Caitlin Bellis, Esq. (SBN 304764)
cbellis.clinic@law.uci.edu
Anne Lai, Esq. (SBN 295394)
alai@law.uci.edu
Immigrant Rights Clinic
University of California, Irvine School of Law
PO Box 5479
Irvine, CA 92616-5479

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UCI LAW SCHOOL IMMIGRANT RIGHTS CLINIC & JUST FUTURES LAW, Plaintiffs, vs. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, Defendant	Case No.: 8:20-cv-01188 COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for injunctive and other appropriate relief, seeking the immediate processing and release of agency records improperly withheld by Defendant United States Immigration and Customs Enforcement ("ICE") in response to a FOIA request submitted by Plaintiffs Just Futures Law ("JFL") and University of

California, Irvine School of Law Immigrant Rights Clinic ("UCI IRC") (collectively, "Plaintiffs").

2. Palantir is a private corporation that sells systems that mine, analyze, and categorize large amounts of data.[1]

3. ICE, one of the largest law enforcement agencies in the United States, increasingly relies on a variety of surveillance technologies supplied by private corporations like Palantir. Little public information is available about these technologies, which collect staggering amounts of sensitive, personally identifying information about millions of people each year.

4. ICE relies on Palantir's electronic databases in particular to collect and then use vast amounts of data about people, ranging from hair color to tattoos

---

[1] Palantir was named after a magical artifact used by villains in J.R.R. Tolkien's *Lord of the Rings* to see events in other places and times. Tolkien's Palantir is used by various characters to deceive and control others, conceal secrets, and misrepresent the truth. Max Slater-Robins, *Big Data Company Palantir has Raised Another $129 Million in Funding*, Business Insider (Dec. 10, 2015) https://www.businessinsider.com/palantir-raises-129-million-2015-12; Palantir has purportedly created an algorithm that can predict crime. This was deployed in New Orleans and Los Angeles. *See* Issie Lapowsky, *How the LAPD Uses Data to Predict Crime*, Wired (May 22, 2018) https://www.wired.com/story/los-angeles-police-department-predictive-policing/; Ali Winston, *Palantir Has Secretly Been Using New Orleans to Test its Predictive Policing Technology*, The Verge https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

to a person's location and private relationships.[2] The public needs to understand these rapidly advancing technologies to meaningfully participate in shaping the scope and bounds of government surveillance of people living within the United States.

5. ICE's use of Palantir's surveillance and data analysis systems implicates core privacy and Fourth Amendment issues; shapes the implementation of immigration policies; may propagate erroneous information; and costs the United States at least $90 million dollars.[3]

6. On October 4, 2019, Plaintiffs submitted a FOIA seeking records related to ICE's Palantir data mining and surveillance systems, the Investigative Case Management system ("ICM") and FALCON Search & Analysis system (together, "the Palantir systems").

---

[2] Peter Waldman, Lizette Chapman, & Jordan Robertson, *Palantir Knows Everything About You,* Bloomberg (April 19, 2018) www.bloomberg.com/features/2018-palantir-peter-thiel (describing Palantir as a "spy brain" that has records of every person's emails, home address, online habits, appearance—a single image can bring up a string of related contacts including such as labels as "'colleague of,' 'lives with,' 'operator of [cell number],' 'owner of [vehicle],' 'sibling of,' or even 'lover of.'")

[3] Mijente, *The War Against Immigrants: Trump's Tech Tools Powered by Palantir,* (Aug. 2019), https://mijente.net/wp-content/uploads/2019/08/Mijente-The-War-Against-Immigrants_-Trumps-Tech-Tools-Powered-by-Palantir_.pdf; Emily Birnbaum, *ICE renew contract with Palantir*, (Aug. 20, 2019), https://thehill.com/policy/technology/458170-ice-renews-contract-with-palantir

7. To date and past the statutory deadline, ICE has not produced any documents in response to Plaintiffs' request.

8. Plaintiffs now file suit under FOIA for declaratory and injunctive relief, seeking the immediate disclosure of the requested records.

