1-1-2016

Biometric Identity

Jonathan T. Weinberg
Wayne State University

DOI:10.1145/2846082

Jonathan T. Weinberg

Law and Technology
Biometric Identity

Assessing the promises and dangers of biometric identity plans.

THREE YEARS AGO, the U.S. Senate passed a comprehensive immigration reform bill. The drafters of that bill pushed for a requirement that every employed person in the U.S.—whether citizen or noncitizen, native-born or immigrant—should have to get a federal government-issued ID card. The holder's biometric information, either fingerprints or a different technology, would be encrypted on the card. Every time a U.S. worker took a new job, the employer would take her fingerprints or other biometric, so as to check her physical characteristics against the information on the card. If the biometric information matched, it would establish the job applicant was the card's rightful bearer. The employer would then transmit the identity information on the card to a central database, to verify she was legally authorized to work. In the end, though, the drafters dropped the ID card proposal from the bill.

In India, the government is undertaking to assign to residents 1.2 billion unique "Aadhaar" ID numbers, linked to each person's biometrics—photograph, 10 fingerprints, and two iris scans. The government aims to make use and verification of one's Aadhaar number an inseparable part of daily life. The card is accepted as identification and proof of address for banking purposes; authorities are pushing forward with plans to use Aadhaar to scrub voting lists; and a host of government agencies are making it mandatory under their programs, all notwithstanding an interim order by India's Supreme Court forbidding such requirements.

Biometric information helps connect abstract legal status to the physical individual.

Both of these stories involve databases with two features. First, they include entries for all or the vast majority of a country's residents. Second, there is a mechanism to tie the data entries to the subjects' biometric characteristics, which can be checked or verified in the field. In that way, the physical person—showing up for work, or presenting herself at an ATM, or seeking health benefits from a government clinic—can be connected to her identity and description in the database. The U.S. plan has been the pet project of a few senators for years, but has never become law. The government of India, by contrast, has invested 50 billion rupees (US$775,000,000) in its project and has collected biometric information from 800 million people so far. That country's Supreme Court, though, is currently pondering the constitutionality of the plan.

Are plans like these desirable? They present some policy advantages; biometric identification techniques enable governments to achieve certain popularly supported goals more successfully. In the U.S., the law forbids employers to hire people who are in the country illegally or on temporary visas, unless the Department of Homeland Security has granted them work authorization. But whether a person at a particular moment has legal work authorization (or legal immigration status) is not apparent when looking at her; the information resides in a database in Washington, D.C. She may present government-issued documents, but those docu-

An employee uses an Aadhaar-based entry system to verify identity at a building in New Delhi, India.

PHOTO BY VIPIN KUMAR/HINDUSTAN TIMES VIA GETTY IMAGES

ments may be somebody else's; taking her biometric information helps connect abstract legal status to the physical individual.

Pakistan was able to rely on biometric (fingerprint-based) ID cards to provide reconstruction grants to families affected by severe flooding, without too much money going astray. Some countries take voters' biometric data in order to de-duplicate voting lists (that is, to ensure single individuals do not appear on voter registration lists multiple times). Integration of biometric identification into the system for paying government employees in Nigeria is said to have helped uncover more than 60,000 "ghost workers."

More generally, people need some way of verifying their identity so governments will provide them with services and businesses will enter into relationships with them. Governments want satisfactory proof of identity, and often proof of residency or citizenship (which in turn is predicated on proof of identity) before they provide payments such as pension or welfare benefits, or allow individuals to vote, or grant passports or register property transfers. Private actors require people to verify their identity before they can take such steps as opening a bank account, renting an apartment, or cashing a check.

In the industrialized West, these concerns have been addressed primarily through birth registration: Children are registered with the state at birth, and are entitled to documents as proof. They can use those documents to get others such as driver's licenses and passports. All of those documents, tied to an entry in some official database, can be used to verify the holder's identity. But in some poorer countries that does not work, because as many as 70% of all births go unregistered. That is why projects like Aadhaar, in a variety of less-industrialized countries, are exploring the use of biometrics as a way of tying individuals directly into identity-verifying databases.

The connection of our physical bodies to entries in government databases, though, is also problematic. Consider the main episodes in U.S. history where government not only issued biometric ID, but required persons to carry that ID. Before the Civil War, free blacks were sometimes required to carry certificates that recited their names and employers and included the mid-19th-century version of biometrics: they described the worker's physical characteristics, including such matters as age, complexion, build, height, and scars. A free black without adequate identification risked being arrested or enslaved. After 1892, U.S. law required all Chinese persons in the U.S. to carry "certificates of residence" validating their immigration status, on penalty of deportation. Congress mandated that each card contained the holder's photograph; that biometric, said a senator, was "the only effective method" for identifying Chinese migrants.

