cities are digitizing older vital and official records, such as birth and death certificates and property records. *See, e.g.*, Emily Alpert Reyes, *Many L.A. Building Records Now Just a Few Clicks Away*, L.A. Times (Jun. 18,

[17] Available at https://www.wcnc.com/article/money/dmvs-sold-driver-vehicle-records-172-million/275-ab069cc3-a646-481c-a1a4-622d1e443180.
[18] Available at https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches.
[19] Available at https://data.sfgov.org/City-Management-and-Ethics/Inventory-of-citywide-enterprise-systems-of-record/ebux-gcnq/data (accessed Aug. 25, 2021).

2015) (noting the Los Angeles Department of Building and Safety digitized "more than 13 million records dating back to 1905").[20]

B. Unique Identifiers are Among the Tried-and-True Methods for Balancing Transparency and Privacy in Records Disclosures

The massive government databases described above cry out for public oversight, both to monitor government operations generally and their collection of personal data specifically. FOIA provides robust avenues for public scrutiny, requiring the release of digital records in a format of the requester's choosing, including privacy-protective forms like aggregate data, and allowing redaction only of exempt portions of records. 5 U.S.C. § 552(a)(3)(B), (a)(8); *see Ctr. for Investigative Reporting*, 982 F.3d at 690-93 (holding that E-FOIA amendments, including § 552(a)(3)(B), required disclosure of aggregate data). Government agencies, researchers, and data experts have demonstrated several methods, including the redaction method in this case, that harmonize FOIA's goals of disclosing government records while preventing disproportionate invasions of peoples' privacy.

Rather than withhold data from the public entirely, government agencies already use methods to obscure, reformat, or rearrange records to communicate

[20] Available at http://www.latimes.com/local/lanow/la-me-ln-online-building-records-20150618-story.html.

their substance while avoiding disclosure of information with a high risk of identifying people. Disclosing data in a privacy-protective form, such as by substituting unique identifiers, thus affords public access and scrutiny of the government's massive data gathering efforts without identifying the people whose data, often personal and expressive, those systems contain.

The California Health and Human Services Agency ("CHHS") established de-identification guidelines to allow public access to certain datasets while still complying with all laws and patient protections, including the de-identification requirements in the federal Health Insurance Portability and Accountability Act. *Data De-identification Guidelines (DDG)*, Cal. Dep't of Health Care Services (Nov. 22, 2016).[21] The guidelines provide statistical masking techniques including aggregation, reducing granularity, and splitting up tables to reduce dimensions. *Id.* at 39. For example, age ranges that span 2 years carry a higher identification risk than those that span 5 years, as the latter is less granular. *Id.* at 18. The CHHS de-identification process is more involved than that proposed by ACLU, but it necessarily accomplishes the same goal: greater disclosure of government data.

The CHHS open data portal provides de-identified records that are valuable to the public, public health officials, journalists, and others. For example, the portal

[21] Available at https://www.dhcs.ca.gov/dataandstats/Documents/DHCS-DDG-V2.1-010821%20(1).pdf.

provides data on the rates of certain diseases, such as the number of cases of antibiotic-resistant staph infections for each hospital in a given year,[22] the demographics of individuals who access healthcare services, including applicants for insurance affordability programs by country of origin,[23] and the dosing and distribution of COVID-19 vaccines by county and various demographics.[24]

Government agencies have also released blurred video records, which can prevent identification of people captured in the video while providing the recording's context. Law enforcement agencies, for example, have experimented with releasing blurred body worn camera video. Jerod Macdonald-Evoy, *Tempe Blurs All Police Body Camera Footage Public Records Requests*, AZ Mirror (Mar. 20, 2020);[25] David Kravets, *Seattle Police Unveil Blurred, Soundless Body Cam YouTube Channel*, Ars Technica (Mar. 2, 2015).[26] The federal FOIA ombudsman