JURISDICTION

9. This Court has both subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331.

10. Venue lies in this district under 5 U.S.C. § 552(a)(4)(B).

11. Plaintiffs have exhausted all administrative remedies in connection with this FOIA request.

PARTIES

12. Plaintiff UCI IRC provides pro bono legal services to clients in immigration, employment and civil rights matters. Students work under faculty supervisors who are licensed attorneys. UCI IRC also engages in non-litigation advocacy work and community education to advance immigrants' rights. For example, UCI IRC has produced reports and commentary on immigrants' rights issues, which it makes available to the public at no cost on its website, www.law.uci.edu/academics/real-life-learning/clinics/immigrantrights.html. Recently, UCI IRC published a report on the state of immigration enforcement in

Orange County, *see* https://www.law.uci.edu/news/in-the-news/2019/irc-oc-immigration.html, and collaborated with Just Futures Law on a Policy Toolkit directly related to ICE's use of surveillance technologies, including Palantir products. The Toolkit is likewise publicly available. *See* https://justfutureslaw.org/wp-content/uploads/2019/07/Tech-Policy-Report_v4LNX.pdf.

13. Plaintiff Just Futures Law is an organization that provides legal support for grassroots organizations engaged in making critical interventions in the United States' deportation and detention systems.[4] JFL employs litigation, education, legal support, and policy advocacy strategies to advance their goals in mitigating or eliminating harsh immigration enforcement and biased immigration policies and policing. In July 2019, JFL published a report "*Blueprint for Terror*" on behalf of Detention Watch Network and Mijente after reviewing documents produced during FOIA litigation on the planning of the biggest immigration enforcement action in ICE history, "Operation MEGA."[5] Several of these FOIA

---

[4] JFL launched in July 2019 and is fiscally sponsored by the Immigrant Legal Resource Center, a nonprofit organization that provides education and training tools in the area of immigration law.

[5] *See Blueprint for Terror: How ICE Planned its Largest Immigration Raid in History*, Mijente (July 3, 2019), https://mijente.net/icepapers/.

productions referred to FALCON and ICM systems utilized in various immigration enforcement operations, such as Operation Safe Cities, Operation Raging Bull, Operation MEGA, and many others. JFL's report was covered by mainstream news outlets and was disseminated through social media.[6] Additionally, JFL has partnered with UCI IRC to publish the policy toolkit described above and conducted trainings about the role of corporate contracting in ICE enforcement.

14. ICE is a component of the U.S. Department of Homeland Security ("DHS"), and an "agency" within the meaning of 5 U.S.C. § 522(f)(1). ICE is headquartered in Washington, D.C. and has field offices around the country.

---

[6] JFL's report was recently reviewed in a New York Times article, *How ICE Picks its Targets in the Surveillance Age*, N.Y. Times (October 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html; *See also* Adam Harris, *When ICE Raids Homes*, The Atlantic (July 17, 2019), https://www.theatlantic.com/family/archive/2019/07/when-ice-raids-homes-immigration/594112/; Brittany Johnson, *Documents Shed Light on ICE Target Lists and Arrest Quotas in Utah*, ABC4 News (July 13, 2019), https://www.abc4.com/news/documents-shed-light-on-ice-target-lists-and-arrest-quotas-in-utah/;. Scott Bixby, *ICE Told Agents 'Happy Hunting!' as They Prepped for Raid*, The Daily Beast (July 3, 2019) https://www.thedailybeast.com/ice-told-agents-happy-hunting-as-they-prepped-for-raid; Maryam Saleh, *As Trump Announces Mass Immigration Raid, Documents Show How ICE Uses Arrest Quotas*, The Intercept (July 3, 2019), https://theintercept.com/2019/07/03/ice-raids-arrest-quotas/; Emma Ockerman, *"It's Gonna be EPIC!" Internal Emails Show ICE Agents Were Amped for Massive Raid*, VICE (July 3, 2019), https://www.vice.com/en_us/article/9kx797/its-gonna-be-epic-internal-emails-show-ice-agents-were-amped-for-massive-raid.

FACT BACKGROUND

15. The Freedom of Information Act protects the public's right to be informed about vital public policy issues, such as those raised by ICE's use of the Palantir systems, which implicates constitutional rights, immigration policies, and government spending.

