IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ASYLUM SEEKERS TRYING
TO ASSURE THEIR SAFETY (made up of 21 Plaintiffs using pseudonyms ROE# 1-21)[1]
C/O Morrison Urena, L.C.
8910 University Lane
Suite 400
Santa Diego, CA 92122

Plaintiffs,

v.

TAE D. JOHNSON, in his official capacity as Acting Director of U.S. Immigration and Customs Enforcement,
500 Twelfth Street SW
Washington, DC 20536,

ALEJANDRO MAYORKAS, *in his official capacity as Secretary of Homeland Security*
c/o Office of the General Counsel
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave, SE
Washington, DC 20528-0485,

MERRICK GARLAND, *in his official capacity as Attorney General of the United States*
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20528-0485,

JOHN DOE 1, in their official capacity as employee of U.S. Immigration and Customs Enforcement,

Defendants.

Civil Action No.: 23-cv-163

CLASS ACTION COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

(Exposing private data of 6,252 vulnerable ICE detainees)

[1] Unopposed Motion for Leave to Proceed under Pseudonyms Filed Concurrently with Complaint.

TABLE OF CONTENTS

Plaintiffs ROE #1, ROE #2, ROE #3, ROE #4, ROE #5, ROE #6, ROE #7, ROE #8, ROE #9, ROE #10, ROE #11, ROE #12, ROE #13, ROE #14, ROE #15, ROE #16, ROE #17, ROE #18, ROE #19, ROE #20, and ROE #21, (collectively "ASYLUM SEEKERS TRYING TO ASSURE THEIR SAFETY" or "Plaintiffs"), by and through the undersigned counsel, respectfully bring this action on behalf of themselves and others similarly situated against Acting Director of U.S. Immigration and Customs Enforcement Tae D. Johnson, Secretary of Homeland Security Alejandro Mayorkas, Attorney General of the United States Merrick Garland, and one unknown JOHN DOE 1 Defendant (collectively, "Defendants"), and allege as follows:

INTRODUCTION

1. Plaintiffs are natives of Colombia, Ecuador, El Salvador, France, Guatemala, Honduras, Jamaica, Mexico, and Nicaragua. Some are currently detained by Defendant ICE at the Aurora Detention Center in Aurora, Colorado; Central Arizona Correctional Florence Detention Center in Florence, Arizona; the El Paso Service Processing Center, in El Paso, Texas; the Eloy Detention Center in Eloy, Arizona; and the Stewart Detention Center in Lumpkin, Georgia. Some Plaintiffs, including ROE #2 and ROE #13, have been released from custody for now.
2. Plaintiffs, and other similarly situated noncitizens (6,252 total), came to the United States to seek asylum and were detained in ICE custody. Many were fleeing torture or persecution in their countries of origin.
3. Some Plaintiffs, and others similarly situated, have already had their asylum claims adjudicated. Some submitted their asylum applications, and their claims are pending adjudications, and some have not yet submitted their asylum applications.

4. Defendants, in violation of the law, published the private data of Plaintiffs and other noncitizens in, or formerly in, ICE custody to their public-facing website. The uploaded data included their names, countries of origin, dates of birth, A-numbers, and locations of detention in the United States. The disclosure identified all individuals as asylum seekers who had initially been in expedited removal proceedings.
5. One currently unknown Defendant JOHN DOE 1 uploaded the data.
6. Defendants' action put Plaintiffs, and other noncitizens in, or formerly in, ICE custody in danger, both today and in the future. Many of them came to the United States to flee gang violence, government retaliation, and persecution on the basis of protected grounds.
7. ICE's unlawful disclosure of asylum seekers' confidential information has the concerning impact of deterring individuals from seeking protection in the United States in the future. Related, that deterrence undermines the United States' capacity to provide protection for asylum seekers, despite being a signer of the Universal Declaration of Human Rights. Article 14 of that declaration proclaims "everyone has the right to seek and enjoy in other countries asylum from persecution".
8. Further, given the crucial role that DHS plays in this nation's security, it is concerning this data breach could have been permitted to occur under any circumstances at all.
9. Plaintiffs now turn to this Court seeking an order to compel the Defendants and those acting under them to immediately and forthwith remedy the harm they have caused, by taking all appropriate action to: (1) extend accommodations to Plaintiffs and others similarly situated so that their asylum and withholding claims can be considered or reconsidered in light of the data breach, with the presumption of risk created by the data breach being presumed; (2) award a monetary award of $10,000 to each Plaintiff and others similarly situated pursuant to the

Privacy Act of 1974; and (3) award compensatory and punitive damages of $5,000 to each Plaintiff and others similarly situated from Defendants pursuant to the other counts brought.

JURISDICTION AND VENUE

10. This case arises under the Fifth Amendment to the United States Constitution; and 5 U.S.C. Sec. 552a(b). This Court has jurisdiction pursuant to 28 U.S.C. § 1331. This Court also has authority to grant declaratory relief under 28 U.S.C. § 2201 and 2202, and injunctive relief under 5 U.S.C. § 702, and the inherent equitable powers of this Court. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1346 because the United States is a defendant.
11. There exists an actual and justiciable controversy between Plaintiffs and Defendants requiring resolution by this Court. Plaintiffs have no adequate remedy at law.
12. The court has further remedial authority under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, and the Administrative Procedure Act, 5 U.S.C. § 500 *et seq.*
13. Pursuant to 28 U.S.C. § 1391(e), venue is proper within this district on the following grounds: (A) the Defendant in the action reside in the district, or (B) a substantial part of the events or omissions giving rise to the claim may have occurred in this district. It was ICE's Management and Administration, Professional Responsibility in Washington, D.C., that issued the November 30, 2022 "Statement on improper disclosure of noncitizen personally identifiable information." Defendants have failed at the headquarters level to protect the privacy of all detainees in ICE custody.
14. Further, venue is proper within this district as the District Court for the District of Columbia has exclusive jurisdiction over claims arising under the Judicial Redress Act.

