



**JUST  
FUTURES  
LAW**

---

**COMMENTS ON:**

**NOTICE OF PROPOSED RULEMAKING: U.S. CITIZENSHIP AND IMMIGRATION SERVICES,  
DEPARTMENT OF HOMELAND SECURITY: COLLECTION AND USE OF BIOMETRICS BY U.S.  
CITIZENSHIP AND IMMIGRATION SERVICES, CIS NO. 2644-19**

**Docket Number: DOCKET NO. USCIS-2019-0007**

**SUBMITTED BY THE NATIONAL IMMIGRATION LAW CENTER AND JUST FUTURES LAW**

The National Immigration Law Center (NILC) and Just Futures Law (JFL) submit the following comments on the Notice of Proposed Rulemaking: U.S. Citizenship and Immigration Services, Department of Homeland Security: Collection and Use of Biometrics by U.S. Citizenship and Immigration Services.<sup>1</sup>

Established in 1979, the National Immigration Law Center (NILC) is one of the leading organizations in the U.S. exclusively dedicated to defending and advancing the rights and opportunities of low-income immigrants and their families. We focus on issues that affect the well-being and economic security of immigrant families, including access to health care and safety net programs; education and training; workers' rights; immigration enforcement and privacy; and other federal and state policies related to immigrants.

Just Futures Law (JFL) is a transformational immigration lawyering project that works to support the immigrant rights movement in partnership with grassroots organizations. JFL staff have decades of experience in providing technical assistance, written legal resources, and training for attorneys, advocates, and community groups in various areas of immigration law.

NILC and Just Futures Law oppose biometrics collection and use authorized by the Notice of Proposed Rulemaking (NPRM). NILC and JFL also object to the 30-day deadline to submit comments. This is an extraordinarily insufficient time to comment on a complex proposed rule, whose justification required several hundred pages.

**WHAT DOES THE NPRM AUTHORIZE?**

The NPRM authorizes:

---

<sup>1</sup> Notice of proposed rulemaking, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (Sept. 11, 2020), <https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf>

- A sweeping redefinition of the terms “biometrics” to include a vast range of physical and personal characteristics, including fingerprints, palm prints, photographs (including “facial images specifically for facial recognition, as well as photographs of physical or anatomical features such as scars, skin marks, and tattoos”), signature, voice print; iris image; and DNA;
- Dramatically expanding when and from whom these physical characteristics are collected, retained and used, by requiring biometrics collection for “any applicants, petitioner, sponsor, beneficiary, or individual filing or associated or associated with a certain benefit” including U.S. citizens and Lawful Permanent Residents (LPRs);
- Expanding biometrics collection as an enforcement tool by expanding the “purposes for which biometrics are collected from individuals filing immigration applications or petitions, to include criminal history and national security background checks; identity enrollment, verification, and management; secure document production, and to administer and enforce immigration and naturalization laws;”
- Expanding the authority of DHS to use and re-use biometrics and to share them with federal, state, and local law enforcement, intelligence community entities, and foreign governments;
- Making biometrics collection the routine, default procedure unless waived by DHS;
- Allowing collection of biometrics from babies and toddlers by expanding biometrics collection to include children under age 14;
- “Continuous immigration vetting” allowing biometrics collection from non-citizens who have been granted immigration benefits until they become U.S. citizens;
- Requiring DNA collection to prove family relationships even where documentary evidence such as birth certificates and medical and school records is available;
- Making self-petitioners in the U.S., including children, under the Violence Against Women Act (VAWA) subject to the biometrics requirement and extending the period of “good moral character” beyond a 3-year period before filing;
- Making T non-immigrant adjustment of status applicants, including children, subject to the biometrics requirement and extending the period of “good moral character” beyond a 3-year period before filing and eliminating a presumption of good moral character for children;
- Collection of biometrics on U.S. citizens and LPRs at regional centers;
- Charging an \$85 biometrics fee for each individual, including children, to be incorporated into the fees for the underlying benefits, unless a fee waiver is granted.