---

[22] *Methicillin-Resistant Staphylococcus Aureus (MRSA) Bloodstream Infections (BSI) in California Hospitals*, CHHS Open Data, available at https://data.chhs.ca.gov/dataset/methicillin-resistant-staphylococcus-aureus-mrsa-bloodstream-infections-bsi-in-california-hospitals (accessed Aug. 25, 2021).
[23] *Ethnicity of Applicants for Insurance Affordability Programs*, CHHS Open Data, available at https://data.chhs.ca.gov/dataset/dhcs_ethnicity-of-applicants-for-insurance-affordability-programs (accessed Aug. 25, 2021).
[24] *COVID-19 Vaccine Progress Dashboard Data*, CHHS Open Data, available at https://data.chhs.ca.gov/dataset/vaccine-progress-dashboard (accessed Aug. 24, 2021).
[25] Available at https://www.azmirror.com/2020/03/20/tempe-blurs-all-police-body-camera-footage-public-records-requests.
[26] Available at https://arstechnica.com/tech-policy/2015/03/seattle-police-unveil-blurred-soundless-body-cam-youtube-channel.

recommends using the "least obtrusive redaction option" when releasing videos, including blurring and "artificially modulat[ing] the voices of individuals who appear on screen." *Best Practices for Video Redaction*, Off. of Gov't Info. Servs. (July 29, 2021).[27] Like blurring, voice modulation can disclose substantive information from the underlying record, such as words spoken, speed, and inflection. Similarly, Washington, D.C.'s government transparency ombudsman found that the city's open records law, modeled after FOIA, requires release of body worn camera videos after "redaction (i.e. blurring out)" of, among other things, the faces of officers and third parties. *See FOIA Body Worn Cameras Advisory Opinion*, Wash., D.C. Off. of Open Gov't (Nov. 5, 2020).[28]

The methods described above could be used to allow greater access to government data that reflects controversial programs or activities. For example, DHS's HART database includes biometric and other sensitive data on a person through the course of their tracked immigration activities—entering the country, applying for benefits, encountering law enforcement, and so on. Records released with unique identifiers would allow the public to map these data trails without directly identifying any person. The resulting public data could allow the public to learn whether the government is focusing on individuals with protected

[27] Available at https://www.archives.gov/ogis/about-ogis/chief-foia-officers-council/tech-comm-video-redaction-bp-07-29-2021.
[28] Available at https://www.open-dc.gov/BWC_FOIA_AdvisoryOpinion_2020.

characteristics or associations, or when and why the government is collecting different types of data.

Replacing personally identifying information with unique identifiers would similarly show what characteristics or associations the government is attempting to find through social media monitoring in DHS's "Visa Lifecycle Vetting" program. The public could see for how long and on how many social media accounts the government is surveilling a particular unidentified person.

II. Substituting Unique Identifiers for A-Numbers is a Form of Redaction Under FOIA That Maximizes Disclosure of the Responsive Records

The district court incorrectly held that FOIA barred ACLU's proposed method of removing personal information from the data it seeks. Rather, FOIA's purpose is to ensure "broad disclosure," which is why Congress required that exemptions and other limitations on public access "be 'given a narrow compass.'" *Milner v. Dep't of the Navy*, 562 U.S. 562, 571 (2011) (quoting *DOJ v. Tax Analysts*, 492 U.S. 136, 151 (1989)).

The above examples show that government agencies can disclose government data to enable greater oversight while protecting privacy, which ACLU seeks to do in this case. Given FOIA's heavy presumption of public access, its segregability provisions provide ample authority to permit ACLU's request.

