OPEN SOCIETY
JUSTICE INITIATIVE

imumi
Instituto para las Mujeres en la Migración A.C.

Comments of the Open Society Justice Initiative and Instituto para las Mujeres en la Migración

RIN 1105-AB56 Proposed Rule, DNA-Sample Collection from Immigration Detainees

November 12, 2019

The Open Society Justice Initiative (OSJI) and Instituto para las Mujeres en la Migración (IMUMI) welcome the opportunity to comment on the Department of Justice's (DOJ's) proposed rule for collecting DNA samples from immigration detainees.

OSJI is an international NGO and arm of the Open Society Foundations. It works to document human rights violations, propose and pilot solutions, engage policymakers and offer expertise that draws on its extensive global legal experience, including efforts to extend access to justice for all.

IMUMI is a Mexican NGO that advocates for women migrants and their families within the region of Mexico, the U.S., and Central America. IMUMI addresses issues important to migrant women and transnational families through legal strategies, research, communication, and policy reform.

We write to express our concern regarding the proposed rule, which abruptly removes protections for non-U.S. persons detained by the Department of Homeland Security (DHS) with respect to the collection, testing and storage of DNA samples.[1] We wish to draw attention to the experiences of other countries, in which the negative effects of DNA sampling are already observed: data breaches revealing highly sensitive personal information, faulty privacy protections leading to public backlash and litigation, and the use of DNA profiles in furtherance of persecution. Indeed, other countries have limited the collection of DNA altogether in non-criminal contexts, due to the many risks associated with its collection and the limited additional value that large-scale collection of DNA would add to the legitimate exercise of relevant government functions. OSJI and IMUMI urge DOJ to reconsider this broad grant of authority on DNA collection in light of these issues, as well as the procedural irregularities and risks associated with the proposed rule.

1. THE AGENCY HAS NOT ENGAGED IN SUFFICIENT CONSULTATION

The proposed rule will affect the lives of millions of alleged non-U.S. nationals,[2] their families, as well as distant relatives, many of whom will likely be U.S. citizens.[3] The rule change is also likely to have knock-on effects on existing and future administration of the Combined DNA Index System (CODIS) database, a

[1] RIN 1105-AB56, 3-4.
[2] RIN 1105-AB56, 13 (estimating an additional 748,000 samples will be collected annually if the proposed rule is implemented and sampling begins as envisioned).
[3] *See, e.g.*, Scott Simon, *Privacy and DNA Tests*, National Public Radio, November 9, 2019 (interview with New York University law professor Erin Murphy, noting that, for example, "[i]f 3 million people of European descent offer their genetic information to a database, you have essentially a universal genetic database for the American population of European descent.").

Federal Bureau of Investigation (FBI) program used by law enforcement to link known criminals to crimes. It is therefore of vital importance that the rulemaking not be a rushed process and that any change to DNA collection and profiling is adequately assessed and scrutinized. The Attorney General's explanation for this rule change falls below that standard.

In particular, the agency has not engaged in adequate consultation in the development of the proposed rule, and it likewise has fixed an excessively short comment period given the complex nature of the proposed rule change and its far-reaching impact.

a. Lack of Appropriate Consultation in the Development of the Proposed Rule

The limited consultation leading to the proposed rule undermines what should be a rigorous assessment process in light of the practical consequences of the proposed change for government at all levels, as well as individuals and their families.

The proposed rule should undergo a risk assessment and consultation process commensurate with the complexities associated with its implementation, including a federalism assessment, ensuring that its implementation will adhere to a tailored, strict legal and policy framework, reflecting the outcomes of such a process. The justifications presented by the Attorney General reflect inadequate effort to understand the full ramifications of collecting DNA samples from close to one million people annually, nor do they contain information concerning the security, design and capacity of the CODIS database, taking into account the decades of innovation and design thinking that have transpired since its establishment.

Lack of appropriate risk assessment and consultation in the design and implementation of new initiatives involving sensitive personal data and utilization of emerging technologies can derail projects entirely, wasting limited public resources unnecessarily. As discussed further below, emerging biometric technologies, in particular wide-scale DNA profile collection and retention, bring with them a range of acute risks to privacy, data protection and equal protection the scale and scope of which have yet to be adequately assessed. Strong legal and policy frameworks based on expert consultation will need to be in place in order to mitigate these substantial risks. The absence or infirmity of such frameworks contributes to data breaches and misuse of data by state and non-state actors.

