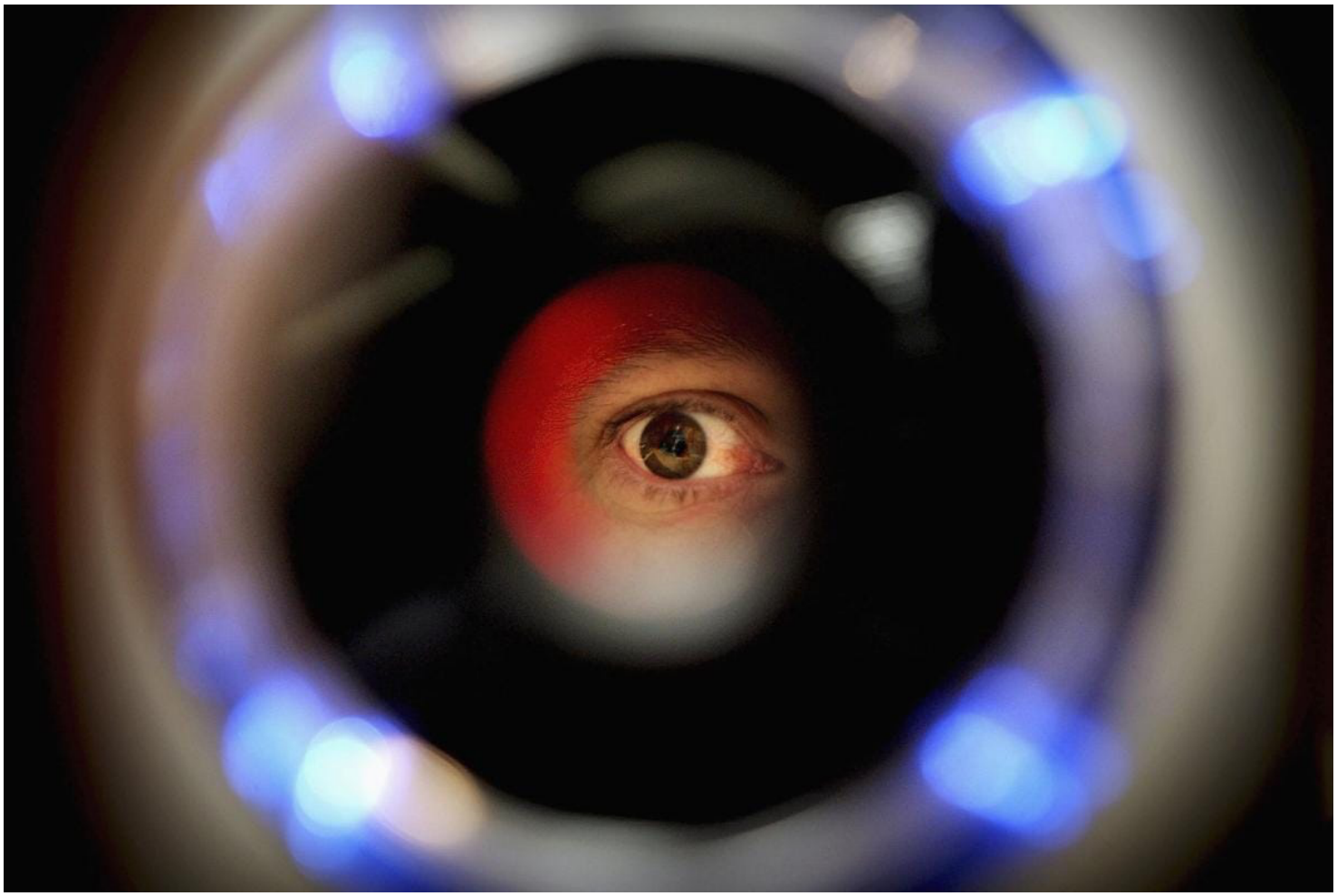
The Rise of Biodigital Surveillance

Unless we collectively decline to participate in this new social experiment, digital IDs —tied to private demographic, financial, location, movement, and biometric data— will become The New Abnormal.

Aaron Kheriaty, MD
Nov 11



This piece was recently published in Compact magazine, reprinted here with permission.

Recently, as I was about to go through airport security, a saleswoman intercepted me asking if I wished to skip the security line. Intrigued, I invited her to tell me more. She shuttled me over to the CLEAR electronic kiosk and explained how the product worked. For only $180 a year, I could skip long lines at airports, sporting events, and other large gatherings. The

company's Web site explains: "Instead of using traditional ID documents, CLEAR uses your eyes and face to confirm it's really you." The CLEAR system uses not just an iris scan and facial recognition, but other biometrics like fingerprints, tied to demographic data you voluntarily hand over, and a link to your credit score (read the fine print on the consent checkbox). CLEAR also has a Health Pass that stores proof of vaccination, negative Covid tests, and health surveys.

