GEORGETOWN LAW
Center on Privacy & Technology

UCI Law | International Justice Clinic

Submission to the United Nations Human Rights Committee During its Periodic Review of United States of America

12 September 2023

The Center on Privacy & Technology at Georgetown Law and the International Justice Clinic at the University of California, Irvine School of Law jointly submit to the Human Rights Committee this written contribution for the Committee's fifth cycle of periodic review on the United States of America.

This submission concerns paragraph 22 (the right to privacy) of the United States' list of issues prior to reporting (CCPR/C/USA/QPR/5). We write to inform the Committee of the U.S. Immigration and Customs Enforcement (ICE)'s dragnet surveillance practices, namely the collection and aggregation of personal information in databases, application of automated analytical tools, and data sharing, which are inconsistent with U.S. obligations under the International Covenant on Civil and Political Rights (ICCPR). The focus of our submission is on data that, unlike communications surveillance, is virtually unregulated by law, including what agencies call commercially or publicly available information. The United States has failed to include this issue in the state report (CCPR/C/USA/5) despite the severe and far-reaching impact caused by ICE's practice.

This report describes ICE's known data practices by referring as much as possible to the work done by civil society organizations and the media; because ICE's public disclosure is extremely limited, this report likely represents only the tip of the iceberg of ICE's intelligence activities. However, even the data practices of ICE that we are aware of violate the right to privacy guaranteed by Article 17 of the ICCPR. Further, the fear of provoking ICE's effectively disincentives immigrants and others from taking various actions, including the exercising fundamental human rights such as freedom of expression and peaceful assembly and of association.

Information of Submitters

The Center on Privacy & Technology at Georgetown Law undertakes research and advocacy to expose and mitigate the disparate impact of government and corporate surveillance on historically marginalized communities. We have published ground-breaking reports on police use of face recognition technology, and on the dragnet surveillance practices of federal immigration authorities in the United States. We are working towards a world where it is more possible for more people to resist mass surveillance.[1]

The International Justice Clinic at the University of California, Irvine School of Law, produces research and conducts advocacy promoting compliance with international human rights law and, *inter alia,* UN

[1] For more information, please see https://www.law.georgetown.edu/privacy-technology-center/.

human rights mechanisms. Since its founding in 2012, under the direction of Professor David Kaye, a former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Clinic has continuously researched and advocated for freedom of expression and privacy.[2]

Information on the United States of America's non-compliance with the Covenant

Relevant Articles of ICCPR
Articles 17(1)(2), 19(2)(3), 21, 22, and 2(3)(a)

The current law, policies, and practices of the United States

1. Backgrounds

U.S. Immigration and Customs Enforcement (ICE), established in 2003 along with the Department of Homeland Security (DHS) in the wake of the attacks of September 11, 2001,[3] is a U.S. federal agency which is responsible for (i) the enforcement of immigration laws such as investigation, arrest, detention, and deportation of immigrants who do not have visas or who are subject to outstanding removal orders (overseen by ICE's Enforcement and Removal Operations division (ERO)) [4], and (ii) investigation of cross-border criminal activity, e.g., terrorism, national security threats, drug, and human trafficking, etc., (overseen by ICE's Homeland Security Investigations division (HIS).[5] Prior to 2003, the functions of ICE, both ERO and HIS, were principally performed by the U.S. Immigration and Naturalization Service (INS) of the Department of Justice.

For much of the 20th century, the United States conducted large-scale deportations only from time to time in response to political events. However, since 1986 when Congress mandated that immigrants convicted of certain crimes be deported expeditiously, the number of deportations has increased dramatically due to the expansion of collaboration and information sharing between immigration agencies and state and local law enforcement agencies. These programs include: the Criminal Alien Program (CAP), which places federal immigration enforcement officers in prisons; 287(g) agreements, which allow state and local police to enforce immigration law; and the Secure Communities program, through which fingerprints of any person who is booked by federal, state, or local law enforcement are sent to ICE.[6]

Deportation policy changed markedly in the wake of the 9/11 terrorist attacks. Two of the fifteen 9/11 hijackers had "overstay" visas, meaning staying in the U.S. beyond the approved duration of their stay. In turn, the U.S. focused on ensuring the deportation of those with overstay visas or outstanding removal orders. Under the rubric of the so-called "war on terror," ICE secretly and aggressively expanded its data sources to include private companies and government agencies with no law enforcement functions. It now uses these sources to identify and locate suspected 'deportable' individuals, taking advantage of the lack of data privacy regulation in the United States.[7] As explained below, ICE carries out its dragnet surveillance with virtually no effective restraint and is routinely abused.

---

[2] For more information, please see https://ijclinic.law.uci.edu/.
[3] The U.S. Department of Homeland Security, *Creation of the Department of Homeland Security*.
[4] The U.S. Department of Homeland Security, *Enforcement and Removal Operations*.
[5] The U.S. Department of Homeland Security, *Homeland Security Investigations*.
[6] The Center on Privacy & Technology, *American Dragnet: Data-Driven Deportation in the 21st Century* (10 May 2022) [hereinafter American Dragnet], pages 18 and 19.
[7] *Id.*, pages 19-21.

While many issues have been reported regarding the exchange of information between ICE and domestic law enforcement agencies,[8] this report focuses on ICE's collection and use of information (especially those for which, unlike interception of communication, no prior judicial authorization is required under the law) obtained from non-law enforcement sources, including government agencies (both domestic and foreign ones) and private companies, where ICE can circumvent public scrutiny and procedural safeguards.[9]

This report aims at depicting the known major information streams by referring as much as possible to work by civil societies and the media to trying to shed light on ICE's practices through, for example, freedom of information requests and litigation; unfortunately, so far we only have "snapshots of specific initiatives" and "the full reach of ICE's surveillance dragnet still remains secret."[10] This report, in other words, does not claim to present a comprehensive picture of ICE's data practices.

2. ICE's data collection and use implicates the right to privacy

Article 17(1) guarantees the right to privacy, which includes informational privacy, meaning "the ability of individuals to determine who holds information about them and how that information is used."[11] As the Human Rights Committee indicated in its concern about the Colombian government's use of social media monitoring tools, privacy protection extends to publicly accessible information especially when systematically collected.[12] Privacy rights are equally guaranteed to all individuals within a state's jurisdiction, including non-citizens, regardless of documented or undocumented status.[13]

ICE has been collecting and using at least the personal information described below for its investigation and law enforcement purposes. The information that ICE obtains and uses is so extensive that ICE can, through the subsequent aggregation and merger with other datasets and the application of data analysis tools, reveal or infer individuals' online and offline behavior and traits, preference, and their relationships, with high granularity.