PARTIES

Plaintiffs

15. Plaintiff ROE #1 is a native of Jamaica, currently detained at Stewart Detention Center, in Lumpkin, Georgia.
16. Plaintiff ROE #2 is a native of Nicaragua and was formerly detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona. Plaintiff ROE #2 has been released from custody.
17. Plaintiff ROE #3 is a native of France, currently detained at Stewart Detention Center, in Lumpkin, Georgia.
18. Plaintiff ROE #4 is a native of Mexico, currently detained at Denver Contract Detention Facility (Aurora), in Aurora, Colorado.
19. Plaintiff ROE #5 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
20. Plaintiff ROE #6 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
21. Plaintiff ROE #7 is a native of Honduras, currently detained at El Paso Service Processing Center, in El Paso, Texas.
22. Plaintiff ROE #8 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
23. Plaintiff ROE #9 is a native of Guatemala, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
24. Plaintiff ROE #10 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.

25. Plaintiff ROE #11 is a native of Mexico, formerly detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona. ROE #11 has been transferred to Nevada Southern Detention Center in Pahrump, Nevada.
26. Plaintiff ROE #12 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
27. Plaintiff ROE #13 is a native of Colombia, formerly detained at Eloy Detention Center in Eloy, Arizona. ROE #13 has been released from custody.
28. Plaintiff ROE #14 is a native of El Salvador, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
29. Plaintiff ROE #15 is a native of Nicaragua, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
30. Plaintiff ROE #16 is a native of Colombia, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
31. Plaintiff ROE #17 is a native of Nicaragua, formerly detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona. ROE #17 has been transferred to Nevada Southern Detention Center in Pahrump, Nevada.
32. Plaintiff ROE #18 is a native of Mexico, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
33. Plaintiff ROE #19 is a native of Ecuador, currently detained at Denver Contract Detention Facility (Aurora), in Aurora, Colorado.
34. Plaintiff ROE #20 is a native of Nicaragua, currently detained at Central Arizona Correctional Florence Detention Center in Florence, Arizona.
35. Plaintiff ROE #21 is a native of Colombia, currently detained at Central Arizona Correctional

Florence Detention Center in Florence, Arizona.

Defendants

36. Defendant Tae D. JOHNSON ("JOHNSON") is the Acting Director of ICE. JOHNSON is responsible for ICE's policies, practices, and procedures, including those relating to the detention and detention conditions of immigrants. JOHNSON is the legal custodian of Plaintiffs. ICE is a federal law enforcement agency within the DHS. ICE is responsible for the criminal and civil enforcement of immigration laws, including the detention and removal of immigrants. ICE has custody over all Plaintiffs, regardless of the facility in which they are held. One component of ICE is the Office of Information Governance and Privacy ("OIGP"). OIGP's mission is, in part, "to ensure that individual privacy is protected." He is sued in his official capacity.

37. Defendant Alejandro MAYORKAS ("MAYORKAS") is the Secretary of the Department of Homeland Security, a cabinet-level department of the U.S. government responsible for implementing and enforcing the Immigration and Nationality Act ("INA"). As the Secretary of the DHS, he is responsible for the general administration and enforcement of the immigration laws of the United States. More specifically, the Secretary of DHS has authority under 5 U.S.C. 301, 552, and 552a, and 6 U.S.C. 112(e) to issue Privacy Act regulations. That authority has been delegated to the Chief Privacy Officer of the Department pursuant to 6 U.S.C. 142 and DHS Del. No. 13001, Rev. 01 (June 2, 2020). DHS is a cabinet-level department of the U.S. government responsible, in part, for implementing and enforcing the INA. One guiding principle of DHS is "to implement safeguards for privacy, transparency, civil rights, and civil liberties when developing and adopting policies and throughout the

performance of its mission to ensure that homeland security programs uphold privacy, civil rights, and civil liberties." MAYORKAS is sued in his official capacity.

38. Defendant Merrick GARLAND ("GARLAND") is the Attorney General of the United States. Pursuant, *inter alia*, to 8 U.S.C. § 1103, he is charged with controlling the determination of all issues of law pertaining to immigration and with representing the United States of America in various legal matters. DOJ is an executive department of the United States charged with enforcing federal law. The Executive Office for Immigration Review ("EOIR") is a federal office/agency within and overseen by DOJ and is responsible for adjudicating immigration cases. GARLAND is sued in his official capacity.

39. Defendant JOHN DOE 1 published the private data to the ICE website. Their identity is not publicly disclosed by Defendants, even though Defendant JOHNSON proclaimed, in the December 30, 2022 ICE Annual Report for FY-2022, "[t]ransparency remains at the forefront of our mission." JOHN DOE 1 is sued in their official capacity as an employee of ICE.

FACTUAL ALLEGATIONS

40. On Monday November 28, 2022, at 9:45 A.M. EST, Defendant JOHN DOE 1 posted the names and other personally identifiable information, along with immigration information, of 6,252 noncitizens in, or formerly in, ICE custody, including Plaintiffs in this action to ICE.gov. The file was published to a page where ICE regularly publishes detention statistics.

41. Approximately 1,000 affected noncitizens were either removed or released from ICE custody prior to the date of the disclosure.

42. At least 170 affected noncitizens were removed from the United States between November 18 and November 30. While ICE claims a large majority of those who were not in custody

are receiving the notification via mail, there is no explanation as to whether this applies to noncitizens deported, and if it does, how the mail itself would put affected noncitizens in danger.

43. During the breach, the information was able to be downloaded, copied, captured by screenshot, and otherwise preserved by the public.

44. The data remained posted, viewable, and downloadable for approximately five hours, until the immigrant advocacy group Human Rights First, flagged the data breach to ICE just before 2:00 PM EST.