A. FOIA's Segregability Provisions Require Agencies to Use a Redaction Method That Extricates Non-Exempt Information

FOIA requires the government to disclose all non-exempt information, including partial information where full disclosure of a record is not possible. 5 U.S.C. § 552(a)(8). Agencies must take reasonable steps to release partial information from a record by redacting exempt information but still disclosing as much of the responsive record as possible. These "reasonable" methods of redaction can vary for digital records—the agency can mute or modulate audio, delete video frames, crop or blur parts of a video, or replace text with different text or a black bar.[29] *See Evans v. Fed. Bureau of Prisons*, 951 F.3d 578, 587 (D.C. Cir. 2020) (discussing blurring of exempt parts of responsive video records and requiring the government "to meet the same sort of segregability standards typically applied to printed material"); *Stahl v. DOJ.*, 2021 WL 1163154, at *6 (E.D.N.Y. Mar. 26, 2021) ("[J]ust as defendants could redact an individual's name from a document, they could blur the faces of the medical staff, crop the videos, or even isolate screenshots.").

Agencies must redact only exempt information, and "non-exempt portions of a [record] must be disclosed unless they are inextricably intertwined with exempt portions." *Trans-Pac. Policing Agreement v. U.S. Customs Serv.*, 177 F.3d 1022,

[29] Here, the government has conceded that ACLU's proposed method of redaction would not be unreasonably burdensome.

1027 (D.C. Cir. 1999) (quoting *Mead Data Cent., Inc. v. U.S. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977)); *Evans*, 951 F.3d at 587 ("[T]he government is required to explain why the possibility of some similar method of segregability is unavailable if it is to claim the protection of the exemption."); *see also Am. Immigr. Laws. Ass'n v. Exec. Off. for Immigr. Rev.*, 830 F.3d 667, 670 (D.C. Cir. 2016) ("[W]e find no statutory basis for redacting ostensibly non-responsive information from a record deemed responsive."). If a particular redaction method more effectively extricates non-exempt portions of a record, then an agency must use it.

Because FOIA requires that an agency may only redact a record to the extent justified by the underlying exemption, redaction is not an all-or-nothing proposition. Even a black bar can reveal some information, like the length of words. Declan Butler, *Censored Words Unmasked*, Nature (May 13, 2004).[30] For example, accepting that an identifying commercial number was exempt but that each digit provided "a greater degree" of information relevant to the requester, the D.C. Circuit found that redaction was appropriate only for the digits that caused the "competitive harm" at issue. *Trans-Pac. Policing Agreement*, 177 F.3d at 1027. Certainly, there are situations in which redactions cannot "avoid the harms that could result from disclosure of the information in full." *See ACLU v. DOJ*, 681

[30] Available at https://www.nature.com/articles/news040510-8.

F.3d 61, 71-72 (2d Cir. 2012). But that is not the case here. The government conceded that ACLU's method would prevent the disclosure of identifying information in the A-numbers.

In light of the foregoing, ACLU's proposal is a workable solution to address privacy concerns and is required by FOIA's segregability provisions. Indeed, ACLU's proposal to substitute the A-numbers in the responsive records with unique identifiers is legally indistinguishable from other redaction methods that withhold only the information exempt from disclosure under FOIA. And FOIA's segregability provisions require such narrow redactions, rather than withholding the data in full. As ACLU explains in its brief, A-numbers convey both personally identifying information and relational information that link records about ICE interactions with the same person. ACLU Opening Brief (ECF No. 31) at 6 ("AOB"). ACLU's proposal extricates the relational information from the A-number and redacts the identifying information.

B. Substituting Unique Identifiers for Personal Identifiers Does Not Create a New Record

Redaction methods required by FOIA's segregability provisions may modify or manipulate the underlying information in a record without creating a new record. To the contrary, numerous courts have ordered agencies to manipulate data—including through unique identifiers—to redact and release records. For

example, blurring a face or other portions of a video can permit the disclosure of records under FOIA. *Evans*, 951 F.3d at 587. The process of blurring an individual's face appearing in a video is technically a manipulation of the underlying record—it replaces pixels in the video with a new value. Blurring redacts identifying data, but it retains contextual data, which can indicate, for example, that the same person, tracked but not identified by a blurred face, appears throughout the video.

What ACLU seeks to do here is the equivalent of blurring data in the ICE database, as the unique identifiers serve to sever the identifying information (akin to a face in a video) while maintaining the data's relationship throughout ICE's records (akin to tracking the de-identified person throughout a video). Indeed, ACLU persuasively shows how cases requiring blurring of video sought under FOIA, such as *Evans* and *Stahl*, apply and require ICE to replace A-numbers with unique identifiers. AOB at 35-36, 44-45.