---

[8] One representative example is the Secure Communities program, which was launched in 2008, and its successor Priority Enforcement Program. S-Comm automatically shares with ICE fingerprints of any person who is arrested or detained by all federal, state, or local law enforcement agencies, in total of 3,181 agencies at the time of 2013. After the public scrutiny, S-Comm was suspended, but a similar information sharing program, Priority Enforcement Program (PEP) was implemented in 2014. Under PEP, the finger print sharing program across the U.S. remains unchanged and is still in place. *See* National Immigration Law Center, *Untangling the Immigration Enforcement Web* (September 2017), page 4, "Many advocates therefore called the changes [from S-Comm to PEP] cosmetic".

[9] *See* Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR): The right to privacy in the digital age, A/HRC/51/17 (4 August 2022), para. 42.

[10] *Supra* note 6, page 13.

[11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 (17 April 2013), para. 22.

[12] Human Rights Committee, Concluding Observation on Nigeria in the absence of its second periodic report , CCPR/C/NGA/CO/2 (29 August 2019), para 40; Human Rights Committee, Concluding Observation on the seventh March periodic report of Colombia, CCPR/C/COL/CO/7 (17 November 2016), para. 32. *See also* OHCHR, *supra* note 9, para. 42.

[13] Article 2(1) of International Covenant on Civil and Political Rights (entered into force 23 March 1976), article 2, para. 1; and Human Rights Committee, General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (26 May 2004), para.10.

The expansion of ICE surveillance has been driven and enabled by private companies. One expert we interviewed observed that some technology companies, in the aftermath of the dot-com bubble burst around 2000, began seeking government contracts, including those from federal departments including DHS, as a means to compensate for declining revenues. The expert went on to explain that, with the heightened participation of private companies, DHS and ICE's surveillance operations have evolved into an industrial complex, with a business model based on mass data collection.[14]

2.1 ICE's data collection

2.1.1 Geolocation data or home address

ICE is obtaining geolocation data or home addresses through various sources without individuals' awareness. These data are particularly sensitive to immigrants as it enables ICE to locate them.

Automated License Plate Scanning

ICE has access to license plate scanning databases, sometimes built and sold by private companies such as Vigilant Solutions, and sometimes created and maintained by local law enforcement agencies. These databases contain billions of pieces of data collected by high speed cameras that capture the license plates of passing vehicles, along with the date, time, and GPS coordinates of where the image was captured. Data is collected without regard to whether a vehicle is under suspicion at the time of scanning, and subsequently, the data is entered into a database for both retrospective and real-time searches through license numbers or geographical queries.[15] According to documents obtained by ACLU of Northern California through a freedom of information request, Vigilant Solutions gathers commercial license plate scans at over 5 billion points of location, including toll roads, parking lots, and garages as well as by private vehicle repossession agents across 47 states.[16] This coverage spans metropolitan areas that include about 54% of the entire population of the United States, and automated license plate readers operate without the awareness of most of the drivers whose data they collect.[17] ICE has obtained access to an additional 1.5 billion records of the automated license plate scanning shared by over 80 local law enforcement agencies.[18]

From the language of ICE's public notice, disclosing the collection of these information associated with a target of investigation,[19] a person could not be expected to anticipate that data is gathered so often in such a wide area, and hosted in a database for ICE's retrospective search of location information.

---

[14] Interview conducted with Alli Finn, the Senior Researcher & Organizer, the Surveillance Resistance Lab. Notes on file with authors. *See also* the Surveillance Resistance Lab, *DHS Open for Business: How Tech Corporations Bring the War on Terror to Our Neighborhoods* (2022); and the Immigrant Defense Project, the Center for Constitutional Rights, *Submission to the Office of the High Commissioner for Human Rights on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies* (February 2022).

[15] *See* The U.S. Department of Homeland Security, *Privacy Impact Assessment for the Acquisition and Use of License Plate Reader (LPR) Data from a Commercial Service* (21 May 2021).

[16] American Civil Liberties Union, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations* (23 March 2019).

[17] *Id.*

[18] *Id*.

[19] The U.S. Department of Homeland Security, *DHS/ICE-009 External Investigations System of Records Notice* (20 November 2020) [hereinafter External Investigations SORN]; and the U.S. Department of Homeland Security, *supra* note 15.

App-based location data

According to the first report by The Wall Street Journal in 2020 and documents subsequently obtained by ACLU through freedom of information requests and litigation,[20] at least until June 2023 ICE was purchasing access to a database of geolocation information operated by a private location data broker, Venntel.[21] The way these companies build their datasets is by leveraging the advertising identifier (or ad ID) – which is randomly but uniquely assigned to individuals' mobile phones, which are originally designed to enable advertisers to track individuals' online behavior and show personalized ads on devices. The ad IDs bundle a variety of data, including but not limited to data generated by apps downloaded to the phones, phone browser history, and precise location information. Individuals often do not know and have no way to discover that their phone use is generating this data and that data from a commercial database is widely shared with law enforcement agencies such as ICE.[22] In its public notice, ICE states "ICE may receive information in the course of its law enforcement investigations from nearly any source," including "commercial data aggregators," failing to provide further details.[23]

Vehicle registration and driver's license database

According to documents obtained by the Center on Privacy and Technology through a FOIA request, ICE has, at least since 2008, accessed detailed records of drivers and vehicle registrations, including name, address, date of birth, physical description, Social Security number, license type, driver's restrictions, license status, license number, and a driver's license photo (if states permit), which are collected and managed by each state's department of motor vehicles ("DMV").[24] In its public notice, ICE discloses that they collect "license information for owners and operators of vehicles;" however, it fails to disclose how and when it accesses the information.[25]

ICE accesses data in at least three different ways.[26] First, ICE either directly requests DMV employees to search a database using biographical information or runs face recognition searches in the database and compares face images which ICE has. Under the long-established relationship between ICE and the particular DMV or a specific data sharing agreement, meaning they automatically follow ICE's requests. Evidence suggests that ICE makes hundreds of thousands of requests to DMV offices.[27] Second, ICE accesses DMV databases via the International Public Safety and Justice Network (Nlets), which is a network through which the DMV databases are shared among states and the federal, state, and local government law enforcement agencies and parallel entities abroad.[28] Nlets hosts states' drivers databases in 34 states. According to the documents obtained by the Center, ICE issues tens of thousands of driver's