45. On November 30, 2022, ICE posted a statement on the same newsroom section of the same website conceding that the release of information was "a breach of policy," and that "the agency [was] investigating the incident and taking all corrective actions necessary," and that "ICE [was] notifying noncitizens impacted by the disclosure."[2]

46. In the statement, ICE promised to take "all corrective actions necessary" to remedy the breach.[3] ICE also announced an investigation but has not provided any additional details about the investigation, including which office will conduct the investigation, its estimated length, or its objectives. Further, ICE has not disclosed any corrective measures that have been taken to ensure a data breach of this nature will be repeated. Further, ICE has not disclosed the identity of the individual who uploaded the data, or whether that individual will be held responsible.

47. Beginning in December 2022, ICE officers began giving notices to Plaintiffs informing them

---

[2] *See Statement on Improper Disclosure of Noncitizen Personally Identifiable Information*, U.S. Dep't of Homeland Security, U.S. Immigration and Customs Enforcement, https://www.ice.gov/news/releases/statement-improper-disclosure-noncitizen-personally-identifiable-information (Nov. 30, 2022).

[3] *Id.*

of the breach. For those subject to removal, their notices indicate that they will not be removed for 30 days.

48. For Plaintiffs and others similarly situated who are subject to a final order of removal, ICE provided an "opt-out' form, which reads "you may ask that ICE proceed with arranging your removal by signing the form below." However, ICE officers have repeatedly attempted to get some Plaintiffs to sign a waiver of the 30 days, even after they refused.

49. Additionally, ICE did not initially share the notice or form with immigration advocates or attorneys, hampering the abilities of service providers to counter the confusion at many detention centers. While ICE is alerting attorneys of record for those impacted by the breach who have counsel, notice is by mail and is inevitably a slow process. Meanwhile, legal proceedings for those without removal orders continue to march forward.

50. On December 7, 2022, ICE gave notices to some affected Cuban detainees that ICE had informed Cuban government officials, in a phone call, that some of them were in a group of 103 individuals awaiting removal to Cuba. While only 46 of those individuals were named in the leak, the DHS's second breach of confidential information in less than one month placed all 103 Cuban individuals in peril if they are returned to Cuba. Thus, ICE released some or all of the affected 103 individuals awaiting removal to Cuba.

51. On December 15, 2022, twelve members of Congress joined Congresswoman Norma J. Torres in a letter to Defendant JOHNSON expressing concern and outrage about the data breach. The letter asks nine questions about how it happened, and what will be done about how the data breach occurred, how victims were notified, and whether the victims' information was downloaded to the countries they fled. The letter also asks ICE to state its data security policies, provide the findings of its internal investigation to Congress and the

public, and confirm what corrective measures will be taken to avoid future breaches and ensure accountability.[4]

52. Further, the letter notes that Congress provided "increased resources to ICE through the Fiscal Year 2022 funding bill (Public Law 117-103)" and asks how Congress can "best work with ICE to protect the data of asylum-seekers."

53. Despite the unanswered questions, immigration judges with EOIR, a federal agency within and overseen by DOJ, have already issued denials of asylum claims where the risks related to the data breach are downplayed and dismissed. For example, this is what one immigration judge did with the asylum decision for Plaintiff ROE #4 on December 19, 2022 in Aurora, Colorado.

54. On January 18, 2023, ICE discretely updated the ICE.gov website with a representation that "Now that ICE is implementing options to help remedy the inadvertent disclosure, we are extending the 30-day pause on removals for the impacted noncitizens to allow them time to further discuss their options with a legal representative." However, the length of the extension was not disclosed.

55. Despite ICE's claim that it placed alerts in record management systems on all noncitizens whose private information was inadvertently made public, some impacted noncitizens were deported after the data breach without being given notice of the data breach.

56. Since the data breach, ICE has released approximately 2,900 impacted noncitizens from its custody.

57. With the leaked information, Plaintiffs' persecutors could now better pursue them inside

[4] December 15, 2022 Letter from Rep. Torres and other members of Congress to JOHNSON, https://torres.house.gov/sites/torres.house.gov/files/221215%20ICE%20Letter%20re_%20Release%20of%20Asylum%20Seeker%20Information%20FINAL.pdf.

and outside the United States.

58. ICE has plans to serve Notices to Appear (NTA) to all individuals impacted by the disclosure have been served so they may apply for or add to an application for relief or protection based in-part or entirely on the disclosure. However, there is no commitment from Defendants to presume any danger associated with the data breach.

59. Pursuant to the APA, 5 U.S.C. §§706(2)(A), 706(2)(D), a reviewing court may also "hold unlawful and set aside agency action, findings, and conclusions found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" and "without observance of procedure required by law."

60. Defendants' actions violate the Due Process Clause of the U.S. Constitution, the Privacy Act of 1974, the APA, and its implementing regulations, and agency policy.

61. As noted above, Defendants' actions have caused Plaintiffs harm.

LEGAL FRAMEWORK OF THE PRIVACY ACT

62. The Privacy Act of 1974 provides civil remedies. Specifically, "[w]henever any agency…fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection." 5 U.S. Code § 552a(g)(1)(D).

63. Defendant DHS promulgated regulations that provide that "Records are protected from public view" and "the area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them." 6 C.F.R. § 5.31(a)(1) and (2). Further, the

regulations state that "[r]ecords are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form." 6 C.F.R. § 5.31(a)(4).

64. The Privacy Act of 1974 defines an individual as "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S. Code § 552a(a)(2). However, modernly, Defendants have themselves argued that the Privacy Act extends even to citizens of Iran who are not lawfully admitted for permanent residence.