Critically, the rule justification states that the regulation "will not have substantial effect on the States, on the relationship between the national Government and the States, or on the distribution of power and responsibilities among the various levels of government" and therefore does not warrant a federalism assessment. Yet, CODIS enables federal, state and local forensic laboratories to exchange and compare DNA profiles electronically.[4] The use of CODIS at the state level is governed by state law and some functions, such as familial searching, are conducted and regulated only at the state level. Thus, legislation around the protection and sharing of data at the state level is highly relevant to this rule.

The cursory justification and consultation process behind this proposed rule change invite legal challenges to the constitutionality of the rule itself and the underlying CODIS database. State and local governments have important interests in the design and eventual implementation of a rule expanding the federal government's mandate to collect DNA profiles in non-criminal contexts.

International experience shows that the failure to adequately consult and perform appropriate risk assessments prior to the introduction of such rules may provoke legal challenges. For examples, in Kenya, a law on biometric data collection (including DNA) for a proposed digital identification system (the

[4] *See CODIS: Discussion Topics for States Considering Familial Searching*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis.

National Integrated Identity Management System, NIIMS) was challenged in February 2019, based in part on the lack of consultation with county governments and the Senate, which is the legislative body that represents county level interests. There, petitioners argued that the new law affects "many areas of both national and county governments' competencies, including the provision of services such as health, education, housing, etcetera," which would relate directly to administrative issues on the county level.[5] In addition to the litigation it has sparked, the parliamentary process has also been openly challenged by Kenya's Senate, which formally protested the failure to engage in bicameral lawmaking calling for a halt to the NIIMS enrolment process.[6]

DNA collection pursuant to the proposed rule change would relate directly to criminal justice and collateral family law and other non-criminal decisions taken at the state or local level and should accordingly benefit from a thorough federalism assessment.

b. Failure to Consider Existing Vulnerabilities in the Combined DNA Index System (CODIS)

The proposed rule brings to the forefront some of the systematic problems underlying CODIS, which would be heightened and intensified through DNA collection from detained immigrants in DHS custody. These foreseeable consequences of the expansion of CODIS envisioned in the proposed rule should have been considered extensively in the rulemaking process, but they do not figure in the Attorney General's justification.

The Federal Bureau of Investigation cites, for example, the need to "re-architect" CODIS's software in connection with the rapid increase in accumulation of biometric data including DNA to date, as well as the need to build a legal framework, in consultation with state and local agencies, to govern familiar searching based on DNA profiles contained in CODIS.[7] The expansion to cover immigration detainees may necessitate the collection of more detailed DNA profiles than presently collected, in order to successfully deduplicate records and perform forensic analysis.[8]

The proposed rule's background and reasoning states that DNA analysis "provides a powerful tool for human identification"[9] and that "DNA identification informs the decision concerning continued detention or release."[10] Yet, it is known that there are flaws with existing biometric records and databases and that reliance on them risks causing miscarriages of justice.

Wide-scale inclusion of DNA information from non-US person DNA within the CODIS database may also create privacy and constitutional concerns for their U.S. citizen relatives, who may be matched (correctly or erroneously) to the profiles collected by DHS. In this regard, even DNA evidence is not foolproof and erroneous matches can occur, as "DNA profiles are often not clean enough to conclusively identify an

---

[5] Nairobi High Court, *Nubian Rights Forum et al. v. The Honourable Attorney General et al.*, Petition No. 56 of 2019, at 22 (2019).
[6] *See, e.g.*, Laban Wanambisi, *Stand-off Between Senate and Interior Ministry over NIIMS Project*, allAfrica, February 28, 2019, https://allafrica.com/stories/201903010100.html.
[7] *See* CODIS, *Overview: The Future*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis.
[8] *See* CODIS, *Planned Process and Timeline for Implementation of Additional CODIS Core Loci*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis; *see also* Douglas R. Hares, *Expanding the CODIS core loci in the United States*, Forensic Sci. Int. Genet. 6 (2012) (describing the Scientific Working Group on DNA Analysis Method's determination that "reduc[ing] the likelihood of adventitious matches as the number of profiles stored in [the National DNA Index System] continues to increase each year" was a major reason for "expanding the CODIS core loci").
[9] RIN 1105-AB56, 7 (citing 73 F.R. at 74933).
[10] RIN 1105-AB56, 9.

