

Opinion | Rights | Mar 11, 2021

Biometric Data and Midnight Regulations

Dan Berger, Margaret Hu, Sara H. Katsanis, and Jennifer K. Wagner



The Biden Administration should assess the long-term effect of a Trump era biometric data collection policy.

The final months and days of the Trump Administration included a flurry of proposed rules, the most troubling of which involved a widespread expansion of mass biometric collection by the U.S. Department of Homeland Security (DHS).

On September 11, 2020, DHS [issued](#) a notice of proposed rulemaking on the collection and use of biometric information—such as digital fingerprints, iris scans, palm and voice prints, and DNA—by the U.S. Citizenship and Immigration Services (USCIS). DHS reportedly [estimated](#) that

biometric submissions under this overall collection rule could increase to over 6 million total submissions of biometric data.

Two months later, shortly after the presidential election, DHS proposed an additional rule on the collection of biometric data from non-U.S. citizens, including those who are [entering](#) and departing the United States. DHS also withdrew two earlier, narrower proposed rules on [leaving](#) the United States from airports and seaports and [participating](#) in the U.S. Visitor and Immigrant Status Indicator Technology Program.

In mid-December, DHS reportedly [finished](#) its internal review of its September proposal on the overall collection and use of biometric data by USCIS, and, on January 13, the [Office of Information and Regulatory Affairs concluded](#) its review of this rule, allowing DHS to take steps to finalize it.

DHS failed, however, to publish its overall biometric collection rule in the *Federal Register* before President Joe Biden was sworn into office on January 20. On Inauguration Day, the new White House Chief of Staff [Ron Klain](#) circulated a [memo](#) to the heads of the executive agencies, calling on them to postpone implementation of midnight regulations and to [withdraw](#) any rules—such as the DHS biometric rule—that had yet to be published in the *Federal Register*.

DHS now has an opportunity to revisit the Trump Administration's regulatory policies on biometrics. In the case of the proposed overall biometrics collection rule, the entire rulemaking was both ill-advised and rushed, as we detailed in the public comment we [submitted](#) to DHS. The notice of proposed rulemaking [provided](#) an extraordinarily short window of 30 days for public comments, making it virtually impossible for experts to assess the proposed rule thoroughly. Indeed, each section of the proposed rule contained scientific, technical, legal, economic, and ethical issues that warranted further evaluation by experts in industries, including those in genetics, biometrics, forensics, ethics, and distinct areas of law such as immigration and data privacy, among other fields.

The proposed rule [outlined](#) two separate collection and analysis processes: the expanded definition and uses of biometrics, and the systematic implementation of DNA testing for verification of family relationships. These modifications are complex and should have been separately addressed since the legal authority—as well as the parameters and oversight for biometric verification and testing—are different for each of these processes.

In addition, the proposed rule aimed to expand DNA testing for detection of child trafficking, yet it lacked key details that would have been necessary to facilitate such an objective. To be effective, a final rule on child trafficking detection must address two realities: first, the presence of a biological relationship does not [eliminate](#) the possibility of a parent trafficking their child, and, second, the absence of a parentage relationship does not [constitute](#) evidence of trafficking.

The proposed rule would have also set forth plans to [retain](#) relationship test results as partial DNA profiles. Any genetic data, however, should be destroyed to prevent misuse of the data. Furthermore, only the resulting test outcomes that confirm or deny a relationship should be retained for immigration records. These results should be subject to the important prerequisite for DHS to demonstrate that the planned DNA testing and data retention is consistent with statutory authority.

The proposed rule would have [relied](#) on rapid DNA tests at border entry points and relationship testing laboratories accredited by the [American Association of Blood Banks](#) (AABB). This accreditation, however, is insufficient oversight, as it would not address how laboratories should communicate test limitations before testing, nor how laboratories should handle unusual test results or unexpected findings. Moreover, oversight of rapid DNA technologies is limited to the technical capabilities of the testing instruments. Similar to the lack of oversight with the AABB accreditation, it is not clear whether there would have been sufficient oversight of rapid testing of DNA to achieve the stated goals of the proposed rule.

To verify family relationships accurately, relationship DNA testing should use technology that measures a range of relationships—not merely parentage. The technology that is most often used in AABB-accredited laboratories and on rapid DNA tests can *only* be [applied](#) to parent-child and full sibling relationships, limiting the scope of the rule’s verification procedures.

In addition to testing issues, the proposed rule lacked clear guidelines for sharing biometric data, including DNA test results. The proposed rule would have [allowed](#) DHS to share DNA test results and biometric data “with other agencies where there are national security, public safety, fraud, or other investigative needs.” Once DNA is collected and testing results are stored, however, there would have been a risk that DHS could have shared this data for uses beyond the initial objectives stated in the proposed rule.

This expansion of DNA collection in the proposed rule would have applied to the collection and storage of data on children as well. Historically, data collected from children has been [recognized](#) as more sensitive than data collected from adults. This increased collection may have subjected children to unnecessary and unjustified criminal and terroristic screening. Furthermore, this expansion would have removed the presumption of innocence for children and would have been contrary to the growing trend to [protect](#) trafficked people from punishment for acts undertaken at the demand of their traffickers. Any proposed change on collecting biometric information from children must be [aligned](#) with congressional action and subject to independent oversight by professionals with relevant expertise.

Not only would the proposed rule have expanded the scope of collection, but it also would have further expanded the definition of biometrics to [authorize](#) the collection of personal data for the purposes of vetting and tracking individuals throughout the “immigration lifecycle.” The

proposed rule would have [marked](#) a major shift toward “dataveillance” of immigrants—and even of U.S. citizens and lawful permanent residents—by [authorizing](#) DHS to move “beyond only eligibility and admissibility determinations” to [enable](#) “identity management” and “enhanced vetting” through data collection and storage. These expanded applications reflected major departures from agency privacy practices that recognize the critical importance of nuance, context, and discretion under the [Privacy Act](#) of 1974.

In addition to privacy concerns, some of the technologies that the proposed rule would have specifically allowed—such as facial recognition—have been scientifically [shown](#) to be [discriminatory](#), for example against [women](#) and [people of color](#). The proposed rule would likely have created disparate and discriminatory effects on certain populations and groups of people.

Overall, the proposed rule’s changes would have been both complex and sweeping. Any such changes should be subject to congressional action and rigorous, sustained oversight.

Now that the DHS changes have been blocked by the Klain memo, DHS should take any further steps needed under the [Administrative Procedure Act](#) to prevent the future implementation of ill-considered biometric policies. The Biden Administration now has the opportunity to review the Trump Administration’s midnight regulatory actions and to consider their long-term impact carefully.



Dan Berger is a partner at Curran, Berger & Kludt.



Margaret Hu is a professor of law and of international affairs at The Pennsylvania State University.



Sara H. Katsanis is a research assistant professor of pediatrics at Northwestern University Feinberg School of Medicine.



Jennifer K. Wagner is an assistant professor in the Center for Translational Bioethics and Health Care Policy at Geisinger.

The views expressed in this essay are those of the authors and not necessarily those of the institutions with which they are affiliated.

Tagged: Biometrics, Data Privacy, Department of Homeland Security