[20] American Civil Liberties Union, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data* (18 July 2022).
[21] *See* Politico, *Homeland Security records show 'shocking' use of phone data, ACLU says*, (18 July 2022).
[22] *See* the Electronic Frontier Foundation, *How Ad Tech Became Cop Spy Tech* (31 August 2022).
[23] External Investigations SORN.
[24] *See* American Dragnet, page 26-41.
[25] External Investigations SORN.
[26] *See* American Dragnet, page 30.
[27] *Id*., page 31-33.
[28] *Id*., page 34. Nlets is operated by a not for profit corporation owned by participating Stated. Despite the sensitivity of shared information as well as the broad scope of information sharing, such an ownership structure makes Nlet avoid audit or public disclosure requirements, which makes the public accountability even more difficult. *See* Nlets Media, *Who We Are*; and Just Futures Law, *State Driver's License Data: Breaking Down Data Sharing and Recommendations for Data Privacy* (5 March 2020).

licenses and vehicle registration queries each month through Nlets. For example, ICE issued 3,185 driver's license or vehicle registration queries to Nlets over a 41-day period in Wisconsin alone.[29] Third, ICE is accessing driver's license records via private data brokers which acquired these data from DMV. According to the government's disclosure on federal spending, in 2021, ICE purchased Law Enforcement Investigative Database (LEIDS) by LexisNexis Risk Solutions. The company directly purchased DMV's driver's license information from 12 states such as Arizona, California, the District of Columbia, Florida, Illinois, Minnesota, Nebraska, Nevada, North Carolina, Oregon, South Carolina, Tennessee, and Wisconsin (for more details of LEIDS, please see 2.1.5 below).[30] Data protection law at the federal level does not reach this information, and most states fail to prohibit their DMV from selling its data to brokers.[31]

Utility companies' billing information databases

Since 2010, ICE has had access to the billing information of utilities customers provided by private data brokers. According to the report by the Center on Privacy and Technology, the data broker, Thomson Reueters acquired the dataset from Equifax, a private consumer credit reporting agency company which operates a database containing millions of utility customers' payment records on behalf of the association of utility companies called National Consumer and Telecom Utilities Exchange (NCTUE), which was established for the purpose of providing participating billing companies with credit risk.[32] In its public notice, ICE states that it "may receive information in the course of its law enforcement investigations from nearly any source," including "commercial data aggregators."[33] Given the sensitivity of utilities data, and the impossibility of opting out of crucial services like water and electricity, ICE's failure to disclose its reliance on utility data is extremely concerning.

In October 2021, NCTUE instructed Equifax to end the sale of customer records; however, LexisNexis, a data broker which ICE is currently contracting, reveals that multiple different utility companies can provide similar services.[34] Some states moved to regulate ICE accessing the data[35] but there has been no movement to regulate on the federal level.

2.1.2 Details of financial transactions

ICE has access to a vast amount of financial transaction records, far more than revealed by ICE's public notice, which says it collects "suspicious financial activity, currency transaction reports, and currency or monetary instrument reports."[36]

Information on money transfers sent to or from the Southwest border region

---

[29] American Dragnet, page 34.
[30] *See* American Dragnet, pages 35 and 36.
[31] *See id*., page 37-41.
[32] *See id.*, page 42-54. *See also*, The Washington Post, *ICE investigators used a private utility database covering millions to pursue immigration violations* (26 February 2021).
[33] For example, External Investigations SORN; and the U.S. Department of Homeland Security, *DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records* (19 October 2016).
[34] *See* American Dragnet, page 49.
[35] *See* NBC San Diego, *Newsom Signs Todd Gloria Bill To Limit ICE's Use of Customer Utility Data* (28 September 2020).
[36] For example, External Investigations SORN.

In 2022, it was revealed that ICE has access to a database of over 145 million records of money transfers. These include transfers sent to or from states bordering Mexico, namely, Arizona, California, New Mexico, Texas, and Mexico, and transfers of more than USD 500 since 2010. The database is owned and operated by an association of federal and state law enforcement agencies (the Transaction Record Analysis Center), including ICE. ICE admitted that, since 2019, it obtained, by using an administrative subpoena (which is issued without independent authorization or oversight) approximately 6 million records from money transfer companies.[37] Such transfers provide essential services to immigrants to transfer to and receive money from families or close friends in other countries.[38]

ICE has suspended its data requests to money transfer companies; however, ICE continues to be a member of the association, meaning maintaining access to the database, which hosts an immense amount of records,[39] where ICE's contributed data consist only of 3%.[40]

Cryptocurrency transaction details

According to documents obtained in 2022 by Tech Inquiry through a freedom of information request, in 2021, ICE obtained access to the details of cryptocurrency transactions from Coinbase Tracer, an intelligence-gathering tool provided by Coinbase, the largest cryptocurrency exchange in the United States. Although the details of cryptocurrency transactions are publicly accessible on cryptocurrency ledgers, Coinbase Tracer enables users to pull meaningful information from the sea of records stored there, which is almost practically impossible without relying on such software.[41]

2.1.3 Face image databases

ICE runs facial recognition tools on DMV's face image databases to find records since as early as 2008, when ICE acquired a facial recognition database from Rhode Island's DMV. Since 2015, ICE has requested face recognition scans of DMV databases in at least 14 states. ICE's use of facial recognition tools further extends to DMV use of 34 states which are hosted by Nlets (for details of Nlets, see 2.1.1). Despite such widespread use, ICE has been applying facial recognition tools in extreme secrecy and without oversight. For example, in Maryland, ICE was conducting facial recognition scans on the database of the Department of Transportation (MDOT) without MDOT's knowledge of the details.[42]

ICE's application of facial recognition tools is not just DMV databases. Government contracting records show that ICE has been one of the clients of Clearview AI, Inc. since 2021,[43] which provides a system enabling searches of facial images against more than 30 billion such images scraped and indexed from

---

[37] *See* Buzzfeed News, *ICE Conducted Sweeping Surveillance of Money Transfers Sent To And From the US, A Senator Says* (8 March 2022).
[38] *See* Just Futures Law, *Consumers Sue ICE and Money Transfer Companies for Secretly Collecting and Sharing Millions of Private Financial Records* (12 December 2022); and First Amended Class Action Complaint, *Sequeira v. Dept. Homeland Security* (12 December 2022).
[39] *Id.*
[40] Buzzfeed News, *supra* note 37.
[41] The Intercept, *Cryptocurrency Titan Coinbase Providing "Geo Tracking Data" to ICE*, (29 June 2022).
[42] *See* American Dragnet, pages 32-35.
[43] *See* USAspending.gov, *Contract Summary*, Purchase Order (PO) PIID 70CMSD20P00000130; and *Contract Summary*, Purchase Order (PO) PIID 70CMSD21P00000127.