65. Further, the Judicial Redress Act of 2015 extends the right to pursue certain civil remedies under the Privacy Act to citizens of designated foreign countries. Immediately before signing President the Judicial Redress Act Bill in a televised ceremony on February 24, 2016, President Barack Obama said "what it does in the simplest terms is makes sure everybody's data is protected in the strongest possible way with our privacy laws. Not only American citizens, but also foreign citizens."[5]

66. On January 17, 2017, the Attorney General designated DHS and the DOJ as federal agencies subject to the Judicial Redress Act. 82 Fed. Reg. 7860 (Jan. 23, 2017).

67. On February 1, 2017, twenty-six countries (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden) were designated each as covered countries under the act. 82 FR 7860. The UK was designated on April 1, 2018. 84 FR 3493. While one Plaintiff, ROE #3 is a citizen of France, it is unclear how many of the other 6,251 asylum seekers whose data was released were also nationals of these twenty-seven covered countries.

[5] *See* Judicial Redress Act Bill Signing Ceremony, https://www.c-span.org/video/?c5048714/user-clip-obama-extending-privacy-protections-foreign-citizens&editTime=1672517522 (last visited Dec. 31, 2022).

68. On January 26, 2017, President Donald Trump issued Executive Order 13768 that "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[6]

69. In a April 25, 2017 DHS "Privacy Policy Guidance Memorandum," aimed at implementing President Trump's order. However, even that memorandum listed regulations, including 8 C.F.R. § 236.6 (DHS regulations protect information regarding pre and post order detainees), to conclude "these regulations are an indicia of regulatory restrictions on disclosure applicable to all persons regardless of immigration status. These authorities are not changed by E.O. 13,768."[7]

70. In a December 4, 2017 DHS Instruction Guide entitled "Privacy Incident Handling Guide," DHS explains the agency:

> "has an obligation to safeguard [personally identifiable information] and implement procedures for handling both privacy and computer security incidents. This obligation is defined in numerous federal statutes, regulations, and directives, including:
>
> Federal Statutes:
>
> Title 5, United States Code (U.S.C.) Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]
> Title 6, U.S.C., Section 142, "Privacy Officer"
> Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security" [The Federal Information Security Modernization Act of 2014, as amended (FISMA)]
>
> OMB/Government-wide Regulations and Guidelines:
>
> Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources (updated July 28, 2016)

[6] DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 25, 2017), https://www.federalregister.gov/d/2017-02102.

[7] https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
OMB Memorandum 18-02, Fiscal Year 2016 - 2017 Guidance On Federal Information Security And Privacy Management Requirements (October 16, 2017)
OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)

DHS Policy:

DHS Delegation 13001, "Delegation to the Chief Privacy Officer" DHS Delegation 04000, "Delegation for Information Technology"
DHS Directive 047-01, "Privacy Policy and Compliance"
DHS Instruction 047-01-005, "Component Privacy Officer"
DHS Instruction 047-01-006, " Privacy Incident Response and Breach Response Team"
DHS Privacy Policy Directive 140-10, "Handbook for Safeguarding Sensitive Personally Identifiable Information"
DHS 4300A, "Sensitive Systems Policy," DHS 4300A Sensitive Systems Policy Handbook, Attachment F, "Incident Response"
DHS 4300 B, "National Security Systems (NSS) Policy"
DHS Management Directive 026-04, Protection of Human Subjects
DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information
DHS Management Directive 11056.1, Sensitive Security Information."[8]

71. On September 20, 2020, Christopher C. Krebs, Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, issued a compulsory operational directive requiring all federal executive branch departments and agencies to develop and publish a vulnerability disclosure policy, which would make it easy for the public to report a data breach on a government website.[9] Defendant JOHNSON did not publish a vulnerability disclosure policy on ICE.gov. If posted, the policy would have made it easier for the public to report the data breach to ICE employees who could have removed it soon.

[8] Privacy Incident Handling Guidance DHS Instruction Guide 047-01-008, https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf.
[9] Binding Operational Directive 20-01, U.S. Department of Homeland Security, https://www.cisa.gov/sites/default/files/bod-20-01.pdf.

72. On January 20, 2021, President Joseph Biden issued Executive Order 13993, rescinding Executive Order 13768. President Biden also ordered that, "[t]he Secretary of State, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Director of the Office of Personnel Management, and the heads of any other relevant executive departments and agencies (agencies) shall review any agency actions developed pursuant to Executive Order 13768 and take action, including issuing revised guidance, as appropriate and consistent with applicable law, that advances the policy set forth in section 1 of this order." Section 1 included the following policy statement:

> The policy of my Administration is to protect national and border security, address the humanitarian challenges at the southern border, and ensure public health and safety. We must also adhere to due process of law as we safeguard the dignity and well-being of all families and communities. My Administration will reset the policies and practices for enforcing civil immigration laws to align enforcement with these values and priorities.[10]

CLASS ALLEGATIONS

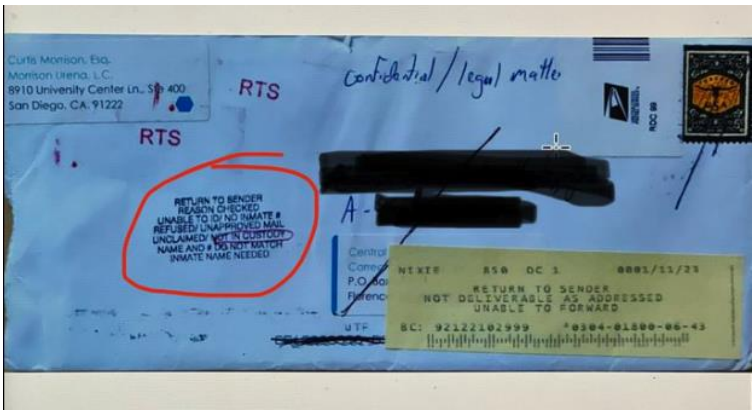
73. Plaintiffs bring claims for injunctive relief on behalf of themselves and all similarly situated persons pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(3).

74. Plaintiffs bring this action on their own behalf and on behalf of the following class: All 6,252 noncitizens whose personal data was published on ICE.gov on November 28, 2022.