## **WHAT’S WRONG WITH THE PROPOSED CHANGES**

- **The NPRM is part of DHS’ under-the-radar creation of a giant “person centric” database called Homeland Advanced Recognition Technology (HART) that will include physical characteristics, biographic and encounter information, and other personal information about millions of citizens and non-citizens.**

The NPRM's biometrics collection is part of DHS' under-the-radar creation of a vast database called Homeland Advanced Recognition Technology (HART),<sup>2</sup> which will replace DHS' current biometrics database IDENT<sup>3</sup> in FY2020.<sup>4</sup> HART will centralize access to federal and international databases, provide real-time access in the field, and involve the use of "multi-modal biometrics" (e.g., the wide range of physical characteristics that the NPRM authorizes).<sup>5</sup>

Creation of this enormous database is central to DHS' strategy of biometric collection and tracking of noncitizens. But it warrants only a footnote in the NPRM, which instead refers only to the more limited biometric database called IDENT (Automated Biometric Identification System) (ft. 21, "IDENT will be replaced by a system called the Homeland Advanced Recognition Technology (HART). DHS will use the term "IDENT" in this rule to refer to both the current and successor systems").

In 2016 DHS disclosed the creation of HART<sup>6</sup> with little fanfare and no overall picture of the immensity of its future operations, which extend well beyond biometrics. Instead, DHS has used piecemeal System of Records Notices (SORNs) to surreptitiously build HART's enormous capabilities. For example, the 2017 External Biometric Records (EBR) System of Records Notice makes clear that HART won't include only biometrics and associated biographic information. It will also include identifiers for derogatory information, miscellaneous officer comment information, and encounter data.<sup>7</sup> These items are undefined and unlimited in scope. HART, through EBR, will also include "records related to the analysis of relationship patterns among individuals and organizations." Likewise, the 2020 Department of Homeland Security/All-043 Enterprise Biometric Administrative Records (EBAR) System of Records (SOR) Notice offers only a vague description of EBAR 's role in HART to allow "DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic."<sup>8</sup>

---

<sup>2</sup> Supplemental Programmatic Environmental Assessment (SPEA) for the Proposed Establishment and Operations of the Office of Biometric Identity Management and the Homeland Advanced Biometric Technology (HART), 81 Fed. Reg. 90862 (Dec. 15, 2016), <https://www.govinfo.gov/content/pkg/FR-2016-12-15/pdf/2016-30187.pdf>

<sup>3</sup> Notice of Updated Privacy Act System of Records Notice, IDENT System of Records (DHS, June 5, 2007) <https://www.govinfo.gov/content/pkg/FR-2007-06-05/html/07-2781.htm>

<sup>4</sup> "DHS is the big winner in DHS's FY 2020 funding budget for biometrics," (Anthony Kimery, Biometric Update January 21, 2020), <https://www.biometricupdate.com/202001/obim-is-the-big-winner-in-dhss-fy-2020-funding-budget-for-biometrics>

<sup>5</sup> Homeland Security releases biometric framework (Zack Martin, Secure ID News, Aug. 31, 2015) <https://www.secureidnews.com/news-item/homeland-security-releases-biometric-framework/>

<sup>6</sup> Supplemental Programmatic Environmental Assessment (SPEA) for the Proposed Establishment and Operations of the Office of Biometric Identity Management and the Homeland Advanced Biometric Technology (HART), 81 Fed. Reg. 90862 (Dec. 15, 2016), <https://www.govinfo.gov/content/pkg/FR-2016-12-15/pdf/2016-30187.pdf>

<sup>7</sup> Notice of a new system of records, Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records (April 24, 2018), <https://www.govinfo.gov/content/pkg/FR-2018-04-24/pdf/2018-08453.pdf>

<sup>8</sup> Notice of a new system of records, Department of Homeland Security/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records (SOR) (March 16, 2020), <https://www.govinfo.gov/content/pkg/FR-2020-03-16/pdf/2020-04979.pdf>

DHS has consistently exempted these components of HART from critical elements of the Privacy Act pertaining to accuracy, relevance, completeness, timeliness, notice, disclosure, ability to correct incorrect information, and more.

As a result, redress and remedies for improper collection and dissemination of information are virtually nonexistent.

HART, like IDENT, will be housed in and managed by DHS' Office of Biometric Identity Management (OBIM). According to the NPRM at ft. 29, OBIM is "the lead designated provider of biometric identity services for DHS, and maintains the largest biometric repository in the U.S. government."