public sources on the Internet.[44] The Office of the United Nations High Commissioner for Human Rights (OHCHR) articulated in its report that the database constitutes "a massive intrusion of privacy rights".[45]

To date, ICE has refused to specify the purposes of its use of the database provided by Clearview AI[46] However, documents obtained by ACLU Northern California and Just Futures Law suggests that ICE uses Clearview AI for "certain types of criminal investigations that meet specific, defined parameters", maintaining an excessively wide discretion on the use of the database.[47]

2.1.4 Social media monitoring

Social media monitoring tools

As revealed in a media report, in 2020 and 2021, ICE purchased social media monitoring tools, which aggregate individuals' public online behaviors on more than 120 social media networks, dating apps, and websites like Amazon as well as on the dark web, and enable users to monitor individuals' online behavior.[48] Such functionalities are well beyond the scope of ICE's public notice, which only mentions "[s]ocial media handles or account names and publicly available social media posts".[49] Although the specific functions of the tools subscribed to by ICE have not been disclosed, some social media monitoring tools perform analytical functions, such as identifying specific individuals as well as their location, behavioral patterns, relationships with others such as suspects as well as predicting potential future crimes.[50] Such social media monitoring tools entail a number of serious human rights risks, including privacy implications,[51] the reinforcement of existing discrimination and bias, and the chilling effect on an individual's exercise of various human rights.[52]

Use of administrative subpoena

It is quite possible to use social monitoring tools to link anonymous accounts to legal identities, but in cases where that is difficult ICE has the fallback option of issuing administrative warrants or subpoenas to social media such as YouTube, Meta, Twitter, etc. According to documents obtained by WIRED through a freedom of information request, ICE issued custom summonses (customs summonses are one type of administrative subpoena), "more than 170,000 times from the beginning of 2016 through mid-August 2022" and the primary recipients include several major tech companies.[53] Media reports indicate a very concerning trend in which social media companies often comply with administrative warrants or subpoenas, without providing users with an opportunity to be heard. In one case in March 2021, Los

---

[44] *See* Clearview AI, Inc., https://www.clearview.ai/.
[45] OHCHR, *supra* note 9, at para. 42.
[46] In response to a media query, ICE stated that its use of Clearview Al database is primarily for investigation of child exploitation and other cybercrime cases. *See* The Register, *ICE to see you: Homeland Security's immigration cops tap up Clearview AI to probe child exploitation, cyber-crime* (15 August 2020).
[47] *See* Just Futures Law, Mijente, Immigrant Defense Project, ACLU Northern California, *Records Provide More Insight into ICE Use of Clearview AI, Suggesting Broader Use, Lack of Oversight, and Internal Concerns* (May 2022).
[48] The Intercept, *Shadowdragon: Inside The Social Media Surveillance Software That Can Watch Your Every Move*, (21 September 2021),
[49] External Investigations SORN.
[50] *Id*.
[51] Human Rights Committee, Concluding Observation on Nigeria, *supra* note 12, para 40.
[52] *See* OHCHR, *supra* note 9, paras. 43-47. *See also* Brennan Center for Justice, *Brennan Center Files Freedom of Information Act Requests for Information on DHS's Use of Social Media Monitoring Tools* (19 September 2022).
[53] WIRED, *ICE is grabbing Data from Schools and Abortion Clinics* (3 April 2023).

Angeles Times reported that Google informed a user whose information was the target of the subpoena that, unless it receives within seven days a copy of a court-stamped motion to quash the request, Google may hand over the requested information by administrative subpoena issued by DHS, a parent agency of ICE, which requests "the names, email addresses, phone numbers, IP addresses, street addresses, length of service such as start date, and means of sources of payment linked in any way to one specific Google account," which was attached to Youtube and Gmail among other services.[54]

2.1.5 Access to data brokers' databases

According to documents obtained by a journalist through a freedom of information request, ICE has subscribed to Law Enforcement Investigative Database (LEIDS) by LexisNexis Risk Solutions, which "vacuums up" and aggregates information about individuals from a myriad of data sources, to support their "all aspects of ICE screening and vetting, lead development, and criminal analysis activities".[55] Although neither ICE nor LexisNexis disclose the list of data sources the database covers, media reports show that such sources would include credit history, bankruptcy records, license plate images, and mobile subscriber information as well as customer data of utility companies or drivers' licenses and vehicle registration information as we see above.[56] As the documents obtained by The Intercept shows, the database works in conjunction with the automated license plate reader systems.[57] The documents also revealed that the database performs automated data analytics on the aggregated data, and apparently identifies links between people, places, and property, and claims to make predictions about potential future criminal and fraudulent behavior.[58]

Neither ICE nor the corporation have disclosed details about the purpose of the database, the algorithms used, or the training data. As OHCHR pointed out, law enforcement is one of the key areas where the application of so-called "AI" tools has given rise to particularly serious concerns, including privacy intrusions, the reliance by law enforcement on inaccurate or discriminatory technology to make decisions that have serious consequences for rights and liberties, the difficulty of government accountability due to the high opacity of algorithm-based decisions, and the enhancement of existing discrimination and bias.[59] ICE's total lack of transparency further heightens these concerns.

2.1.6 Welfare records of unaccompanied children at Office of Refugee Resettlement[60]

Each year, unaccompanied children cross the U.S. borders to flee from violence and poverty. In 2018, the number of such children reached nearly 50,000. When these children encounter border control agencies, they are referred to the Office of Refugee Resettlement (ORR), which is responsible for finding family members or guardians who can sponsor each child.[61] During the course of the process, ORR interviews children and requests that potential sponsors provide extensive personal information such as "their contact

---

[54] Los Angeles Times, *This is what happens when ICE asks Google for your user information* (24 March 2021).
[55] The Intercept, *Lexisnexis Is Selling Your Personal Data to ICE So It Can Try To Predict Crimes* (20 June 2023).
[56] The Intercept, *Lexisnexis to provide Giant Database of Personal Information to ICE* (10 April 2021).
[57] The Intercept, *supra* note 55.
[58] *Id*.
[59] Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age, A/HRC/48/31 (13 September 2021), paras. 21-24.
[60] For this section in general, *see* American Dragnet, pages 56-64.
[61] Trafficking Victims Protection Reauthorization Act (TVPRA) of 2003, Pub. L. No. 110-457, § 235(b)(3), 117 Stat. 5077 (2008).