individual," particularly where physical evidence at a crime scene has been damaged by exposure to the elements or degradation.[11] CODIS allows for familial searches, meaning that collection of DNA from migrants in custody could potentially affect other family members, especially if they decide to later migrate to the U.S.[12]

This proposed rule will also accelerate racial disparities in the makeup of DNA data in the CODIS database. It is known that less privileged groups are subject to differential policing and arrest in the US, "leading to different rates of incarceration and DNA recording;"[13] this rule further criminalizes Latin American communities in particular.[14]

A recent case, *Gonzalez et al. v. Immigration and Customs Enforcement* (ICE) (C.D. Cal. 2019), regarding the constitutionality of immigration detainers based solely on biometric database checks, highlights the unreliability of biometric databases. The Court found current government immigration databases to be "largely erroneous" and of "dubious reliability," and held that "the collection of datapoints ICE gathers from the various databases does not provide affirmative indicia of removability to satisfy probable cause determination because the aggregation of information ICE receives from the databases is largely erroneous and fails to capture certain complexities and nuances of immigration law."[15] Given the existing flaws in an unreliability of biometric databases in the country, the absence of provisions in the proposed rule for processes to review personal data that has been captured, challenge flawed data, or provide limitations on how the data can be used in the criminal justice context is likely to provoke court challenges and public backlash.

In Kenya, for example, the NIIMS biometric identification project, described above, has also been vulnerable to legal challenges due to the known inaccuracies in functional databases that are, in that project, intended to be linked through the new system.[16]

The lack of transparent and accountable means to identify and resolve the implications of database flaws exposes CODIS to similar legal challenges, unless these foreseeable gaps are appropriately analyzed and comprehensively addressed prior to the significant expansion of the database envisioned in the rule justification.

---

[11] Naomi Elster, *How Forensic DNA Evidence Can Lead to Wrongful Convictions*, JSTOR Daily (December 6, 2017), https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions/.

[12] *See* Natalie Ram, *The Mismatch Between Probable Cause and Partial Matching*, The Yale Law Journal Forum (Apr. 13, 2009), https://www.yalelawjournal.org/forum/the-mismatch-between-probable-cause-and-partial-matching, ("[A] match, however, may inculpate close genetic relatives not otherwise in the relevant database who, like the crime scene sample, share some but not all of the examined loci with the individual whose CODIS profile provided the partial match.").

[13] *Id.*

[14] *See, e.g.*, Dr. Craig Klugman, *Immigrant DNA Collection: Fighting Crime or Moral Panic*, Bioethics.net (October 23, 2019), http://www.bioethics.net/2019/10/immigrant-dna-collection-fighting-crime-or-moral-panic/ (noting that immigrants from Spanish-speaking and Muslim-majority countries are significantly more likely to be detained than other immigrants) (citing Freedom for Immigrants, *Detention by the Numbers* (presenting statistics on detained immigrants by country of origin), https://www.freedomforimmigrants.org/detention-statistics; American Immigration Council, *The Landscape of Immigration Detention in the United States*, December 5, 2018, https://americanimmigrationcouncil.org/research/landscape-immigration-detention-united-states).

[15] *Gerardo Gonzales et al. v. Immigration and Customs Enforcement et al.*, No. 12-9021 (C.D. Cal. Sept. 27, 2019).

[16] *See* Nairobi High Court, *Nubian Rights Forum et al. v. The Honourable Attorney General et al*, Petition No. 56 (2019).

c. Lack of Appropriate Comment Period

The proposed rule has a comment period of only 20 days, which is excessively brief for adequate consideration of a rule with such complex consequences. Moreover, international experience discussed throughout this comment demonstrates that when rules to permit large-scale DNA collection are introduced abruptly and without adequate public comment and debate, they frequently produce backlash in public and in the courts.