When the U.S. government next told a group of people they had to carry cards with biometric identifiers at all times, it was 1952. The card in ques-

tion was the "green card" issued to noncitizen residents in the U.S.; the motivation was fear of the Communist threat. Congress members, worrying that outsiders sympathetic to enemy countries would act as a fifth column, mandated that all noncitizens carry their immigration documentation wherever they went. That law is still on the books today.

That is not a confidence-inspiring record. When U.S. law has imposed requirements that certain people carry biometric ID at all times, it has been so a target could be required to show a document linking him to a dataset telling law enforcement officers whether to enslave, detain, or deport him. That is the promise and the danger of biometric ID systems. ID systems without a biometric component have limited law-enforcement value, because they lack good mechanisms by means of which police can connect the persons standing in front of them to the documents they produce. Biometric ID systems enable better identification, but more effective policing carries risks of its own.

It is perhaps not coincidental, then, that modern U.S. thinking incorporates a severe allergy to anything that looks like a biometric national ID card. Americans have accepted the Social Security number, which in practice serves as a unique common identifier linking them to entries in a variety of federal and private databases. They have accepted a requirement that they carry—and often produce—driver's licenses while driving. But they need not carry or display driver's licenses at other times, and driver's licenses do not display a unique common identifier that could reliably identify the holder across federal databases. In particular, it is illegal for a driver's license or any other state-issued identification document to display the holder's Social Security number.

Besides the baseline concerns associated with police being able to easily and effectively identify citizens, one can identify a wide range of more nuanced risks flowing from government identity systems' coming to rely on biometric identifiers and a central database in some manner associated with them. One risk relates to data security: Can the government keep this information safe, avoiding either privacy breaches or identity theft? One of the claims made by plaintiffs in the Aadhaar litigation is that data security for the submitted information is unacceptably weak. A second risk relates to the damage done by (the inevitable) bad information in the database, especially if use of the card or biometrics becomes ubiquitous. Will the database become so useful it is treated as presumptively correct, with bad information difficult or impossible to change? Intentionally planting bad information would then be an excellent route to identity theft or worse.

It is important to be mindful of the substantial privacy risks associated with biometric identity plans.

Another concern: To the extent the use of a biometric or card to verify identity becomes routine in everyday transactions, it would be easy to structure the system so each use of the card adds information to the relevant databases. That would fatten the data portfolios maintained on each citizen and would limit individuals' ability to undertake everyday activities free of surveillance. Finally, the government might gain leverage over the citizenry through its power to revoke or limit the use of card or biometric data to verify identity—what happens when government decides to flag the database entries of undesirable citizens so their biometrics or cards can no longer be used to obtain services?

The implementation details of any biometric identity plan are key. The designers of the proposed U.S. worker ID plan, thus, sought to forestall objections by ensuring no biometrics would be stored in the central database; rather, their plan was that biometrics would be stored only on individuals' cards, to be checked against their physical characteristics using card readers in the field. That way, central government authorities would not have access to the biometrics at all. The Aadhaar plan, by contrast, does not rely on cards: biometrics are stored centrally so a person's merely presenting his fingerprints identifies him to the system.

Another approach avoiding some risks would tie citizens' biometrics only to limited-purpose databases—designed for particular functions and not calling up other information in the government's possession—rather than to an all-encompassing database (or a linked set of databases) containing multiple classes of information. Such functional structures can be less expensive than multipurpose identity platforms (although not if a country ends up establishing multiple, separate biometric systems serving separate goals). Some countries, for example, have done biometric registration for the limited purpose of enabling voting in national elections. But limited-purpose biometric identity plans can find their focus shifting; in several countries that have set up single-purpose voter registration systems, the voter registration card has become a de facto national ID card. In the U.S., the Social Security number, created for a limited purpose, rapidly became a unique common identifier.

It is important to be mindful of the substantial privacy risks associated with biometric identity plans. This does not mean they are always a bad idea; in a country where many individuals have no means of identity verification at all, some form of appropriately structured biometric identification system can make people better off. But we have not done well in the past in the U.S. imposing biometric ID requirements, and—given the strength of our existing systems for identity verification—the risks (and costs) of any such plan in the U.S. would likely far outweigh the benefits. C

Jonathan T. Weinberg (weinberg@wayne.edu) is a Professor of Law at Wayne State University in Detroit, MI.