information, proof of address, information about others living in the household, financial information, and information about their relationship to the child".[62]

From 2017 to 2021, ICE accessed years of ORR's records containing information provided by unaccompanied children and potential sponsors, and used that information to arrest and deport potential sponsors and their community members through a data sharing agreement with ORR. They did this under the pretext of investigating human trafficking. Out of 400 individuals who were arrested during the life of this program, nobody was ever charged with human trafficking crimes.[63] In addition to the privacy harms that resulted from this information sharing program, it is well documented that ICE's use of ORR records for enforcement activity deterred potential sponsors from coming forward. A survey conducted by the Women's Refugee Commission and National Immigrant Justice Center of people working with unaccompanied children (e.g., child advocates, lawyers, biometric technicians) showed that 75% of respondents knew of potential sponsors who gave up becoming sponsors as a result of data-sharing between ORR and ICE.[64] This resulted in an even greater number of already traumatized children languishing in overcrowded cells at border patrol facilities.

2.1.7 Surveillance under Alternatives to Detention programs

Since 2004, ICE ERO has been expanding its Alternatives to Detention (ATD) programs, which are a suite of different surveillance programs that ICE defines as "a cost-effective alternative to detention for a subset of noncitizens who are deemed suitable for enrollment on ICE's non-detained docket".[65] In fact, ICE does not use ATD to reduce the number of people subject to immigration detention, but to expand the custody net overall. The detention budget is increasing alongside ICE's budget for ATD programs, and ICE is using ATD programs to extend their control over a greater number of people and to expand their surveillance mechanisms across a wide range of technologies and platforms.[66]

Under one ATD program, 4,874 people are forced to wear an ankle bracelet which continuously tracks and logs GPS points and is subject to 24-hour, real-time GPS surveillance by ICE.[67] 252,185 individuals are being monitored using a so-called SmartLINK smartphone app downloaded to people's smartphones, enabling ICE to send a request to people to check-in by submitting their facial images, sometimes at a predetermined time and sometimes spontaneously. ICE confirms "location, curfew compliance and travel restriction compliance" at the time of check-in.[68] ICE's disclosure states that ICE only obtains location information during check-ins or when people log into the app, but reports indicate that people were told by

[62] American Dragnet, *supra* note 5, page 58.
[63] NPR, *ICE Has Arrested More Than 400 In Operation Targeting Parents Who Pay Smugglers* (18 August 2017).
[64] National Immigrant Justice Center, Women's Refugee Commission, *Children as Bait: Impacts of the ORR-DHS Information-Sharing Agreement* (March 2019).
[65] The U.S. Department of Homeland Security, *Privacy Impact Assessment for the Alternatives to Detention (ATD) Program* (17 March 2023).
[66] *See* American Immigration Council, *Alternatives to Immigration Detention: An Overview* (11 July 2023), page 2.
[67] *Id*., page 3; EPIC, *New ICE Privacy Impact Assessment Shows All the Way the Agency Fails to Protect Immigrants' Privacy* (20 April 2023) ("'Whoever finds out that I'm wearing [the ankle monitor], they don't get close to me anymore,' said a 39-year-old man from Mexico. 'I dream of the day somebody will cut it.'"); and The Guardian, *A US surveillance program tracks nearly 200,000 immigrants. What happens to their data?* (14 Mar 2022).
[68] Inewsource, *ICE uses cellphones to track thousands in San Diego, Imperial counties* (23 May 2022) ("When ICE enrolled [one SmartLINK user] in SmartLINK, they told him they could see everywhere he went, he said. 'It just puts a sense of fear in me that at any given moment I can be taken into custody again,' he said.)

ICE's contractor that it "always running and she always had to have [their] location services on", suggesting a wider collection of location data and surveillance.[69] Data collected through these programs are stored in ICE databases, including the Enforcement Integrated Database (EID) (see 2.2 below), which enables ICE to access historical data.[70]

2.1.8 Information shared by foreign governments

ICE has obtained access to a large set of personal information from foreign law enforcement agencies (such as criminal history and gang affiliation) through data sharing agreements such as the ICE-led Security Alliance for Fugitive Enforcement (SAFE) program, which is a network composed of foreign law enforcement agencies and immigration authorities. ICE relies on data from countries which have serious deficiencies in the rule of law such as El Salvador, Guatemala, and Honduras.[71] Another example of problematic transnational datasets is theFBI-led Transnational Anti-Gang (TAG) Task Force Initiatives. Just as gang designations made by law enforcement agencies in the U.S. have been shown to be subjective, shifting and often pretextual, gang affiliation as determined by law enforcement agencies in other countries is often based on "vague and ill-defined factors", "including 'tattoos; associates; family members; residential locations; locations frequently visited; dialect and words using while speaking; manner of dress' and other factors".[72] ICE detains and deports people and deprives immigration benefits based on, sometimes solely on, allegations of foreign crimes or affiliation with gangs without verifiable evidence.[73]

Aside from the serious lack of accuracy and credibility of gathered data and total denial of due process, ICE's public notice only vaguely suggests that they collect case files, indexes, and records of foreign government agencies,[74] and the above detrimental consequences cannot be anticipated from such disclosures.

2.2 ICE's use of information

According to ICE's major public notices, the information obtained by ICE is merged into databases, fed into analytics tools, and shared with other law enforcement agencies.

Merged into databases and retrieved for law enforcement activities

---

[69] EPIC, *New ICE Privacy Impact Assessment Shows All the Way the Agency Fails to Protect Immigrants' Privacy* (April 20, 2023).
[70] The U.S. Department of Homeland Security, *supra* note 65.
[71] *See* National Immigrant Justice Center, Access Now, Cristosal, and Stanford Law School's International Human Rights & Conflict Resolution Clinic, a Complaint with the Office of Civil Rights and Civil Liberties at the U.S. Department of Homeland Security, (6 June 2023) ("In using unreliable information from El Salvador, the United States violates the ICCPR right to the presumption of innocence and the right to privacy." *See also* relevant case examples at pages included in the complaint); National Immigrant Justice Center, *Caught in the Web* (December 2022), pages 3-5.
[72] National Immigrant Justice Center, Caught in the Web, *supra* note 71, page 4.
[73] *See* National Immigrant Justice Center, Access Now, Cristosal, and Stanford Law School's International Human Rights & Conflict Resolution Clinic, *supra* note 71; and National Immigrant Justice Center, Caught in the Web, *supra* note 71, pages 4-5.
[74] *See* the U.S. Department of Homeland Security, Privacy Impact Assessment for the enforcement integrated database (EID) (14 January 2010) [hereinafter PIA for EID]; External Investigations SORN; and supra note 33.