The Administrative Procedure Act of 1946 (APA) generally provides for a 30 day waiting period before a rule can become effective.[17] While certain rules are exempt from this in the APA, the *Federal Register* estimates that agencies "will specify a comment period ranging from 30 to 60 days" and that "for complex rulemakings, agencies may provide for longer time periods, such as 180 days or more."[18]

The 20-day comment period is even shorter than the consultation relating to previous amendments regarding DNA collection under the same Act.[19] By comparison, the comment period for a highly specific proposed rule on requirements for fingerprint-based criminal history records checks for individuals seeking unescorted access to research or test reactors was initially set at 86 days and later extended to 206 days.[20]

The comment period of 20 days does not, furthermore, permit the suitable consideration of examples and lessons from other jurisdictions presented in this comment.

2. THE EXPANSION OF DNA PROFILING ABSENT STRICT SAFEGUARDS WASTES PUBLIC RESOURCES

The proposed rule, among other things, expands the federal government's power to mandate DNA sampling from individuals who have no plausible connection to the forensic purposes of the CODIS system. Countries that expend massive public resources toward DNA collection have frequently found their resources wasted, following judicial challenges that invalidate or substantially constrain the proposed system. In fact, courts across Europe, the Middle East, and Africa, have found the scaling of DNA collection, including for non-forensic purposes, to be a violation of privacy rights and personal freedoms. The United Nations has expressed similar views.

a. United Kingdom

In 2006, the UK proposed a universal DNA database to include every citizen and visitor to Britain, which sparked intense political debates in the country. Critiques included the potential for misuse by the police, the State or anyone who might infiltrate the system; the increased risk of errors and false matches with crime scene DNA as the database expands and the imposition of criminal sanctions against all those members of the population and visitors who might refuse to voluntarily provide their DNA.[21]

---

[17] 5 U.S.C. §553.
[18] Office of the Federal Register, *A Guide to the Rulemaking Process*, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.
[19] In 2008, there was a 30 day comment period for amendments to proposed Rule RIN 1105-AB24, *see* Federal Register Vol. 23, No. 238 (December 10, 2008), https://www.justice.gov/archive/olp/pdf/final-dna-collection.pdf.
[20] *See* Nuclear Regulatory Commission, *Requirements for Fingerprint-based Criminal History Records Checks for Individuals Seeking Unescorted Access to Research or Test Reactors,* RIN 3150-AI25, https://www.regulations.gov/document?D=NRC-2008-0619-0021.
[21] H.M. Wallace et al., *Forensic DNA databases: Ethical and Legal Standards – a global review*, Egyptian Journal of Forensic Sciences, Vol. 4, Issue 3, 57-63 (September 2013), https://www.sciencedirect.com/science/article/pii/S2090536X14000239.

In 2008, the European Court of Human Rights reached a unanimous judgment in a case against the UK on DNA collection, holding that "the retention [of DNA, biological samples and fingerprints] constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society".[22] The Court found that the retention of innocent people's DNA constituted a breach of privacy enshrined in the European Convention on Human Rights, finding that "an individual's concern about the possible future use of private information retained by the authorities is legitimate."[23] The Court stated that "bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today."[24] Regarding proportionality and criminal justice purposes raised by the UK government, the Court noted that "notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving the proper balance with the competing interests of preserving respect for private life."[25]

In response to the judgment and debate around the issue of DNA collection, the Protection of Freedoms Act 2012 came into force in England and Wales, which saw the removal of over 1.7 million DNA profiles of innocent people and children and the destruction of close to 8 million DNA samples.[26]

The European Court judgment influenced and shaped the legal framework of DNA collection throughout the European Union and the wider Council of Europe region.

It should be noted in relation to the Court's concerns directly addressing the *retention* of DNA profiles, that the rule justification from the Attorney General presents no information concerning the expungement of immigrants' DNA from the CODIS system.[27]

b. Kenya

In Kenya, proposed legislative amendments introducing a digital identification system, described above, allow for mandatory DNA collection of all individuals resident in Kenya. In April 2019, following a challenge to the controversial National Identity Management System (NIIMS), the Kenyan High Court issued an interim order (preliminary injunction), limiting the type of data that can be collected by the Kenyan government. Stating that "there is a risk of prejudice being caused to members of the public and their right to privacy by the disclosure of certain types of information, in the absence of proposals on how that data will be protected", the Court held that DNA data cannot be collected for NIIMS.