Moreover, as far back as 2009, a federal court under FOIA ordered the government to obscure and release videos used as evidence in a death penalty case. *Prison Legal News v. Exec. Off. for U.S. Att'ys*, 2009 WL 2982841, at *4 n.8 (D. Colo. Sept. 16, 2009), *appealed on other grounds*, 628 F.3d 1243, 1247 n.1 (10th Cir. 2011). The court ordered portions of the video that depicted two individuals' genitalia "electronically or otherwise obscured to preserve their privacy interests."

Id.

Similarly, a federal court ordered the government to release gun trace data under FOIA, holding that obscuring specific information would protect exempt information while still permitting disclosure of government data. *City of Chicago v. ATF*, 2001 WL 34088619, at *1 (N.D. Ill. Mar. 8, 2001), *rev'd on other grounds*, 423 F.3d 777 (7th Cir. 2005). The city wanted to "track the relationship between guns recovered in connection with crime, gun purchasers and gun manufacturers" by knowing "that a particular individual purchased the recovered weapon, not the identity of that individual," nor "the exact identifying serial number." *Id*. at *5.

Although the Seventh Circuit reversed on grounds similar to this Court's decision in *Everytown for Gun Safety Support Fund v. ATF*, 984 F.3d 30 (2d Cir. 2020), it did not decide whether FOIA required disclosure of the relational information in ATF data. *See City of Chicago*, 423 F.3d at 779-83 (holding that Congress exempted information from disclosure). Like the ACLU here, the City of Chicago wanted the relational information. The district court ordered encryption, rather than deletion, of the names and serial numbers because "[e]ncryption deletes sensitive information, such as exact identity, by obscuring it, while retaining useful information." *City of Chicago*, 2001 WL 34088619, at *5 ("Encryption is a modern form of computer deletion for redaction purposes."). *Accord Ctr. for Investigative Reporting*, 982 F.3d at 690-93 (requiring disclosure of aggregate ATF data).

State courts have similarly required modifications to public data to ensure the broadest possible public disclosure. The California Supreme Court, for example, has found that the substitution of unique identifiers is a type of redaction under the California Public Records Act, which is modeled on FOIA. *ACLU v. Superior Ct.*, 400 P.3d 432, 436 (Cal. 2017). There the plaintiffs (including EFF) sought data on police use of automated license-plate readers ("ALPR"). *Id*. at 434. The court held that "anonymization and redaction methods" could address the privacy and safety interests of "everyone associated with a scanned plate" and allow for the release of records that "would be helpful in determining the extent to which ALPR technology threatens privacy." *Id*. at 440, 441. The court found, for example, that "replacing actual license plate numbers with . . . unique (fictional) number[s]" rather than "simply removing the plate numbers altogether" would be more "informative." *Id*. at 441.

The Supreme Court of Illinois ordered a school district to release test scores, with manipulated data to avoid identifying individual students, to parent requesters under FOIA. *Bowie v. Evanston Cmty. Consol. Sch. Dist. No. 65*, 538 N.E.2d 557, 561 (Ill. 1989) (citing *Kryston v. Board of Education, East Ramapo Central School District*, 77 A.D.2d 896, 897 (N.Y. App. Div. 1980)). Although disclosure would require the school district to delete student names, randomly rearrange students test scores, and replace demographic information, those procedures did not create a

new record because "the district is only being required to delete the exempt matter, protecting the student's privacy, and disclose the nonexempt portion of the record." *Id*. at 561.

And a court discussing redaction methods under Oregon's state public records law, which was modeled on FOIA, *see Marks v. McKenzie High Sch. Fact-Finding Team*, 878 P.2d 417, 423 (Or. 1994), noted that "predetermined names of companies, experimental medications, and staff could be electronically deleted or replaced by initials, code words, or other obscuring information." *In Def. of Animals v. Oregon Health Scis. Univ.*, 112 P.3d 336, 353 n.15 (Or. Ct. App. 2005).