The information that ICE gathers through the methods described above goes to populate a myriad of federal databases,[75] which enables users to retrieve information about specific individuals. The representative example is the Enforcement Integrated Database (EID), which ICE describes in its public notice as "a common database repository owned and operated by [ICE] that supports the law enforcement activities of ICE and other DHS components".[76] EID hosts extensive information which is "collected from witnesses, victims, or criminal associates, and from official records of other agencies, businesses, and other sources during the course of DHS mission operations", such as the data described in the 2.1 of this report.[77]

Typically, authorized ICE officers can make queries to EID and import the retrieved data to a specific case file created on Investigative Case Management (ICM), which is ICE's "core law enforcement case management tool", and use the retrieved data for their investigations or law enforcement.[78]

Use of data in algorithmic analysis tools (RAVEn)

ICE is ingesting information contained in EID, ICM, and other government or commercial databases to an algorithmic platform called the Repository for Analytics in a Virtualized Environment (RAVEn), which started to be developed in 2018 and currently partially implemented.[79] RAVEn "facilitate[s] large, complex analytical projects" by "curat[ing] and chain[ing] together seemingly disparate raw datasets" and "isolate patterns of activity which are indicative of criminal activity and provide investigators access to the information needed to successfully disrupt and dismantle criminal networks."[80] Notably, ICE asserts that it uses "Artificial Intelligence (AI), or machine learning, in many RAVEn tools to better recognize patterns in data and enhance the tool's effectiveness."[81] ICE offers no guidance on what it means by the terms "artificial intelligence" or "machine learning" which are notoriously vague terms which corporations use to market a wide range of algorithmic products that use a wide range of different types of data.

In spite of the contract size (reportedly worth up to USD 300 million),[82] publicly available information is very limited. While the DHS website gives examples of some of the technologies developed and operated under the RAVEn project such as facial recognition services and mobile data analytics services which they say allows them "to view and analyze massive amounts of data resulting from court ordered mobile device extractions",[83] ICE has not disclosed the full list of tools in operation or planned for future deployment, let alone the underlying algorithms used, training data, and data analyzed for each tool.

---

[75] American Immigration Council, *Uncovering Immigration Enforcement Agency Databases* (15 March 2021).
[76] PIA for EID, page 2. *See also*, External Investigations SORN; and The U.S. Department of Homeland Security, *supra* note 33.
[77] PIA for EID, page 9.
[78] The U.S. Department of Homeland Security, *Privacy Impact Assessment for ICE Investigative Case Management* (16 June 2016).
[79] Brennan Center for Justice, *A Realignment for Homeland Security Investigations* (29 June 2023), page 12 and footnote 173.
[80] The U.S. Department of Homeland Security, *Privacy Impact Assessment for Repository for Analytics in a Virtualized Environment (RAVEn)* (13 May 2020), page 2.
[81] *Id*.
[82] Insider, *Amazon, Google, Microsoft, and other tech companies are in a 'frenzy' to help ICE build its own data-mining tool for targeting unauthorized workers* (1 September 2021).
[83] The U.S. Department of Homeland Security, *Artificial Intelligence Use Case Inventory*.

Data sharing with other government agencies within and outside of the United States

ICE widely shares its databases, and specific information sets within those databases, with other agencies. In the case of the information hosted by EID, according to ICE's public notice, other agencies within DHS are granted access to EID to the extent that the access to the data is within their authorities.[84] Outside of DHS, EID data is shared with other U.S. law enforcement agencies (i.e., those on federal, state, local, and tribal levels) based on law enforcement sharing agreements or through data sharing networks (state and local law enforcement agencies delegated DHS's law enforcement authority have access to EID). ICE's EID is plugged into DHS's Homeland Advanced Recognition Technology System (HART), where a large set of databases owned by different agencies within and outside of the US, are consolidated for the facilitation of inter-agency information sharing.[85] ICE also shares EID data on an ad-hoc basis with other U.S. agencies as well as foreign or international agencies that "demonstrate a need to know in the performance of their missions" or during the course of collaborating, assisting, and supporting national intelligence and security investigations.[86]

Because of the myriad of such agreements and arrangements, it remains difficult to get a comprehensive picture of information sharing between ICE and other agencies (both domestic and international) and to ascertain the conditions of information sharing or the existence and effectiveness of oversight mechanisms.[87] Experts point out that it is urgently needed to shed light on the complex mechanisms of information sharing among these different institutions.[88]

3. ICE fails to fulfill its obligations under Article 17

ICE's data practices put the U.S. in violation of its obligations under Article 17, which prohibits unlawful or arbitrary interference with the right to privacy.

3.1 Legality

Article 17(1) requires that any interference with privacy should be lawful, meaning based solely on laws that are themselves governed by the provisions, purpose, and intent of the ICCPR.[89] Further, the law must be sufficiently accessible, clear, and specific to avoid affording states unchecked discretion and to enable individuals to determine who has the authority to engage in data surveillance and under what conditions.[90]

A legal basis for each of the ICE data practices described above and their conformity to these requirements must be verified. ICE appears to be engaging in the above-described data practices as an

[84] PIA for EID, page 17.
[85] The U.S. Department of Homeland Security, *Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1* (24 February 2020).
[86] PIA for EID, page 19.
[87] *See* EPIC, *Government Databases*.
[88] Interview conducted with Jesse Franzblau, Senior Policy Analyst, National Immigrant Justice Center. Notes on file with authors. The Human Rights Committee expressed concerns multiple times about the human rights risks associated with the cross-border intelligence sharing (Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7 (17 August 2015), para. 24; and Concluding observations on the seventh periodic report of Sweden, CCPR/C/SWE/CO/7 (28 April 2016), para. 36).
[89] Human Rights Committee, General Comment No. 16 (1988): Article 17 (Right to Privacy), CCPR/C/GC/16 (8 April 1988), para. 3.
[90] Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (30 June 2014), A/HRC/27/37, para. 23.