75. *Numerosity*. The size of the class, 6,252 class members, makes a class action both necessary and appropriate. Further, joinder is impracticable as putative class members are in the custody of Defendant ICE, where their access to legal counsel is limited. Further, many putative class members are not fluent in English. Further, ICE detainees cannot use email and can only

[10] https://www.federalregister.gov/d/2021-01768.

make Skype calls when scheduled in advance with the facilities. Some putative class members have no friends or family to help them with legal matters while they are detained. Further, ICE makes it difficult for an attorney to even retain clients they have detained. In the undersigned counsel's process of retaining clients to be plaintiffs in this case, ICE relocated detainees attempting to enter a contract for representation over the data breach matter. Defendant ICE transferred ROE #11, and other affected detainees attempting to participate in this case, from Central Arizona Florence Correctional Center to Nevada Southern Detention Center. In one instance, the Central Arizona Florence Correctional Center opened mail addressed to a detainee who was trying to participate in this case, then taped it shut, and dropped it back in the mail marked "RTS" and circling "No longer detained," when the prospective client is still detained. (Defendants transferred that detainee from Central Arizona Florence Correctional Center to Nevada Southern Detention Center about the same time.)



76. *Typicality*. The claims of the Plaintiffs are typical of the claims of the class as a whole. Each of the Plaintiffs was subjected to a betrayal of trust and violations of law by Defendants. As a result of the data breach, each of the Plaintiffs faces varying increased risk of harm should they be deported.

77. *Common Questions of Law and Fact*. This case poses common questions of law and fact

affecting the rights of all members of the class, including but not limited to:

a. Whether Defendant JOHN DOE 1 uploaded the private information of class members?

b. Whether the actions of Defendant JOHN DOE 1 were intentional or willful?

c. How Defendant JOHN DOE 1 was able to upload the private information of class members without any intervention from other superiors, including other Defendants?

d. Whether anyone at ICE raised concerns about the uploaded private information prior to ICE being notified by Human Rights First?

e. How long it took for ICE take to remove the private information from its website after it was notified by Human Rights First?

f. What has ICE done to aid those at risk of retaliation due to this data breach in each of the sub-categories (currently in custody, formerly in custody, and already removed)?

g. What ICE division, if any, is investigating the data breach, and what are the results of its investigation?

h. What caused ICE to release a statement determining the data breach was "unintentional" before the conclusion its investigation?

i. How many times was the private information was downloaded?

j. Were any downloads in countries that these individuals are claiming asylum from, or were any of the downloads from VPNs where the downloader's location could not be certain?

k. What has ICE done to ensure those who downloaded the information deleted it?

l. How many of the affected victims have been notified by ICE, and how many have not been notified by ICE?

m. How many of the class members have had their asylum claims adjudicated without consideration or a presumption of, enhanced risk of danger because of the data breach?

n. How many of the class members have been deported?

o. For those class members whom Defendants have deported, have Defendants collected contact information so that they can update them about foreseeable obligations compelled by this or any other court?

p. Whether class members are entitled to damages under the Privacy Act, or any other provision of law?

q. Did any of the released data include constitutionally protected data of minors?

78. *Adequacy of Class Representation*. Plaintiffs can adequately and fairly represent the interests of the class as defined above, because their individual interests are consistent with, and not antagonistic to, the interests of the class.

79. *Adequacy of Counsel for the Class.* Counsel for Plaintiffs possess the requisite resources and ability to prosecute this case as a class action and are experienced immigration litigation attorneys who have successfully litigated other multiparticipant cases against government Defendants in this District.

80. *Propriety of Class Action Mechanism.* Class certification is appropriate because the questions of law or fact common to class members predominate over any questions affecting only individual members, and a class action is superior to other available methods for fairly and efficiently adjudicating the controversy. The lives of class members are already upended, and thus, they have limited capacity to individually initiate or control the prosecution of separate actions. Further, there is no other litigation concerning ICE's November 28, 2022 data breach. Further, this litigation should take place in this forum as Privacy Act causes of action must be brought in this district. Finally, the Court should not expect difficulties in managing a class action, as Defendants know the identities of all class members, and hold most in custody. Also, Defendants know they have made a mistake, and have presumably already given notice to most or all class members that they should consider consulting with an attorney.

FIRST CLAIM FOR RELIEF
Privacy Act of 1974, 5 U.S.C. Sec. 552a(a)-(l)
(Against all Defendants)

81. The above paragraphs are incorporated herein by reference.

82. "[N]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request, or with...written consent of, the individual to whom the record pertains." 5 U.S.C. Sec. 552a(b).

83. "The purpose of the Privacy Act (5 U.S.C. Sec. 552a) is to protect privacy of individuals identified in computerized information systems maintained by federal agencies by preventing misuse of information." *Thomas v. United States Dep't of Energy*, 719 F.2d 342, 1983 U.S. App. LEXIS 15986 (10th Cir. 1983).

84. "Agencies subject to Privacy Act must establish appropriate administrative, technical, and physical safeguards to ensure security and confidentiality of private information under their charge under 5 USCS § 552a(e)(10)." *Alexander v. FBI*, 691 F. Supp. 2d 182, 2010 U.S. Dist. LEXIS 21386 (D.D.C. 2010).

85. Of note, ROE #3, is a native of France, a covered country under the Judicial Redress Act, and thus explicitly and unquestionably entitled to protections under the Privacy Act by law.

86. On information and belief, DHS and ICE specifically, did not establish appropriate administrative, technical, and physical safeguards to prevent the data breach.

87. Actual damages faced by Plaintiffs are a result of Defendants providing Plaintiffs' persecutors with information that makes it easier for Plaintiffs to be located today or in the future, Defendants have cursed Plaintiffs to a lifetime of added security needs that will be

expensive to meet. Plaintiffs and those similarly affected face persecution and/or death if they are forced to return to their home countries where, as a result of the data breach, the foreign governments may know or learn that they sought asylum in the U.S.