But the proposed regulation masks the critical role that OBIM will play in hosting, managing, storing and/or analyzing information in HART for ICE and CBP. OBIM, a component at the DHS Directorate level, sets rules for data sharing amongst agencies. A recipient of increasing Congressional funds, little is known about it even though it plays a central role in biometric services and identity management.<sup>9</sup>

DHS contracted with Northrop Grumman<sup>10</sup> to develop HART, but little public information is available. The proposed rule expands the authority of DHS to use and re-use biometrics and to share them with federal, state, and local law enforcement, intelligence community entities, and foreign governments. HART will permit this unfettered information sharing without guidelines, accountability or redress.

Only a 2020 HART Privacy Impact Assessment (PIA) attempts to describe HART and privacy implications.<sup>11</sup> But no legal commitments underlie the claims about how HART will operate, which are based simply on DHS' current assertions. Moreover, the PIA focuses only on fingerprints, facial recognition and iris matching, and does not address the full range of biometrics that the NPRM contemplates.

- **The NPRM will outsource this massive biometric collection enterprise within DHS to the data collection and data broker market.**

HART will not limit the data collected to what is available from government entities. According to the PIA, "HART may use information from publicly available sources, collected according to the data provider's authority. Specific publicly available sources are discussed in more detail in

---

<sup>9</sup> "Information Paper, OBIM," February 2020, [https://events.afcea.org/FedID20/CUSTOM/pdf/DHS\\_OBIM\\_0220\\_InfoPaper\\_OBIM\\_Overview\\_Final.pdf](https://events.afcea.org/FedID20/CUSTOM/pdf/DHS_OBIM_0220_InfoPaper_OBIM_Overview_Final.pdf)

<sup>10</sup> Legacy Systems Held DHS' Biometrics Programs Back. Not Anymore (Jack Corrigan, Nextgov, Oct. 3, 2019), <https://www.nextgov.com/it-modernization/2019/10/legacy-systems-held-dhs-biometrics-programs-back-not-anymore/160347/>

<sup>11</sup> Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA DHS/OBIM/PIA-004 (Feb. 24, 2020), [https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf)

the appropriate data provider’s privacy compliance documentation.”<sup>12</sup> But the PIA itself provides no meaningful information about the role that information from commercial entities will play in HART.

Multiple articles demonstrate that DHS has become one of the largest consumers of biometric technology, second only to the Department of Defense. The brief reference in the Hart PIA opens a whole world of acquisition of biometrics from unregulated commercial entities, such as technology corporations or data brokers. These commercial entities have become a vital source of data for immigration enforcement.<sup>13</sup> Companies with a strong record of unfettered biometric collection, data sharing and analytics continue to build and host systems for ICE, yet little is known about their contracts or their use, collection, and third party sharing of data with other federal, local, state agencies or other companies.<sup>14</sup>

For example, DHS recently requisitioned biometrics analytics and services from Clearview AI, a company that has collected facial scans by scraping social media.<sup>15</sup> Clearview AI’s Board of Directors is known to have misused Clearview AI for personal interests.<sup>16</sup> Palantir, a company that went public off government contracts with ICE, has been characterized as being “high risk” for committing human rights violations.<sup>17</sup> A powerful and intrusive DHS case management software called Integrated Case Management (ICM) is being developed by Palantir. This software is designed to handle biometric meta-data.

The Trump administration is engaging in open warfare<sup>18</sup> against states and localities (“sanctuary cities”) that have imposed legal restrictions on sharing personal information that would diminish the privacy rights of immigrants and citizens and that can be used for immigration enforcement. Reliance on private companies that sweep up personal information, including biometrics, and sell it to the federal government is part of the government’s strategy to circumvent the legal restrictions that these states and localities have imposed.

---

<sup>12</sup> Id. at 18.

<sup>13</sup> Who’s Behind ICE: the Tech and Data Companies Fueling Deportations (Mijente, the National Immigration Project, and the Immigrant Defense Project), [https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE\\_-The-Tech-and-Data-Companies-Fueling-Deportations\\_v1.pdf](https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v1.pdf)

<sup>14</sup> Immigrant Rights Groups, Law School and Legal Organization FOIA for Info on Thomson Reuters, RELX Group Contracts with ICE (Center for Constitutional Rights, Sept. 14, 2020), <https://ccrjustice.org/home/press-center/press-releases/immigrant-rights-groups-law-school-and-legal-organization-foia-info>

<sup>15</sup> ICE just signed a contract with facial recognition company Clearview AI, (Kim Lyons, The Verge, August 14, 2020); <https://www.msn.com/en-us/news/technology/ice-just-signed-a-contract-with-facial-recognition-company-clearview-ai/ar-BB17Yb4B>.