16. The Palantir systems collect and analyze a wide range of data sourced from private companies (including social media platforms), government agencies, and law enforcement surveillance.[7] The data collected includes financial information, photographs (including but not limited to Facebook pictures, DMV photographs, and images recorded by ICE agents), video (including but not limited to private surveillance camera footage and agents' field recordings), emails, phone records, text messages, license plate numbers, location data, and biometric data such as hair color and tattoos.[8]

---

[7] U.S. Department of Homeland Security, *Privacy Impact Assessment for ICE Investigative Case Management,* 9 (June 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf; Spencer Woodman, *Palantir Provides the Engine for Donald Trump's Deportation Machine*, The Intercept (Mar. 2, 2017), https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

[8] Adam Mazmanian, *ICE Extends Palantir's Case Management Contract,* Federal Computer Week (Aug. 21, 2019), https://fcw.com/articles/2019/08/21/palantir-ice-sole-source-extension.aspx

17. In short, using Palantir technology, ICE can access almost all of a person's identifying information, from the contours of their face to the scope of their social network to the location of their car.

18. The Palantir systems collect data and make it immediately available to ICE agents working in the field or office.[9] Using this data, ICE builds "Subject Records" specific to particular individuals. A Subject Record is a virtual file containing all information even tenuously related to a person, including their personal information, including name, birth date, and address, biometric data, biometric data, whereabouts, and relationships.

19. ICE then uses these Subject Records to investigate and prosecute civil and criminal immigration cases and other criminal cases. ICE provides little information to permit the public to assess how the Palantir systems, and the Subject Records derived therefrom, conform to U.S. law, including Constitutional requirements.

---

[9] U.S. Department of Homeland Security, *Privacy Impact Assessment for the FALCON Search & Analysis System,* 1 (January 16, 2014), https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf

20. DHS has released a Privacy Impact Assessment relating to these systems, conceding a variety of privacy and other public policy concerns.[10] Yet the only oversight of these vast and powerful systems of data collection and analysis comes from an internal DHS component, the ICE Office of Professional Responsibility ("OPR"). The specific nature of OPR's oversight of the Palantir systems is not public, however. ICE asserts that employees with access to the Palantir systems are "trained," but the content of that training is also not public.[11]

21. Neither Palantir nor ICE are transparent about their relationship, and FOIA requests are the only way for the public to learn about how ICE uses the Palantir systems. Palantir has previously denied involvement with ICE's interior enforcement, and the public only learned of its key role in deportation after ICE was forced to divulge information in response to a 2017 FOIA request led by the American Immigration Council in partnership with other immigration rights groups.[12]

---

[10] U.S. Department of Homeland Security, *Privacy Impact Assessment for ICE Investigative Case Management,* 21 (June 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf

[11] *Id*. at 1.

[12] Rosalie Chan, *Protestors Blocked Palantir's Cafeteria to Pressure the $20 Billion Big Data Company to Drop its Contract with ICE*, Business Insider (Aug.

22. The public has an interest in assessing whether ICE protects privacy and adheres to Fourth Amendment requirements; how the Palantir systems affect the implementation and enforcement of federal immigration policy; how ICE ensures that Subject Records derived from the Palantir systems are based on accurate data; and what ICE has spent over $90 million dollars to purchase.

A. The Public Has a Vital Interest in Understanding How ICE's Use of Surveillance and Data Analysis Technologies Impacts Privacy.

23. The Palantir systems are able to access unprecedented quantities of personal data and use complex algorithms to categorize and aggregate that data. The public has an interest in defining the limits of how, where, and when the government can surveil residents, what private information the government can obtain, and how the government ensures data is stored securely and used in a manner that is consistent with constitutional and other legal limitations.

24. The Palantir systems collect and share data on noncitizens and citizens alike, and they contain data about third parties who are not the target of any legitimate law enforcement investigation.[13]

16, 2019), https://www.businessinsider.com/palantir-protest-palo-alto-activists-ice-contracts-2019-8.

[13] *Id.* at 9.