exercise of a blanket investigatory power, which the U.S. Congress has not explicitly granted. For example, in its public notice on the Enforcement Integrated Database (EID), ICE lists laws which it claims authorize the collection of information to be hosted in EID.[91] The list includes 8 U.S.C. § 1357(a), which sets out the powers that ICE offices have to arrest, detain, and interrogate people without a warrant; however, there is nothing in the language of that section of the statute that relates at all to documentary evidence, to digital record keeping, or could in an way provide a legal basis for the acquisition, aggregation, and analysis of such extensive data as implicated in the case of the EID database.[92]

3.2 Necessity and Proportionality

Article 17(1) requires any interference with privacy to be nonarbitrary, meaning it should be necessary to pursue a legitimate aim, as well as proportionate to the aim.[93] Specifically, the necessity test requires the method deployed to be the least restrictive or only means of achieving a legitimate aim pursued.[94] The proportionality test requires the existence of a benefit that is balanced by the degree of infringement of the right to privacy, e.g., the seriousness of the crime involved (in particular, the acquisition and use of data for the purpose of mere removal of people with overstay visa is strongly presumed to violate proportionality test), the indispensability of the data to the investigation or prevention of the crime, the unavailability of other methods, and the limitation of the scope of data to be collected and used the minimum.[95]

Further, such evaluation should be demonstrated by states on a case-by-case basis, prohibiting them from collecting and using bulk data.[96] States are prohibited from setting aside these detailed tests in the name of countering terrorism and serious crimes.[97]

Due to extremely limited transparency, it is difficult to say with certainty which of ICE's data collection activities may meet the test of necessity and proportionality. Nonetheless, it is quite evident from what we do know that the primary purpose of ICE's dragnet surveillance practices is to aggregate as much data as possible to create a surveillance environment in which ICE will be able to use its data infrastructure to carry out a*ny goal that might arise for the agency at any time in the future*. The speculative nature of this purpose is in stark opposition to the spirit of the necessity and proportionality requirements of the ICCPR. ICE employees apparently collect personal information or access EID (ICE's common database which hosts a wide variety of personal information obtained in the course of investigation or enforcement activities), whenever there is *some* investigative or law enforcement need to do so, without examining the degree of importance of the aim sought, the relevance of data to the aim, the availability of less intrusive options to pursue the aim, and the scope of data to be acquired and used. For example, the public notice about EID states "DHS officers/agents capture this information for the purpose of conducting

[91] The U.S. Department of Homeland Security, supra note 72, page 13.
[92] 8 U.S.C. § 1357(a).
[93] Human Rights Committee, *Madhewoo v Mauritius*, CCPR/C/131/D/3163/2018 (16 September 2021), paras. 7.4 and 7.6. *See also*, *Vandom v. Republic of Korea*, CCPR/C/123/D/2273/2013 (10 August 2018), para. 8.8; *Van Hulst v. Netherlands*, Communication No. 903/1999, CCPR/C/82/D/903/1999 (15 November 2004), para. 7.3; and *Toonen v. Australia*, communication No. 488/1992 (31 March 1994), para. 8.3.
[94] OHCHR, *supra* note 90, para. 25.
[95] *See id.,* at 25-27; and the Electronic Frontier Foundation and a coalition of NGOs, *Necessary & Proportionate on the application of human rights to communication surveillance* (May 2014).
[96] *See* Human Rights Committee, *supra* note 89, para. 8; and OHCHR, *supra* note 90, para. 25.
[97] OHCHR, *supra* note 90, para. 24.

investigations, operations and other enforcement and case management activities related to the enforcement of U.S. immigration laws and federal criminal laws enforced by DHS",[98] and EID can be accessed by those who "have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions".[99]

3.3 Protection of the law

Article 17(2) states that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. To guarantee such protection, states must ensure that any privacy interference is authorized by law which (i) is sufficiently accessible to individuals, meaning being publicly accessible and sufficiently precise and specify the precise circumstances in which the privacy interference may be permitted with sufficient details to enable individuals to foresee the consequences that a given action may entail and self regulate their conducts accordingly and (ii) provides for effective safeguards against abuse.[100] Given the severe level of privacy interference caused by the ICE' above data practices, Article 17(2) requires robust safeguards.

First of all, there is no general privacy protection law at the federal level in the United States, enabling private companies such as data brokers to make profits from an almost free hand in acquiring personal information, irrespective of its sensitivity, and providing it to law enforcement agencies such as ICE. Relying on private companies' claim that they obtained this data "legally," ICE also labels such data as commercially available data or open source data and obtains and uses it almost freehand. As a result, tens of millions of people remain susceptible to privacy interference of which they have no notice.

Aside from the general lack of privacy law, we see the following deficiencies in ICE's data practice.

Accessibility

ICE's data practices well exceed what a reasonable individual would expect based on its public disclosure. Against the background of this lack of accessibility in ICE's notice of its data practices, immigrants in the U.S, are engaging in activities (including activities that are necessary for survival) which may end up subjecting them or their loved ones to detention and deportation, a consequence that they have no chance to foresee. For example, as the Center on Privacy of Technology reported, immigrants who have spent decades of years in the US are being suddenly arrested and deported just because, for example, they obtained a driver's license or signed up for electricity and water, never imagining that those agencies that claim to exist to provide essential services and benefits would turn around and share sensitive information with immigration authorities. This betrayal of trust is further exacerbated in states and municipalities which have adopted sanctuary policies promising not only that they are a safe place for immigrants "live, work, drive, and thrive" (as in Washington state), [101] but also in many cases pledging not to cooperate with ICE.[102]

---

[98] The U.S. Department of Homeland Security, *supra* note 72, page 11.
[99] External Investigations SORN.
[100] Human Rights Committee, *supra* note 89, para. 8; Concluding Observation on the United States of America, CCPR/C/USA/CO/4 (23 April 2014), para. 22. *See also* OHCHR, *supra* note 90, paras. 28-30.
[101] *See* American Dragnet, pages 11-12 and 27.
[102] In general, sanctuary policy prohibits local law enforcement agencies from helping with federal immigration enforcement. *See* the Immigrant Legal Resource Center, *Searching for Sanctuary and The Rise of Sanctuary* (December 2019) and *National Map of Local Entanglement with ICE* (13 November 2019).

Effective safeguards

ICE explains in its public notice that various safeguards prevent any abuse of their authority for data collection and use. For example, they claim that there are security policies and procedures to ensure that only authorized users have access to EID, that individual users have access levels that are appropriate only to their role, and that users of EID are monitored and tracked so that inappropriate users can be detected.[103] None of these policies involve third party oversight, however, and given ICE's well documented history of ignoring legal limits on its powers, and of evading attempts by Congress and other agencies to scrutinize its activities, unspecified internal security policies and procedures are not sufficient to satisfy the country's obligations under the treaty.