<sup>16</sup> Controversial Clearview AI raises 8 million, (BuzzFeed News, September 24, 2020), <https://www.buzzfeednews.com/article/ryanmac/controversial-clearview-ai-raises-8-million>

<sup>17</sup> Palantir’s ICE Contracts ‘Raise Human Rights Concerns’, Report Warns as Firm Prepares To Go Public, (Chantal da Silva, Forbes, 9/28/2020). <https://www.forbes.com/sites/chantaldasilva/2020/09/28/palantirs-ice-contracts-raise-human-rights-concerns-report-warns-as-firm-prepares-to-go-public/#2cca01d73792>;

<sup>18</sup> William Barr unveils ‘significant escalation’ of Trump administration battle against ‘sanctuary city’ policies, (AP, Feb. 10, 2020), <https://www.marketwatch.com/story/william-barr-unveils-significant-escalation-of-trump-administration-battle-against-sanctuary-city-polices-2020-02-10>

Although the structure of HART explicitly includes acquisition of biometrics from commercial entities, the biometrics NPRM itself does not even mention the subject.

- **The NPRM authorizes baby-to-grave surveillance of immigrants and citizens**

HART, supported by the biometrics collection, retention and use is a critical element of a larger program of continuous surveillance of immigrants that DHS initially called “extreme vetting” and later dubbed as Visa Lifecycle Vetting.<sup>19</sup> As DHS wrote in 2017 as part of an event to discuss future contracts for vetting of non-citizens, “the gaps in the current vetting model along with existing limitations in the vetting process create a compelling case for ICE to take action to develop and implement a continuous vetting strategy, framework and process.”<sup>20</sup> Other DHS notices have made clear that the monitoring and surveillance will continue even when noncitizens become citizens.<sup>21</sup>

The NPRM explicitly authorizes collection, retention and use of biometrics for vetting during the “immigration lifecycle.” That includes:

- Dramatically expanding when and from whom these physical characteristics are collected, retained and used, by requiring biometrics collection for “any applicants, petitioner, sponsor, beneficiary, or individual filing or associated with an immigration certain benefit.”
- Applying those requirements not only to immigrant beneficiaries but also to citizens and Lawful Permanent Residents (LPRs) petitioners, sponsors or the remarkably unclear persons “associated with an immigration benefit.”
- Eliminating age limitations so that even babies, toddlers and children are subject to the requirements.
- Authorizing biometrics collection even after a non-citizen obtains status: “This rule proposes that any individual alien who is present in the United States following an approved immigration benefit may be required to submit biometrics unless and until they are granted U.S. citizenship.”<sup>22</sup>

Biometrics collection under the above circumstances is the rule, not the exception. It applies unless DHS waives the collection. But no standards or criteria exist for a waiver. And there is no review of how DHS exercises its waiver authority.

---

<sup>19</sup> ICE Rebrands Its AI-Enhanced 'Extreme Vetting' Plan as 'Visa Lifecycle Vetting' (Bryan Menegus, Gizmodo, Nov. 22, 2017) <https://gizmodo.com/ice-rebrands-its-ai-enhanced-extreme-vetting-plan-as-vi-1820686047>

<sup>20</sup> Information Vacuuming: The Trump Administration Is Collecting Massive Amounts of Data for Its Immigrant Surveillance and Deportation Machine , (National Immigration Law Center, Aug. 22, 2018), <https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/>

<sup>21</sup> DHS Is Collecting Information on Immigrants’ and Citizens’ Social Media Use and Making It Part of Their Permanent Records, (National Immigration Law Center, Nov. 30, 2017), <https://www.nilc.org/news/the-torch/11-30-17/>

<sup>22</sup> <https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf>, p. 56352.

Once collected, the biometrics are available for all surveillance purposes. As the NPRM states, “DHS proposes to further clarify the purposes for which biometrics are collected from individuals filing immigration applications or petitions, to include criminal history and national security background checks; identity enrollment, verification, and management; secure document production, and to administer and enforce immigration and naturalization laws.”