25. Because the Palantir systems can draw data from so many sources—including government agencies, commercial sources, and individual ICE agents—they risk collecting more data than necessary, including collecting private information that is not reasonably related to any legitimate investigative purpose. ICE agents can mine, store, and view the private information of individuals who have no connection to any investigation.[14]

26. ICE shares information derived from the Palantir systems with a large number of outside agencies, individuals, and commercial partners. Thus, ICE's use of these systems creates real risks of unauthorized access to, inappropriate use of, or disclosure of personal information contained in the Palantir systems. The public also does not know whether there are restrictions on Palantir's ability to use or share the data that ICE inputs into the Palantir systems and/or directs Palantir to gather.

27. ICE has never released any public information about what events trigger the creation of a Subject Record or other forms of digital surveillance, under what circumstances, if any, ICE and/or Palantir discontinues or deletes a

---

[14] *Id.* at 23; 27.

Subject Record, or what limits, if any, ICE places on who it surveils and how ICE uses the data it gathers.

28. The Palantir systems provide ICE agents with the power to gather and weaponize personal, sensitive information, and the public has an interest in understanding what training and supervision controls an ICE agent's use of this invasive technology. Using the Palantir systems, an ICE agent could record an interaction with a person they encounter who is wearing an "Abolish ICE" shirt. The agent could then open a Subject Record on the person, upload an image of the person's face (to be analyzed with facial recognition software) and potentially other biometric data; and also access and compile into one record their social media and other private online activity to probe their personal relationships, job, home address, and hobbies. The agent could input the person's license plate and could track that person's location indefinitely.

29. ICE can use the Palantir systems to perform searches and gather private information in ways that may circumvent constitutional protections. The Palantir systems are capable of compiling information that in other contexts would require a warrant, a process that includes several safeguards ensuring credible information has led to a reasonable finding of probable cause. Immigrant communities are already especially vulnerable to violative investigations because it is difficult to challenge such investigations in the immigration court system.

Respondents in immigration court often lack representation; discovery in immigration court is limited; and the remedy of suppression is often unavailable.[15] That is if the individual subject to a bad investigation makes it to court – noncitizens are often placed in expedited proceedings short of a hearing, and removed without any recourse for errors or legal violations that occurred during their cases. In part due to the vulnerability of this targeted community and its members' lack of access to meaningful legal recourse, there is a heightened public interest in understanding and holding ICE accountable for its use of the Palantir systems.

30. The public has no information about the extent of the information ICE can collect on a single person.

31. The public has no information about how many or which people ICE is currently tracking, or the process for selecting a target of investigation.

32. The public has no information about how ICE safeguards against breaches of its data, or how it regulates the sharing of that data among government agencies and outside partners.

---

[15] 8 U.S.C. § 1229a(b)(4)(A); 8 U.S.C. § 1229a(b)(4)(B); *Immigration & Naturalization Serv. v. Lopez-Mendoza*, 468 U.S. 1032 (1984).

33. FOIA protects the public's right to be informed about how ICE is using new technology to surveil citizens and noncitizens residing in the United States.

B. The Public Has a Vital Interest in Participating in Democratic Debate About the Ways that ICE Uses Palantir Technology to Implement and Enforce Immigration Policy.

34. ICE uses the Palantir systems to weaponize private information, personal relationships, and recorded surveillance against immigrant communities. Immigration policy is a constantly changing, central issue in American democracy. Timely access to information is essential in this context. For example, timely information about policies like "Zero Tolerance" (which led to thousands of family separations at the border) sparked public outcry and resulted in important policy changes.[16] ICE is not simply using the Palantir systems to implement old policy more efficiently; the capacity these systems give ICE leads to the creation of new agency policies and allow ICE to carry out controversial new missions. The public has a vital interest in understanding these systems and the new policies and practices that result.

---

[16] Southern Poverty Law Center, *Family Separation Under the Trump Administration—A Timeline,* (Sept. 24, 2019) https://www.splcenter.org/news/2019/09/24/family-separation-under-trump-administration-timeline

35. ICE has frequently used the Palantir systems for controversial new practices. In a 2017 operation, ICE used the Palantir systems to target the families of migrant children. Agents were instructed to document interactions with unaccompanied minors attempting to enter the United States. Agents detained the children in shelters, and when families came forward to claim their children, ICE arrested the undocumented members of that child's family. ICE told its agents to use the data for the purpose of bringing criminal smuggling charges against the minors' parents or sponsors living in the United States, as part of the Trump administration's family separation plan. The Palantir systems allowed agents to upload recordings of children, create Subject Records for the minors and their US contacts, then prosecute any undocumented person attempting to help the minor. [17]