---

[22] European Court of Human Rights, Judgment, *Marper v. The United Kingdom* (2008), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}.
[23] *Id.* at para. 71.
[24] *Id.*
[25] *Id.* at para. 112.
[26] National DNA Database Annual Report 2012/13, The Home Office, London, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/252885/NDNAD_Annual_Report_2012-13.pdf.
[27] RIN 1105-AB56. See also *CODIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (citing expungement policies in place with respect to criminal detainees only).

In a hearing on the merits of the legal challenge, the Kenyan Government has since walked back its intention to collect DNA information from its citizens, stating that despite the framing of the draft legislation, the Government was not planning to collect any new information from citizens.[28]

c. Kuwait

In 2015, Kuwait introduced legislation proposing to force citizens and visitors to provide DNA samples to the Government. The Government argued the law was necessary for national security reasons.[29]

The law was challenged, with the petitioners arguing that "compelling every citizen, resident and visitor to submit a DNA sample to the government is similar to forcing house searches without a warrant," adding that "the body is more sacred than houses."[30]

In 2017, Kuwait was forced to abandon the project to which the Interior Ministry had allocated $400 million.[31] The Court found that the DNA law violated the Kuwaiti constitutional provisions on personal liberty and privacy.[32] The UN Human Rights Committee (HRC) had previously found that the law "imposed unnecessary restrictions on the right to privacy."[33] The HRC specifically criticized "the lack of clarity on whether necessary safeguards are in place to guarantee confidentiality and prevent the arbitrary use of the DNA samples collected"[34] and recommended that the law should be amended to "limit DNA collection to individuals suspecting of having committed serious crimes and on the basis of a court decision."[35]

d. Malaysia

When Malaysia introduced a DNA Identification Bill, the draft bill was highly criticized for its use as a tool to suppress political dissent and the lack of protection mechanisms.[36] The absence of data protection schemes and the presence of privacy concerns, as well as the fact that data was going to be stored for indefinite time periods, led to calls for the bill to be withdrawn.[37] A current proposal to collect DNA

---

[28] Standard Digital, *Witness tells court huduma number project was not to collect fresh information from Kenyans* (September 27, 2019), https://www.standardmedia.co.ke/article/2001343531/queries-over-huduma-number-as-state-says-it-already-had-data.

[29] IFL Science, *DNA Testing now mandatory in Kuwait*, https://www.iflscience.com/technology/dna-testing-now-mandatory-kuwait/.

[30] New Scientist, *Kuwait lawyers fight world's first mandatory DNA sampling law* (September 22, 2016), https://www.newscientist.com/article/2106835-kuwait-lawyers-fight-worlds-first-mandatory-dna-sampling-law/.

[31] *See* IFL Science, *DNA Testing now mandatory in Kuwait*, https://www.iflscience.com/technology/dna-testing-now-mandatory-kuwait/; *see also* New Scientist, *Kuwait's plans for mandatory DNA database have been cancelled*, (October 9, 2017), https://www.newscientist.com/article/2149830-kuwaits-plans-for-mandatory-dna-database-have-been-cancelled/.

[32] Human Rights Watch, *Kuwait court strikes down draconian DNA law* (October 17, 2017), https://www.hrw.org/news/2017/10/17/kuwait-court-strikes-down-draconian-dna-law.

[33] United Nations Human Rights Committee, CCPR/C/KWT/CO/3 (August 11, 2016), https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fKWT%2fCO%2f3&Lang=en.

[34] *Id*. at para. 20(c).

[35] *Id*. at para. 21.

[36] Reuters, *Malaysian government submits controversial DNA bill* (August 26, 2018), https://uk.reuters.com/article/uk-malaysia-dna-law/malaysian-government-submits-controversial-dna-bill-idUKKLR11608320080826.