DHS justifies its sweeping surveillance program with specious arguments, claiming the need for immigrants to continuously prove identity or making vague claims about promoting national security or protecting children. The underlying sentiment, however, is that immigrants and citizens who act on their behalf create an ongoing criminal and national security threat to the country.

Expanding the authority to collect, retain and use biometrics is not benign, despite DHS’ claim that it is necessary for establishing proof of identity or other law enforcement reasons. DHS has already accumulated a deeply troubling track record of pernicious and retaliatory surveillance against activists. See *NWDC Resistance v. ICE* (U.S.D.C., W. Dist. WA, Case No. 3:18-cv-05860-RBL) for evidence of surveillance activities and retaliatory actions taken by DHS.<sup>23</sup> The complaint details several incidents and/or lawsuits brought against DHS component agencies for retaliatory actions and surveillance. Biometrics collection enhances the harmful, lifelong impacts of DHS misconduct.

The NPRM specifically mentions use of facial recognition technology, as well as DHS’ use of mobile devices in the field to collect biometrics. Facial recognition “frequently is an inaccurate and unreliable biometric identifier,” often misidentifying people of color and women and relying on photographs collected in a discriminatory criminal justice and immigration databases.<sup>24</sup> And use of mobile devices means that DHS agencies will be able to collect fingerprints, photographs and perhaps more in unregulated “encounters” where abuse is harder to monitor. As the Electronic Frontier Foundation has reported about HART:

The records DHS plans to include in HART will chill and deter people from exercising their First Amendment protected rights to speak, assemble, and associate. Data like face recognition makes it possible to identify and track people in real time, including at lawful political protests and other gatherings. Other data DHS is planning to collect—including information about people’s “relationship patterns” and from officer “encounters” with the public—can be used to identify political affiliations, religious activities, and familial and friendly relationships. These data points are also frequently colored by conjecture and bias.<sup>25</sup>

---

<sup>23</sup> *NWDC Resistance v. ICE* (U.S.D.C., W. Dist. WA, Case No. 3:18-cv-05860-RB), <https://justfutureslaw.org/wp-content/uploads/2020/03/2020.12.20.NWDCvICE.amended.complaint.pdf>

<sup>24</sup> HART: Homeland Security’s Massive New Database Will Include Face Recognition, DNA, and Peoples’ “Non-Obvious Relationships” (Jennifer Lynch, Electronic frontier Foundation, June 7, 2018), <https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and>

<sup>25</sup> *Id.*

- **The biometrics expansion is part of a Trump administration campaign to discourage legal immigration**
  - **DHS has eviscerated the availability of fee waivers while proposing dramatic fee increases.**

The NPRM misrepresents the availability of fee waivers, suggesting instead that fee waivers are widely available. Unmentioned in the NPRM, the Trump administration has increased fees for immigration applications dramatically, set to begin on October 2, 2020.<sup>26</sup> For example, the fee for a naturalization application increased 80% to more than \$1,100. Even children have to pay the fee. Applications that never charged a fee now will charge one. Even asylum seekers who are fleeing for their lives will be required to pay a \$50 filing fee.

At the same time, the administration has tried to eliminate fee waivers for many applications, including citizenship, unless the Immigration and Nationality Act requires that one be available. This barrier would leave most immigration processes ineligible for a fee waiver. DHS has likewise made it much more difficult for applicants to qualify for a waiver by eliminating receipt of a means-tested benefit as a basis for a waiver and by imposing burdensome documentation requirements.

On September 30, 2020, a federal judge issued a preliminary injunction blocking the fee increases and fee waiver elimination.<sup>27</sup> The judge ruled that DHS officials acted illegally. But the final outcome of the litigation is unknown, while the administration's intent to use fees to create barriers to obtaining legal status is clear.

- **The NPRM will make it more difficult for survivors of abuse and trafficking to obtain legal status.**

The NPRM makes self-petitioners in the U.S., including children, under the Violence Against Women Act (VAWA) subject to the NPRM's biometrics expansion and extends the period for establishing "good moral character" beyond a 3-year period before filing. It also makes T (trafficking) adjustment of status applicants, including children, subject to the biometrics requirement, extends the period of "good moral character" beyond a 3-year period before filing and eliminates a presumption of good moral character for children.