36. In addition to changing *how* ICE prosecutes immigration violations, the data analysis algorithms could play a role in determining *whom* ICE targets for prosecution. The public has no information about the role Palantir systems play in determining when an investigation is triggered. Algorithms—though they may

---

[17] Douglas MacMillan and Elizabeth Dwoskin, *The War Inside Palantir: Data-mining Firm's Ties to ICE Under Attack by Employees*, The Washington Post (August 22, 2019) https://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/; Mijente, *Palantir Played a Key Role in Arresting Families for Deportation, Document Shows,* (May 2, 2019) https://mijente.net/2019/05/palantir-arresting-families/

appear impartial on the surface—incorporate the biases of their creators, including and especially insidious forms of racial and gender discrimination.[18] The public has an interest in understanding how these algorithms categorize data, create matches, and select targets.[19]

37. The public has a right to understand ICE's contract with Palantir, a company often referred to as secretive, and to have sufficient information to assess ICE's use of the Palantir systems to implement controversial immigration policy in novel ways with far-reaching consequences.[20]

C. The Public Has a Vital Interest in Understanding How ICE Ensures Accuracy in its Use of the Palantir Systems.

38. There is a substantial risk that information in the Palantir systems could be inaccurate because so many of the sources from which the systems collect

---

[18] Amina Khan, *When computers make biased health decisions, black patients pay the price, study says*, Los Angeles Times, (Oct. 24, 2019) https://www.latimes.com/science/story/2019-10-24/computer-algorithm-fuels-racial-bias-in-us-healthcare

[19] Craig Smith, *Dealing with Bias in Artificial Intelligence,* The New York Times, (Nov. 19, 2019) https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html

[20] Mark Harris, *How Peter Thiel's Secretive Data Company Pushed Into Policing,* Wired (Aug. 9, 2017), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/; Rosalie Chan, *Here's what you need to know about Palantir, the secretive $20 billion data-analysis company whose work with ICE is dragging Amazon into controversy,* Business Insider (July 19, 2019), https://www.businessinsider.com/palantir-ice-explainer-data-startup-2019-7.

data are prone to human error or are not properly verified. Additionally, algorithms could produce false matches or incorrectly flag a person as a target.[21] The consequences of an error in the Palantir systems are wide-reaching, because the systems act to choreograph programs across government agencies. If an ICE agent erroneously flags someone as a target or wrongdoer, that person will automatically be flagged in other connected systems used by Customs and Border Protection ("CBP"), United States Citizenship and Immigration Services, Homeland Security Investigations, and potentially by outside agencies. To a Border Patrol Agent opening that same person's file, it may appear as if CBP, ICE, and other agencies each independently identified the person as a threat. A single human or algorithmic error can metastasize across systems, creating a hall of mirrors that reverberates the unchecked error.

39. The hundreds of algorithms working to mine and categorize data could make an incorrect match, erroneously labeling someone a criminal or target.

---

[21] California State Auditor, *Due to an Inadequate Leadership Structure CalGang Has Failed to Comply With Requirements Designed to Protect Individuals' Rights to Privacy*, (2015), https://auditor.ca.gov/reports/2015-130/auditresults.html; U.S. Department of Homeland Security, *Privacy Impact Assessment for ICE Investigative Case Management,* 27 (June 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf

The public does not know if there is a mechanism for ensuring accuracy of matches or categorization made by the Palantir systems' algorithms.

40. Because ICE may surveil individuals who are not targets of investigations, there is a risk that ICE may use the Palantir systems to target individuals who are citizens or lawfully present, causing them to suffer erroneous enforcement consequences. Among other concerns, this may cause immigration officials to wrongfully detain individuals or wrongfully deny entry to individuals at Ports of Entry, where CBP uses information from ICE's Palantir systems in screening.[22] The public does not know what data patterns might trigger the creation a Subject Record, including whether those data triggers reflect facsimiles of racial identifiers, creating systemic discrimination in how targets are chosen for investigation. These systems can also exacerbate existing racial discrimination in an agency that is allowed to profile people based on race and national origin.[23]

41. The public has no information about what safeguards ensure that an algorithm-generated match is accurate, or that the data the Palantir systems rely on is accurate.