These cases demonstrate that FOIA's segregability provisions require extricating as much non-exempt information from a responsive record as reasonably possible, including by data manipulation. Substituting unique identifiers as ACLU proposes does just that, and FOIA requires ICE to use it and disclose the remaining records.

C. This Court Should Construe FOIA Broadly in Light of Congress Repeatedly Mandating Greater Public Access to Digital Data

The district court's decision also failed to appreciate that Congress has repeatedly mandated that government agencies do more to make their data publicly available, both under FOIA and the OPEN Data Act. In refusing to allow ACLU to replace A-numbers with de-identified values, the district court ignored Congress'

concerted efforts to require that agencies foster public access to data to the greatest extent possible. Moreover, the decision below implicitly allowed ICE's failure to meet Congress' data transparency mandates to serve as an excuse to foreclose public access here. That result creates perverse incentives: federal agencies that fail to maintain readily disclosable records systems can use that failure as an excuse to avoid their disclosure obligations under FOIA. This Court should avoid endorsing that result.

Starting with the E-FOIA Amendments, Congress required government agencies to "use new technology to enhance public access to agency records and information" and to "maximize the usefulness of agency records and information collected, maintained, used, retained, and disseminated by the Federal Government." Pub. L. No. 104-231, § 2(a)(6), (b)(4), 110 Stat. at 3048-49. The key operative provision of the E-FOIA Amendments requires that in response to a FOIA request, "an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format." Pub. L. No. 104-231, § 5, 110 Stat. at 3050. That provision required agencies to take necessary, reasonable steps to store data in ways that could be easily disclosed to the public.

Further, Congress' passage of the OPEN Data Act in 2018 reaffirms that ICE has an obligation to design its systems in a way that encourages public

disclosure. Like the E-FOIA Amendments, the OPEN Data Act recognized that electronic government data has proliferated. Congress asserted that "[m]anaging Federal Government data to make it open, available, discoverable, and usable to the general public, businesses, journalists, academics, and advocates promotes efficiency and effectiveness in government . . . and more importantly, strengthens our democracy." OPEN Data Act, § 2(a)(1). The law requires the federal government to make data "open by default" and "machine-readable." *Id*. at § 202(b)-(c).

Thus, in addition to ICE's legal claims lacking merit under FOIA, the record here demonstrates that the agency is not complying with Congress' command in the E-FOIA Amendments to "maximize the usefulness of agency records." *See* AOB at 9-11. Nor has ICE complied with the OPEN Government Data Act's text or purpose. Instead, the agency appears to have set up its records systems in such a way that frustrates efforts, like those ACLU's, to disclose ICE's records. ICE's failure to follow the E-FOIA Amendments should not excuse it from its disclosure obligations, however. And as the ACLU has shown, ICE can easily and quickly run the replacement script. AOB at 11.

This Court should not permit ICE to use its own failures—namely, to comply with Congress' command to make its records systems open by default—as an excuse to avoid ACLU's FOIA request here. Such an outcome would both blunt

public access in this case and reward federal agencies for their failure to adopt database management practices that would increase public access.

CONCLUSION

For the foregoing reasons, EFF respectfully requests that this Court reverse the district court and order ICE to comply with ACLU's FOIA request.

Dated: August 27, 2021

Respectfully submitted,

/s/ David Greene
David Greene
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
davidg@eff.org
(415) 436-9333

Attorneys for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Plaintiff-Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,380 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); 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 2016, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: August 27, 2021

By: /s/ David Greene
David Greene

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I certify that on this 27th day of August 2021, I electronically filed the foregoing Brief of Amicus Curiae using the Court's CM/ECF system which will send notification of such filing to all parties of record.

Dated: August 27, 2021

By: /s/ David Greene
David Greene

Counsel for Amicus Curiae
Electronic Frontier Foundation