[37] *See, e.g.*, The Malaysian Bar, *Bar Council Memorandum on the Deoxyribonucleic Acid Identification Bill* (March 6, 2009), https://www.malaysianbar.org.my/legal/general_news/bar_council_memorandum_on_the_deoxyribonucleic_acid_dna_identification_bill.html.

information and record it through the birth registration process has suffered from backlash and is said to be undergoing a "comprehensive study" before it progresses any further.[38]

In order to avoid repeating the missteps of other countries, the agencies proposing the rule change should halt its introduction and instead undertake a comprehensive assessment grounded in comparative as well as national research on best practices.

3. THE FAILURE TO ADDRESS CIVIL RIGHTS IMPLICATIONS OF THE RULE CHANGE JEOPARDIZES ITS IMPLEMENTATION

While the agency justification presents this rule change as a minor housekeeping matter, the proposed rule in reality has the potential to implicate civil rights of millions of American citizens and immigrants, in light of the unique properties of DNA as an identification tool. The relevant agencies should, accordingly, avoid the procedural missteps followed in other jurisdictions, outlined briefly here, by reconsidering the approach to rulemaking in this matter.

New technologies are naturally vulnerable and open to abuse, as global examples presented below readily illustrate. Legislation and regulatory frameworks applicable to new technologies must limit the inherent risk of "purpose creep" that can plague these powerful systems, often leading to the disproportionate targeting and surveillance of particularly vulnerable communities. Technological advancements in the capture, storage and centralization of personal data have been adopted in other countries without strong legal protections in place, leading to a notorious human rights and privacy violations.

The proposed rule seeks to strike 28 CFR § 28.12(b)(4), a regulation under the DNA Fingerprint Act of 2005, which in itself does not include strong enough protection provisions on what type of data can be collected for what purpose and how long it can be stored. The underlying DNA Identification Act of 1994 (42 U.S.C. §14132) does not include any such provisions either. The current regulation of biometric databases in the United States carries the same risks that are observable in other contexts described below.

These dangers relate to the disparate impact that racially biased datasets have on the operation of databases like CODIS (noted above, section 1(b)), as well as threats posed by external entities who access and use the data collected and government agencies who may re-appropriate what the data are used for, without the data subject's knowledge, consent or recourse.[39] The proposed rule would exacerbate these known risks posed by DNA data collection and storage in CODIS, creating an unnecessarily heightened liability to legal challenges.

a. India

In India, a legal challenge to the national biometric identity system, Aadhaar, emphasized the legal frameworks that must be in place prior to the collection and centralization of sensitive biometric data collection. The constitutionality of the Aadhaar system was challenged in dozens of substantive petitions that have embroiled the system in more than eight years of litigation. The Indian Supreme Court has ordered, inter alia, the adoption of a robust law for data protection, limited data sharing options, and limited the ability of private companies to access Aadhaar data.

---

[38] Malay Mail, *Proposal to create DNA data bank needs comprehensive study says National Registration Dept*. (September 24, 2019), https://www.malaymail.com/news/malaysia/2019/09/24/proposal-to-create-dna-data-bank-needs-comprehensive-study-says-national-re/1793913.

[39] *See, e.g.*, FBI, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.

In 2018, India's Supreme Court limited the application of the highly controversial Aadhaar digital identification system, which records both biometric and biographical information on approximately 1.2 billion people.[40] Following the rollout of the project that saw people's biometrics stored in a single central database, the system was exposed to hacks and leaks.[41]

In a more recent concerning development, however, agencies in India are using data and information gained through the Aadhaar scheme to perpetrate human rights abuses against ethnic and religious minorities.

In Assam state in northeast India, the government is updating a National Register of Citizens (NRC) with the intention of cataloging all legal residents. However, over time, indications increased that the NRC would be used to detain and expel vulnerable minority groups, most prominently poor and/or illiterate members of the Muslim minority, out of the region.[42] 4.1 Million people have been removed or left off the list, placing them at risk of statelessness.[43]

It has been reported that the central agency administering Aadhaar, Unique Identification Authority of India (UDAI), is providing "technical support" to the government of Assam state in building a biometric NRC database and that information collected by the UDAI, will be under the control of Assam's Home and Political Department, which oversees the NRC, prisons and police.[44] Thus, the collection of data originally intended to assist with the distribution of state benefits is now governed by a different set of rules for the apparent purpose of indefinite detention in appalling conditions and mass expulsion of individuals who did not fully understand the risks resulting from providing their information.