---

[22] *Id*. at 22.

[23] Dara Lind, *Feds*: *Racial profiling is bad…except at airports and the border*, VOX (Dec. 8, 2014) http://vox.com/2014/12/8/7351285/racial-profiling?_c=1

42. FOIA protects the public's right to be informed about how ICE ensures accuracy in these systems, which have such broad and far-reaching consequences.

D. The Public Has a Vital Interest in Understanding How ICE is Spending Millions of Taxpayer Dollars.

43. These systems come at an enormous fiscal cost to the United States. ICE has signed at least two contracts with Palantir, totaling at least $90 million since 2014.[24] FOIA protects the public's right to be informed about how the government spends taxpayer dollars.

44. ICE's failure to provide the requested agency records violates FOIA and deprives the public of understanding how this powerful tool is used, what privacy and civil rights are implicated, how the systems are shaping immigration policy and practices, how ICE safeguards against errors in its application, and the content of ICE's multimillion dollar contracts with Palantir.

PLAINTIFF'S FOIA REQUEST

---

[24] Ali Breland, *ICE Accidentally Just Revealed How Much its New Contract with Peter Thiel's Palantir is Worth*, Mother Jones (Aug. 20, 2019), https://www.motherjones.com/politics/2019/08/ice-palantir-contract-amount-revealed/

45. By email and certified postal mail to ICE's FOIA Officer Catrina Pavlik-Keenan on October 4, 2019, Plaintiffs submitted a FOIA request regarding ICE's contracts with Palantir to build and/or maintain information systems that include vast amounts of information on individuals. A copy of this request is attached as Exhibit A, and the request is hereby incorporated by reference.

46. Plaintiff requested expedited processing of their request pursuant to 5 U.S.C. § 552(a)(6)(E) and 6 C.F.R. § 5.5(e)(1)(ii).

47. Plaintiffs also requested a fee waiver or limitation for their request pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II) and 5 U.S.C. § 552(a)(4)(A)(iii).

48. On October 4, 2019, Plaintiffs submitted their request via email to ice-foia@dhs.gov. On information and belief, ICE received the request on the same day.

49. ICE acknowledged receipt of Plaintiffs' request on November 4, 2019. Instead of providing a statutorily appropriate response, however, ICE claimed Plaintiffs' FOIA request was "too broad in scope, did not specifically identify the records which [Plaintiffs] are seeking, or only posed questions to the agency." A copy of this response is attached as Exhibit B, and is hereby incorporated by reference.

50. Contrary to ICE's assertion, Plaintiffs have sufficiently identified the records requested, including by specifying relevant contract number(s) and document type(s).

51. Plaintiff's FOIA seeks communications between Palantir and ICE that contain the terms "ICM," "Integrated Case Management," "Falcon," or "PCloud." [Doc (1) p. 3 Ex. A] Plaintiffs also requested any Memoranda of Understanding between ICE and Palantir, as well as sources of data for GPS tracking utilized by the Falcon system. [Doc (4) p. 4 Ex. A] Plaintiffs requested specific training materials and instruction documents related to training ICE employees to use the ICM and FALCON systems. [Docs (7, 8, 19, 20, 25, 29, 36, 39, 51) p. 4, 5, 6, 7 Ex. A] Lastly, Plaintiffs specifically requested contracts by their respective contract number. [Docs (5-6, 9-15, 21-24, 46-52) p. 4-7 Ex. A]

52. On November 21, 2019, Plaintiffs responded to ICE, affirming their continued interest in pursuing their FOIA request and asking ICE to provide further explanation as to how the request was "too broad." A copy of Plaintiffs' correspondence is attached as Exhibit C, and hereby incorporated by reference. ICE never responded to this request for clarification.[25]

---

[25] In its November 4, 2019 response, ICE failed to articulate a clear determination or inform Plaintiffs of their right to seek assistance from the FOIA Public Liaison

53. On March 30, 2020, Plaintiffs appealed ICE's decision via email to foia@hq.dhs.gov. Plaintiffs submitted the appeal by email, based on the understanding that most DHS nonessential offices had closed and were not actively receiving physical mail due to COVID-19. A copy of Plaintiffs' appeal is attached as Exhibit D, and hereby incorporated by reference. On April 7, 2020, the Government Information Law Division sent confirmation of its receipt of the appeal by email, attached as Exhibit E.