Furthermore, given the serious invasion of privacy caused by ICE's data practices described above, Article 17(2) requires, at a minimum: (i) a prior approval by an independent, competent, and well-resourced judicial body, not administrative warrant and subpoena, at least for the collection of social media account information or other sensitive information; (ii) ex-post auditing of data collection and use; and (iii) public disclosure of the aggregate information on the specific number of requests approved and rejected, a disaggregated number on the requests by each data source, and number of individuals affected by each.[104] None of which are currently in place.

Reports by civil society organizations and the media indicate that ICE has a "culture of abuse and unchecked power" with respect to its authority to access and use personal information.[105] For example, according to a report by WIRED based on documents obtained through a freedom of information request, ICE initiated at least 414 internal investigations into the misuse of databases since 2016 and nearly half of those cases have been regarded as serious misconduct, including those criminal, and further escalated to ICE's Office of Professional Relations. Two dozen investigations were categorized criminal and in at least 14 incidents, ICE employees were investigated for allegedly using agency databases to harass someone or make threats or disclose retrieved data, including videos of detainees. In serious cases, ICE employees were investigated for the allegation of "online solicitation of an intellectually disabled adult" and stealing immigrants' identities in an attempt to defraud credit card companies. What is further striking is that much of the misconduct that internal investigators flagged involves employees looking up information about themselves—so-called self-queries. Importantly, these abuses were discovered by ICE's *internal* investigations, which are most certainly self-serving in most cases. This raises the question of how many more abuses would be discovered by an investigation by an independent, competent body with adequate resources. An expert articulated "[ICE is] always pushing to the limits of what they are allowed to do and fudging around the edges without oversight".[106]

---

[103] PIA for EID, pages 15-16.
[104] *See* Human Rights Committee, supra note 89, para. 8; Concluding Observation on the United States of America, CCPR/C/USA/CO/4 (23 April 2014), para. 22; OHCHR, supra note 90, paras. 28-30; and the Electronic Frontier Foundation and a coalition of NGOs, *supra* note 95.
[105] WIRED, *ICE Records Reveal How Agents Abuse Access to Secret Data* (17 April 2023).
[106] *Id.*

Safeguards are even weaker in contexts where ICE is attempting to access data outside its own purchased databases and networks. There is considerable evidence that ICE has been abusing its subpoena power. For example, ICE sent administrative warrants to abortion clinics although custom summons are meant to be used only in criminal investigations about illegal imports or unpaid customs duties, which strongly indicates the abuse of administrative warrants.[107]

4. ICE's practice of data collection and use violates Article 19(2)(3), 21, 22

4.1 Chilling effect caused by the ICE's data practice

ICE data practices and the surveillance they fuel deters people who fear the detention or deportation of themselves or their loved ones from engaging in a wide range of activities that are (1) necessary for their survival and (2) protected under international human rights law. For example, ICE's access to the billing information of utility companies may make people reluctant to access the essential services provided by utility companies. The data brokers that sell information to ICE in fact market their utility data sets as including information on people who are otherwise hard to find, because they typically avoid interacting with entities that keep digital records (like banks). Since ICE is not transparent about its data practices, the chilling effect may extend far beyond the contexts where ICE is known to be collecting data. Immigrant families that are aware of ICE surveillance, but uncertain of its scope, may be generally dissuaded from taking any actions that could lead to enforcement if data were shared with ICE, even the access to legal and medical services.[108] Such impacts could in some cases constitute a violation of other rights, such as the right to life (ICCPR Article 6) and the right to a fair trial (ICCPR Article 14(1)).

The impact on the freedom of expression, peaceful assembly, and of association is also particularly severe. Article 19(2) protects the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers [...]". Among those expressions protected under Article 19(2), the right to peaceful assembly, meaning "the non-violent gathering by persons for specific purposes, principally expressive ones", is protected under Article 21, and the right to freedom of association is protected under Article 22(1). These rights are equally guaranteed to all individuals including non-citizens, regardless of documented or undocumented, and a state is obliged to protect the rights of individuals who may be within a state's territory or anyone within its power or effective control.[109] Out of the fear that any online or offline actions are being watched by ICE, immigrants and U.S. citizens who have a close tie with them would refrain from seeking information, expressing themselves online and offline, organizing or participating in peaceful protests or association on its real names or anonymously, being restricting those rights.

4.2 ICE's practices put the U.S. in violation of Articles 19(2)(3), 21, and 22

These articles require states to have "clear and publicly available guidelines to ensure that the collection of information of individuals who exercise freedom of expression does not have a chilling effect on part".[110] The collection of data related to individuals' expressions must be subject to independent and transparent

[107] *See* WIRED, *supra* note 53.
[108] *See* American Dragnet, pages 61-64.
[109] ICCPR, *supra* note 13, article 2, para. 1; and Human Rights Committee, *supra* note 13, para.10.
[110] Human Rights Committee, *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*, CCPR/C/GC/37 (17 September 2020), para 94.

scrutiny and oversight.[111] As we see in detail above, ICE has been failing to meet these requirements, violating these Articles.

Suggested questions to be asked to the United States

- What mechanism, if any, does the United States have for ensuring that ICE's immigration enforcement operations generally, and in particular with respect to data surveillance, comply with ICCPR?
- How and when will the United States investigate ICE's data practices, hold the relevant actors accountable, provide meaningful remedies to people affected, and ensure non-repetition?

Suggested recommendations to be included in the Concluding Observations

- Congress should immediately review each component of of ICE's data cycle, and issue a public report analyzing the question of whether each of these components, as well as ICE's data practices taken together, comply with the country's obligations under including data ICCPR;
- The executive branch should terminate or remediate ICE's practices which do not comply with ICCPR;
- The executive branch should issue formal policies and regular oversight mechanisms to prevent the recurrence of data practices that would not comply with ICCPR;
- Congress should investigate all the alleged abuses, as well as civil and human rights violations, that have resulted from ICE's data practice, and provide avenues by which all people who have been affected can pursue effective remedies; and
- Congress should establish federal-level privacy protection laws which satisfy the requirements of Article 17 of ICCPR.

Thank you very much for your consideration. If you have any questions on this submission, please contact Emily Tucker (et599@georgetown.edu) at the Center on Privacy & Technology at Georgetown Law and Hinako Sugiyama (hsugiyama@law.uci.edu) at the International Justice Clinic, the University of California, Irvine School of Law.

[111] *Id.*, para 62.