b. Kenya

The recent hearings on the NIIMS system in Kenya highlighted the risks of exclusion and abuse associated with the collection of biometric information. The High Court heard evidence from the petitioners that the proposed information to be collected could lead to mass surveillance and irreversible data braches.[45] The petitioner's cybersecurity expert testified that the information gathered could be used to profile certain segments of society and manipulate behavior over time.[46] Further, while passwords can be replaced if they are compromised in the event of a breach, the kind of personal information collected through emerging technologies – most especially DNA – is irreplaceable and increases the risks of identity theft and other forms of abuse.

---

[40] Quartz India, *Aadhaar is voluntary – but millions of Indians are already trapped* (September 26, 2018), https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/.
[41] Scroll India, *Reading List: Six articles on the controversy surrounding Aadhaar*, https://scroll.in/latest/865329/reading-list-six-articles-on-the-controversy-surrounding-aadhaar.
[42] Time, *4 Million Citizens Could Be Made Stateless Tomorrow. Here's What to Know* (August 30, 2019), https://time.com/5665262/india-national-register-of-citizens-stateless-assam/.
[43] BBC, *Assam NRC: what next for 1.9 million stateless Indians* (August 31, 2019), https://www.bbc.co.uk/news/world-asia-india-49520593.
[44] Huffington Post, *All Your Aadhaar Fears May Be Coming True in Assam* (July 11, 2019), https://www.huffingtonpost.in/entry/aadhaar-fears-coming-true-in-assam_in_5d26956be4b0cfb59600624f?guccounter=2.
[45] Standard Digital, *State bought bogus system for Huduma number listing* (September 24, 2019), https://www.standardmedia.co.ke/article/2001343060/state-bought-bogus-system-for-huduma-number-listing.
[46] *Id.*

c. China

It is also important to consider, in the context of expanding CODIS, the potency of large centralized databases when they operate without constraint, and to understand the applications that could be integrated into CODIS in the future if not appropriately constrained.

China's history in population surveillance is well-documented. Now, the country is using biometric technologies, including DNA collection and facial recognition, to specifically target minority groups which have long faced discriminatory practices, such as the predominantly Muslim Uyghur community.[47]

In the US and the UK, renowned universities and journals have hosted projects and published studies on technologies specifically designed to identify Chinese minorities.[48] The backlash and controversy around these publications have led one journal's editor-in-chief to state that "like other technologies in the area of intelligent systems, facial recognition can and will have far-reaching implications, both positive and negative and can potentially be used for possible unexpected malicious purposes," adding that he does "not agree with or support such usages of the developed concepts or methods."[49]

The campaign to track members of the Uyghur community in China relies in part on public DNA databases and violates scientific norms of consent with Chinese scientists contributing Uyghur DNA samples to a global database.[50] No limitations on genetic surveillance have been built in to the proposed US rule in relation to CODIS, which specifically targets certain communities as a result of its focus on immigration detainees and their relatives.

4. CONCLUSIONS AND RECOMMENDATIONS

The short comment period, lack of state, cross-agency and public consultation, and inadequate risk assessment prior to the publication of the proposed rule, leave the rulemaking process vulnerable to legal challenge and present foreseeable risks to citizens and immigrants.

We therefore recommend that the proposed rule should be withdrawn and undergo significant consultation and risk assessment prior to its further consideration, including a federalism assessment. Any comment period connected with the contents of the proposed rule should be significantly increased in recognition of the complex and wide-ranging scope of its foreseeable impact.

---

[47] Coda, *Western Academia Helps Build China's Automated Racism* (August 6, 2019), https://codastory.com/authoritarian-tech/western-academia-china-automated-racism/ ("From facial recognition cameras in mosques to mass DNA collection and iris scans, biometrics are being deployed in Xinjiang to track Uyghurs and other minorities on an unprecedented scale. Most of China's billion-dollar facial recognition startups now sell ethnicity analytics software for police to automatically distinguish Uyghurs from others.").
[48] *Id.*
[49] *Id.*
[50] N.Y. Times, *China uses DNA to track its People with the Help of American Expertise* (February 21, 2019), https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.