54. On May 4, 2020, Plaintiffs received notice that the administrative appeal was granted and the request remanded to the agency, because new searches could be made. A copy of this decision is attached as Exhibit F, and hereby incorporated by reference.

55. On June 4, 2020, Plaintiffs followed up by emailing ICE and inquiring whether records would be released. This correspondence is attached as Exhibit G,

---

of the agency or appeal to the head of the agency and seek dispute resolution services from the FOIA Public Liaison of the agency. (5 U.S.C. § 552(a)(6)(A)(i).) Because of this, Plaintiffs were not required to administratively appeal that "determination" before bringing suit. *See CREW v. FEC*, 711 F.3d 180, 182 (D.C. Cir. 2013); *see also Khine v. DHS*, 943 F.3d 959, 964 (D.C. Cir. 2019); *see also* 5 U.S.C. § 552(a)(6)(B)–(C).)

and hereby incorporated by reference. To date, the agency has not contacted Plaintiffs regarding either the remand or the status of the FOIA.

56. To date, ICE has not responded to Plaintiffs as required by statute. 5 U.S.C. § 552(a)(6)(A)(i).

CLAIMS FOR RELIEF

57. Plaintiffs repeat, re-allege, and incorporate the allegations in the foregoing paragraphs as though fully set forth herein.

58. ICE is an agency and a component thereof subject to FOIA, 5 U.S.C. § 552(f), and must therefore release in response to a FOIA request any disclosable records in its possession at the time of the request and provide a lawful reason for withholding any materials as to which it claims an exemption, under 5 U.S.C. § 552(a)(3) and ICE's corresponding regulations, *see* 6 C.F.R. § 5.4.

59. ICE's failure to make a reasonable effort to search for records sought by the Request violates FOIA, 5 U.S.C. § 552(a)(3), and ICE's corresponding regulations, *see* 6 C.F.R. § 5.4.

60. ICE's failure to promptly make available the records sought by the Request violates FOIA, 5 U.S.C. § 552(a)(6)(A), and ICE's corresponding regulations, *see* 6 C.F.R. § 5.6.

61. ICE's failure to process Plaintiffs' Request as soon as practicable violates FOIA, 5 U.S.C. § 552(a)(6)(E), and ICE's corresponding regulations, *see* 6 C.F.R. § 5.5(d).

62. ICE's failure to grant Plaintiffs' request for a waiver of search, review, and duplication fees violates FOIA, 5 U.S.C. § 552(a)(4), and ICE's corresponding regulations, *see* 6 C.F.R. § 5.11(k). Further, ICE's failure to grant Plaintiff's request for a limitation of fees violates FOIA, 5 U.S.C. § 552(a)(4)(6), and ICE's corresponding regulations *see* 6 C.F.R. § 5.11(d).

REQUESTED RELIEF

WHEREFORE, Plaintiffs pray that this Court:

A. Declare that the ICE's failure to make a reasonable effort to search for records sought by the Plaintiff's Request; to promptly make available the records sought by the Plaintiff's Request; to process Plaintiffs' Request as soon as practicable; and to grant Plaintiffs' request for a waiver of search, review, and duplication fees is unlawful;

B. Issue an injunction ordering ICE to immediately process and release all records responsive to the Request;

C. Enjoin ICE from charging Plaintiffs search, review, or duplication fees for the processing of the Request;

D. Award Plaintiffs their costs and reasonable attorneys' fees incurred in this action; and

E. Grant such other relief as the Court may deem just and proper.

Dated this sixth of July, 2020.

/s/ Caitlin Bellis

Caitlin Bellis, Esq.
Annie Lai, Esq.
Attorneys for Plaintiffs

Paromita Shah, Esq.
Just Futures Law
95 Washington St., Suite 104-149
Canton, MA 02021
paromita@justfutureslaw.org
Of Counsel