88. For example, whether removed from the U.S. or not, Plaintiffs at risk of retaliation may need to adopt a nomadic lifestyle making it more difficult to establish a normal life. Similarly, Plaintiffs may need to purchase security systems, change door and window locks, private mailboxes or obtain other protection to ensure their physical safety. Some Plaintiffs have spouses and children residing in the United States and fear their families may have increased risk of harm. Some Plaintiffs will incur costs related to legally changing their name.

89. Plaintiffs may also need counseling to process their experience. Traumatic events, such as a threat to one's safety or a situation where one fears for their life, can cause lasting changes in the brain.[11] The risk is heightened for those who experience repeated traumatic stress, such as asylum seekers. Plaintiffs may require professional support to feel safe in their own bodies, and professional psychological support often comes at a substantial financial cost.

90. Even the Defendants' own notice to Plaintiffs suggests they violated "obligations" that make it necessary for Plaintiffs to consider "actions you wish to take, including consulting with an attorney," yet Defendants have not offered to assume that expense, so most affected likely have not done so.

91. Further, these individuals fled to the U.S. because they believed the U.S. government would protect them from harm in their countries of origin. Their faith has been shattered, and their safety is still at risk. They will have to look over their shoulders for the rest of their lives.

[11] Bremner J. D. (2006). Traumatic stress: effects on the brain. *Dialogues in clinical neuroscience, 8*(4), 445–461, *available at* https://doi.org/10.31887/DCNS.2006.8.4/jbremner.

SECOND CLAIM FOR RELIEF
Administrative Procedure Act, 5 U.S.C. §§ 706(2)(A), 706(2)(D)
(Against all Defendants)

92. The above paragraphs are incorporated herein by reference.

93. Pursuant to the APA, 5 U.S.C. §§706(2)(A), 706(2)(D), a reviewing court may also "hold unlawful and set aside agency action, findings, and conclusions found to be arbitrary, capricious, and abuse of discretion, or otherwise not in accordance with law" and agency action taken "without observance of procedure required by law" "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," 5 U.S.C. 706(C); or "without observance of procedure required by law," 5 U.S.C. § 706(D). "Agency action" includes, in relevant part, "an agency rule, order, license, sanction, relief, or the equivalent thereof, or failure to act." 5 U.S.C. § 551(13).

94. Defendants' failure to safeguard Plaintiffs' personal information from public disclosure constitutes agency action taken not in accordance with the law.

95. Defendant JOHNSON's failure to post a vulnerability disclosure policy on ICE.gov constitutes agency action taken not in accordance with the law.

96. ICE's failure to sufficiently address the harm the agency caused, by offering merely a 30-day grace period on effectuation of existing removal orders, constitutes agency action taken not in accordance with the law.

97. DOJ's failure to account for the harms to Plaintiffs and proceed with removal processes despite those harms constitutes an abuse of discretion.

98. As a result of Defendants' actions, Plaintiffs have an enhanced risk of injury. No alternative

remedy exists to compel action by Defendants.

THIRD CLAIM FOR RELIEF

Defendants have failed to protect Plaintiffs According to Department Policy in a Violation of the *Accardi* Doctrine

(Against Defendant DHS)

99. The above paragraphs are incorporated herein by reference.

100. First recognized in *United States ex rel. Accardi v. Shaughnessy*, the doctrine dictates that administrative agencies are bound to follow their rules and guidelines. *See United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260, 74 S.Ct. 499, 98 L.Ed. 681 (1954). The Supreme Court bolstered the principle in *Morton v. Ruiz*, holding that "where the rights of individuals are affected, it is incumbent upon agencies to follow their own procedures." *Morton v. Ruiz*, 415 U.S. 199, 235, 39 L. Ed. 2d 270, 94 S. Ct. 1055 (1974). "This is so even where the internal procedures are possibly more rigorous than otherwise would be required." *Id*.

101. An *Accardi* claim can stand on its own as a freestanding claim, and "is at heart a claim of procedural fairness that owes as much to the Due Process Clause as to the Administrative Procedure Act." *Jefferson v. Harris*, 285 F. Supp. 3d 173, 185 (D.D.C. 2018).

102. "Agencies cannot relax or modify regulations that provide the only safeguard individuals have against unlimited agency discretion." *Lopez v. FAA*, 318 F.3d 242, 247 (D.C. Cir.

103. 2003).

104. Pursuant to the *Accardi* doctrine, Defendant DHS is bound to the confidentiality protections for individuals in asylum-related proceedings in 8 C.F.R. § 208.6. Per 8 C.F.R. § 208.6(b), "[t]he confidentiality of other records kept by DHS and the Executive Office for

Immigration Review that indicate that a specific alien has applied for refugee admission, asylum, withholding of removal under section 241(b)(3) of the Act, or protection under regulations issued pursuant to the Convention Against Torture's implementing legislation, or has received a credible fear or reasonable fear interview, or received a credible fear or reasonable fear review shall also be protected from disclosure…"

105. In the notices that ICE provided to Plaintiffs, ICE conceded that the incident violated its confidentiality obligations under 8 C.F.R. § 208.6(b).

106. In a June 2005 DHS interoffice memorandum, prepared by the USCIS Asylum Division called "Fact Sheet on Confidentiality," DHS explains "public disclosure [of information contained pertaining to asylum applications] might, albeit in rare circumstances, give rise to a plausible protection claim where one would not otherwise exist by bringing an otherwise ineligible claimant to the attention of the government authority or non-state actor against which the claimant has made allegations of mistreatment."[12] This is Defendants admitting that Plaintiffs will face and suffer harm if not given a meaningful opportunity to apply for asylum based on the repercussions of the ICE data breach.