The addition of standardless, subjective requirements gives DHS expanded leeway to deny the applications. In addition, these requirements create unnecessary administrative barriers and costs that will impede the ability of survivors to obtain permanent status in the U.S.

---

<sup>26</sup> USCIS Fee Increases Effective October 2, 2020 (Victor Valdez Gonzalez, Immigrant Legal Resource Center, Aug. 2020), [https://www.ilrc.org/sites/default/files/resources/revised\\_uscis\\_fee\\_increases\\_october\\_2020.pdf](https://www.ilrc.org/sites/default/files/resources/revised_uscis_fee_increases_october_2020.pdf)

<sup>27</sup> Immigrant Legal Resource Center v. Wolf, Case No. 4:20-cv-05883 (N.D. Cal., order issued Sept. 29, 2020); Federal Judge Enjoins DHS' Illegal and Immoral Immigration Fee Increase (CLINIC, Sept. 30, 2020), <https://cliniclegal.org/press-releases/federal-judge-enjoins-dhs-illegal-and-immoral-immigration-fee-increase>



- **The NPRM’s authorization for DHS to require, request, or accept DNA evidence to demonstrate the existence of a claimed genetic relationship reflects racial animus.**

The proposed rule authorizes DHS to require, request, or accept DNA evidence to demonstrate the existence of a claimed genetic relationship, though it claims that only DNA results and not the raw DNA will be made part of an individual’s immigration record. The rule suggests no standards regarding when a requirement or request is appropriate and does not provide for any review of how DHS has implemented this authority.

DHS thus would have wide authority to require DNA testing, even where significant documentary evidence, such as birth certificates or medical or school records is available. Obtaining DNA testing is not a benign exercise, particularly for applicants or beneficiaries who live outside of the U.S., where testing would require travel or is prohibitively expensive.

DHS already has placed multiple roadblocks in the path of obtaining legal status. As outlined by the Migration Policy Institute, the Trump administration has accomplished this through regulatory, policy and programmatic measures, not by seeking Congressional action.<sup>28</sup> These changes are motivated by racial animus, as reflected in the president’s own characterization of Mexican immigrants<sup>29</sup> as rapists and drug dealers, his condemnation of immigrants from “shithole countries,”<sup>30</sup> a ban on Muslim immigrants,<sup>31</sup> his efforts to add a citizenship question to the census,<sup>32</sup> and more.

## **CONCLUSION**

The NPRM is evidence of DHS’ plan to establish and expand extensive data mining and surveillance against immigrants and citizens alike. It is deeply troubling that DHS remains so opposed to transparency, accountability, redress and the protection of privacy. The NPRM should be withdrawn.

---

<sup>28</sup> Dismantling and Reconstructing the U.S. Immigration System: A Catalog of Changes under the Trump Presidency (Sarah Pierce and Jessica Bolter, Migration Policy Institute, July 2020),

<https://www.migrationpolicy.org/research/us-immigration-system-changes-trump-presidency>

<sup>29</sup> Trump basically called Mexicans rapists again (Z. Byron Wolf, CNN, Apr. 6, 2020),

<https://www.cnn.com/2018/04/06/politics/trump-mexico-rapists/index.html>

<sup>30</sup> How the world is reacting to Trump’s use of s\*\*\*hole, (PBS, Jan. 12, 2018),

<https://www.pbs.org/newshour/world/how-the-world-is-reacting-to-trumps-use-of-shole>

<sup>31</sup> Understanding Trump’s Muslim Bans (No Muslim Ban Ever, March 8, 2019),

<https://www.nilc.org/issues/immigration-enforcement/understanding-the-muslim-bans/>

<sup>32</sup> Trump’s racist comments can be used against him in court as judges cite them to block policies, (Fred Barbash, Washington Post, July 16, 2019), [https://www.washingtonpost.com/national-security/trumps-racist-comments-can-be-used-against-him-in-court-as-judges-cite-them-to-block-policies/2019/07/16/6ed0ea6a-a7f1-11e9-86dd-d7f0e60391e9\\_story.html](https://www.washingtonpost.com/national-security/trumps-racist-comments-can-be-used-against-him-in-court-as-judges-cite-them-to-block-policies/2019/07/16/6ed0ea6a-a7f1-11e9-86dd-d7f0e60391e9_story.html)