107. In the interoffice memorandum, DHS also explains "confidentiality is breached when information contained in or pertaining to an asylum application is disclosed to a third party in violation of the regulations, and the unauthorized disclosure is of a nature that allows the third party to link the identity of the applicant to: (1) the fact that the applicant has applied for asylum; (2) specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or (3) facts or allegations that are sufficient to give rise

[12] USCIS Interoffice Memorandum re: Fact Sheet on Confidentiality (June 15, 2005), https://www.uscis.gov/sites/default/files/document/fact-sheets/fctsheetconf061505.pdf.

to a reasonable inference that the applicant has applied for asylum."[13]

108. In an October 18, 2012 DHS document called "Fact Sheet: Federal Regulation Protecting the Confidentiality of Asylum Applicants," Defendants conceded, "Public disclosure of asylum-related information may subject the claimant to retaliatory measures by government authorities or non-state actors in the event that the claimant is repatriated, or endanger the security of the claimant's family members who may still be residing in the country of origin. Moreover, public disclosure might, albeit in some limited circumstances, give rise to a plausible protection claim where one would not otherwise exist by bringing an otherwise ineligible claimant to the attention of the government authority or non-state actor against which the claimant has made allegations of mistreatment."

109. Further, in the December 4, 2017 DHS Instruction Guide noted above, Defendants admitted they have other privacy obligations as defined in numerous federal statutes, regulations, and directives. Defendants have other privacy obligations still, whose interpretations are outlined in subsequently issued DHS Instruction Guides.

110. Of note, Roe #3, is a native of France, a covered country under the Judicial Redress Act.

111. Contrary to these confidentiality protections, Defendants have subjected the Plaintiffs to imminent risks of retaliatory measures by government authorities or non-state actors if deported.

112. The premise underlying the *Accardi* doctrine is that agencies can be held accountable to their own codifications of procedures and policies – and particularly those that affect individual rights.

[13] *Id.*

FOURTH CLAIM FOR RELIEF
Violation of Equal Protection Principles Embedded in the Fifth Amendment pursuant to *DeShaney*
(Against all Defendants)

113. The above paragraphs are incorporated herein by reference.

114. Defendants have violated the equal protection principles of the Fourteenth Amendment, embedded in the Due Process Clause of the Fifth Amendment.

115. The purpose of the Due Process Clause is "to protect the people from the State, not to ensure that the State protected them from each other." *DeShaney v. Winnebago Cnty. Dep't of Soc. Servs.*, 489 U.S. 189, 196 (1989). However, "[i]t is true that in certain limited circumstances the Constitution imposes upon the State affirmative duties of care and protection with respect to particular individuals." *DeShaney*, 489 U.S. at 198. There are Due Process claims that are exceptions to *DeShaney*, applicable to Defendants under the Fifth Amendment. *DeShaney*, 489 U.S. at 196.

116. The D.C. Circuit has recognized two such circumstances. *Gormly v. Walker*, No. 21-cv-2688 (CRC), 2022 U.S. Dist. LEXIS 100080, at *15 (D.D.C. June 6, 2022) (*citing Pollard v. District of Columbia*, 191 F. Supp. 3d 58, 80 (D.D.C. 2016)). "First is the **custody exception**, which imposes a higher duty of care when the state holds an individual in some form of involuntary custody." *Id*., (citing *DeShaney*, 489 U.S. at 199-2). "Second is the **state-endangerment** exception, under which 'an individual can assert a substantive due process right to protection by the District of Columbia from third-party violence when District of Columbia officials affirmatively act to increase or create the danger that ultimately results in the individual's harm.'" *Id*. (citing *Butera v. District of Columbia*, 235 F.3d 637,

651 U.S. App. D.C. 265 (D.C. Cir. 2001)).

117. Although Defendants' actions need only fall under one *Deshaney* exception for recovery to be viable, here, they fall into both the custody exception and the state endangerment exception.

Custody Exception

118. Plaintiffs and all similarly situated were in ICE custody at the time of the data breach. The custody exception is met here.

119. "The affirmative duty to protect arises not from the State's knowledge of the individual's predicament or from its expressions of intent to help him, but from the limitation which it has imposed on his freedom to act on his own behalf." *DeShaney*, 489 U.S. at 200.

120. The conscience's susceptibility to shock varies radically with whether the government has previously taken an "affirmative act of restraining the individual's freedom to act on his own behalf—through incarceration, institutionalization, or similar restraint of personal liberty." *DeShaney* 489 at 200. Thus, a prisoner who has "already been deprived of [his] liberty," for example, has a plausible claim to affirmative governmental protection. *Collins v. City of Harker Heights*, 503 U.S. 115, 127, 112 S. Ct. 1061, 117 L. Ed. 2d 261 (1992).

121. "The state must protect those it throws into snake pits, but the state need not guarantee that volunteer snake charmers will not be bitten." *Walker v. Rowe*, 791 F.2d 507, 511 (7th Cir. 1986) (explaining that although a state has a constitutional duty to protect prisoners in its custody, it has no such obligation toward prison guards who have voluntarily accepted employment with the state). *AFGE v. OPM (In re United States OPM Data Sec.*

Breach Litig.), 442 U.S. App. D.C. 42, 74-75, 928 F.3d 42, 74-75 (2019). When the state has a heightened obligation toward an individual, "governmental 'deliberate indifference' will shock the conscience sufficiently" to establish a substantive due process violation. *Harvey v. District of Columbia*, 418 U.S. App. D.C. 321, 329, 798 F.3d 1042, 1050 (2015) (quoting *Smith*, 413 F.3d at 93)

122. By releasing the private information of asylum seekers on their public-facing website, Defendants have increased the risk that Plaintiffs' persecutors (1) know Plaintiffs seek refuge from the United States and (2) know more information about Plaintiffs, including their location, making it easier to carry out the persecutions. With the leaked information, Plaintiffs' persecutors could even better pursue them inside the United States. Defendants have thrown Plaintiffs "into the snake pits," and thus owe them a duty of protection. Thus far, the extent of protection offered has been merely to give them a mere 30-day reprieve from deportation and facing the consequences of Defendants' actions.

State Endangerment Exception

123. The state endangerment exception is met here. Defendants apprehended Plaintiffs and held them in custody. In so doing, Defendants collected Plaintiffs' information and stored it in its databases. By storing and centralizing the names, locations, and other personally identifiable information of asylum seekers, without either implementing or adhering to procedures that protect that data, Defendants placed Plaintiffs in a position of danger.

124. Plaintiffs are in danger of imminent harm. Due to Defendants' actions, an untold number of persecutors and bad actors have the information they need to track Plaintiffs down and kill them. Even if their persecutors missed the initial leak, the data was easily copied, downloaded, or otherwise preserved. Therefore, it can be distributed indefinitely and presents

a permanent risk to the safety of Plaintiffs and those similarly situated.

125. Defendants know that government databases and accounts are regularly subject to attempted cyberattacks and hacking. Defendants also know some attacks have been successful in the recent past.

126. For example, the Cybersecurity and Infrastructure Security Agency ("CISA"), a DHS agency, posted a series of reports related to the infamous 2020 "SolarWinds Compromise." The reports allege that nefarious foreign actors, later identified as the Russian Foreign Intelligence Service ("SVR"), used malware to covertly infiltrate government networks, targeting cloud resources and email databases to obtain information across multiple federal agencies. [14]

127. Defendant DHS authored and co-authored several of these reports, which demonstrates DHS' detailed knowledge of the threats to federal government databases.

128. The SolarWinds Compromise is just one example of a threat to DHS data security.

129. On April 22, 2022, Defendant DHS announced the results of its "Hack DHS" bug bounty program, where cybersecurity and ethical hackers were invited to identify vulnerabilities in DHS systems. Defendant DHS confirmed that, in the first stage of the program alone, participants "identified 122 vulnerabilities, of which 27 were determined to be critical."[15]

---

[14] *See About CISA,* Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/about-cisa, (last accessed Jan. 3, 2023); *see also Remediating Networks Affected by the SolarWinds Active Directory/M365 Compromise – Resources: CISA, Federal Government, and International Partner Publications*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/remediating-apt-compromised-networks (last accessed Jan. 3, 2023).

[15] *See "Hack DHS" Program Successfully Concludes First Bug Bounty Program*, U.S. Dept. of Homeland Security, https://www.dhs.gov/news/2022/04/22/hack-dhs-program-successfully-concludes-first-bug-bounty-program, (last accessed Jan 3., 2023).

130. In the same announcement, Defendant Mayorkas stated, "Organizations of every size and across every sector, including federal agencies like the Department of Homeland Security, must remain vigilant and take steps to increase their cybersecurity. Hack DHS underscores our Department's commitment to lead by example and protect our nation's networks and infrastructure from evolving cybersecurity threats."

131. Defendants' conduct and statements demonstrate their knowledge of their own data security vulnerabilities. Defendants' prior statements also demonstrate their knowledge of the dangers of public disclosure of asylum-related information.

132. Despite the known and obvious risks of centralizing asylum-related information in a government database, Defendants failed to implement sufficient procedural or technical barriers to prevent public disclosure.

133. Instead, Defendant JOHN DOE 1 was able to post the information onto ICE.gov for any persecutor or bad actor anywhere in the world to view, download, distribute, and use for nefarious purposes. Therefore, Defendants were deliberately indifferent to the safety of Plaintiffs and those similarly situated.

134. The second exception in *DeShaney* applies. Therefore, the Equal Protection Clause imposes an affirmative duty of care and protection on Defendants toward Plaintiffs.

135. Defendants grossly violated their duties to Plaintiffs and those similarly situated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully ask this Court to issue judgment in their favor and against all Defendants, and to grant the following relief:

A. Certify a Class under Rule 23(b)(2), as described above;

B. Declare that Defendants violated the Privacy Act of 1974; the APA, and the equal protection principles of the Fourteenth Amendment, embedded in the Due Process Clause of the Fifth Amendment;

C. Order Defendant ICE to extend the original 30-day stay of removal for all impacted individuals to one year, and provide individuals who may have opted out (with or without coercion or full consent) with notice that they may take advantage of the additional stay.

D. Order Defendant ICE to cease the removal of Plaintiffs, and others similarly situated until their asylum and withholding of removal claims can be re-adjudicated, with the presumption of risk created by the data breach being presumed;

E. Order DOJ to rescind removal orders and reopen removal proceedings for individuals impacted by the unlawful disclosure of their confidential information;

F. Order Defendant DOJ to extend accommodations to Plaintiffs and others similarly situated so that the merits of any application for asylum, withholding of removal, and/or protection under the Convention Against Torture can be considered or reconsidered in light of the data breach, with the presumption of risk of danger created by the data breach being presumed;

G. Order Defendant DOJ to instruct immigration judges to take administrative notice of the breach and the presumption that the data breach created a risk of danger for all affected;

H. Award from Defendants a monetary award of $10,000 to each Plaintiff, and others similarly situated, pursuant to the Privacy Act;

I. Award compensatory and punitive damages of $5,000 to each Plaintiff and others similarly situated from Defendants, pursuant to the other counts above;

J. Retain jurisdiction over this action and any attendant proceedings until Defendants have fully implemented the Court's order;

K. Award Plaintiffs reasonable costs and attorneys' fees pursuant to the Equal Access to Justice Act, 28 U.S.C. § 2412; and

L. Grant such further relief as this Court deems just and proper.

Dated: January 20, 2023

Respectfully submitted,

/s/*Curtis Lee Morrison*

Curtis Lee Morrison

Morrison Urena, L.C.
8910 University Lane
Suite 400
Santa Diego, CA 92122
Tel: (323) 489-5688
Email: curtis@morrisonurena.com