CLEAR isn't the only enterprise working at the intersection of biometric and digital authentication. Plans for digital IDs have been in the works for several years, but they gained traction during the pandemic. ID2020 is a nonprofit alliance founded in 2016 with seed money from Microsoft, Accenture, PricewaterhouseCoopers, the Rockefeller Foundation, Cisco, and Gavi (a vaccine alliance founded by the Gates Foundation). The stated mission of ID2020 is to provide digital identities for all people worldwide by 2030. Digital IDs will be tied to fingerprints and other biometric data like iris scans, demographic information, medical records, data on education, travel, financial transactions, and bank accounts.

Almost two years before Covid, ID2020 published an article titled "Immunization: An Entry Point of Digital Identity." It argued that "immunization poses a huge opportunity to scale digital identity." The article noted cumbersome inefficiencies with paper immunization records and delineated how health challenges in developing nations could be leveraged as the pretext for implementing digital IDs. The year before, Seth Berkeley, CEO of Gavi, published a piece in *Nature*making the same argument: To achieve 100 percent vaccination

rates in underdeveloped nations, we need digital IDs. Gavi has promoted the same message at gatherings of the World Economic Forum in Davos.

The ID2020 article attempted to frame the benefits of this system as follows: "Because immunization is conducted in infancy, providing children with a digital child health card would give them a unique, portable digital identity early in life." It goes on to explain that "as children grow, their digital child health card can be used to access secondary services, such as primary school, or ease the process of obtaining alternative credentials. Effectively, the child health card becomes the first step in establishing a legal, broadly recognized identity."

This may at first glance sound sensible. But consider: If an impoverished family doesn't accept the health NGO's preferred interventions for its children, these children may not be provided any other opportunity to establish a "legal, broadly recognized identity" necessary to access things like primary school. In other words, you are literally nobody until you are vaccinated.

Just before the pandemic broke, in September 2019, ID2020 partnered with Gavi and began putting this plan into action. Using vaccines as leverage, it launched a biometrics-based digital-identity program for newborn infants in Bangladesh. The country's government embraced the initiative. When the pandemic began, ID2020 pivoted immediately to fold digital identification into Covid testing and other pandemic measures.

India's biometric ID system, Aadhaar, is the largest on the planet, with 1.3 billion digital IDs issued, covering 92 percent of the population. It requires Indian citizens to submit their photograph, iris scan, and fingerprints to qualify for social services, benefits, compensation, scholarships, legal entitlements, and nutrition programs. According to an article in the *Financial Times*, "Indian media has reported several cases of cardless individuals starving to death because they could not access benefits to which they were entitled." As the author notes, some critics argue the Indian Aadhaar system "has largely failed to fulfill its original promise of improving welfare and now acts as a tool for social exclusion and corporate influence."

"We are conditioning children to accept biometric verification."

Using biometrics for everyday transactions routinizes these technologies. We are

Using biometrics for everyday transactions routinizes these technologies. We are conditioning children to accept biometric verification as a matter of course. Face IDs are now used in multiple school districts to expedite the movement of students through school lunch lines. Until recently, biometrics such as fingerprints were used only for high-security purposes—when charging someone with a crime, for example, or when notarizing an important document. Today, routine biometric verification for repetitive activities from mobile phones to lunch lines gets young people used to the idea that *their bodies are tools used in transactions*. We are instrumentalizing the body in subtle but powerful ways.

Those with economic interests in creating markets for their products—whether vaccines, digital surveillance products, or harvested data—will continue to deploy the carrots and sticks of access to medical care and other services to promote digital IDs in underdeveloped nations. In developed nations, they will initially use a velvet glove approach of nudges, selling digital IDs as convenience and time-saving measures that will be hard for many to turn down, like skipping long Transportation Security Administration security lines at airports. The privacy risks, including the possibility for constant surveillance and data harvesting, will fade into the background when you are about to miss your flight if you can't skip to the front of the line.

But as Nick Corbishley, author of a recent book on digital IDs, points out, decisions made in the moment may carry long-term negative consequences: "If biometric data is hacked, there is no way of undoing the damage. You cannot change or cancel your iris, fingerprint, or DNA like you can change a password or cancel your credit card." Unless we collectively decline to participate in this new social experiment, digital IDs—tied to private demographic, financial, location, movement, and biometric data—will become mechanisms for bulk data harvesting and tracking of populations around the globe. Welcome to The New Abnormal.

This column was adapted from the author's forthcoming book, The New Abnormal: The Rise of the Biomedical Security State.

The day after this was published I had a thoughtful podcast conversation on the article and my book with Compact Magazine editor Geoff Shullenberger:

Podcasts

EPISODE 37 · 37 MIN

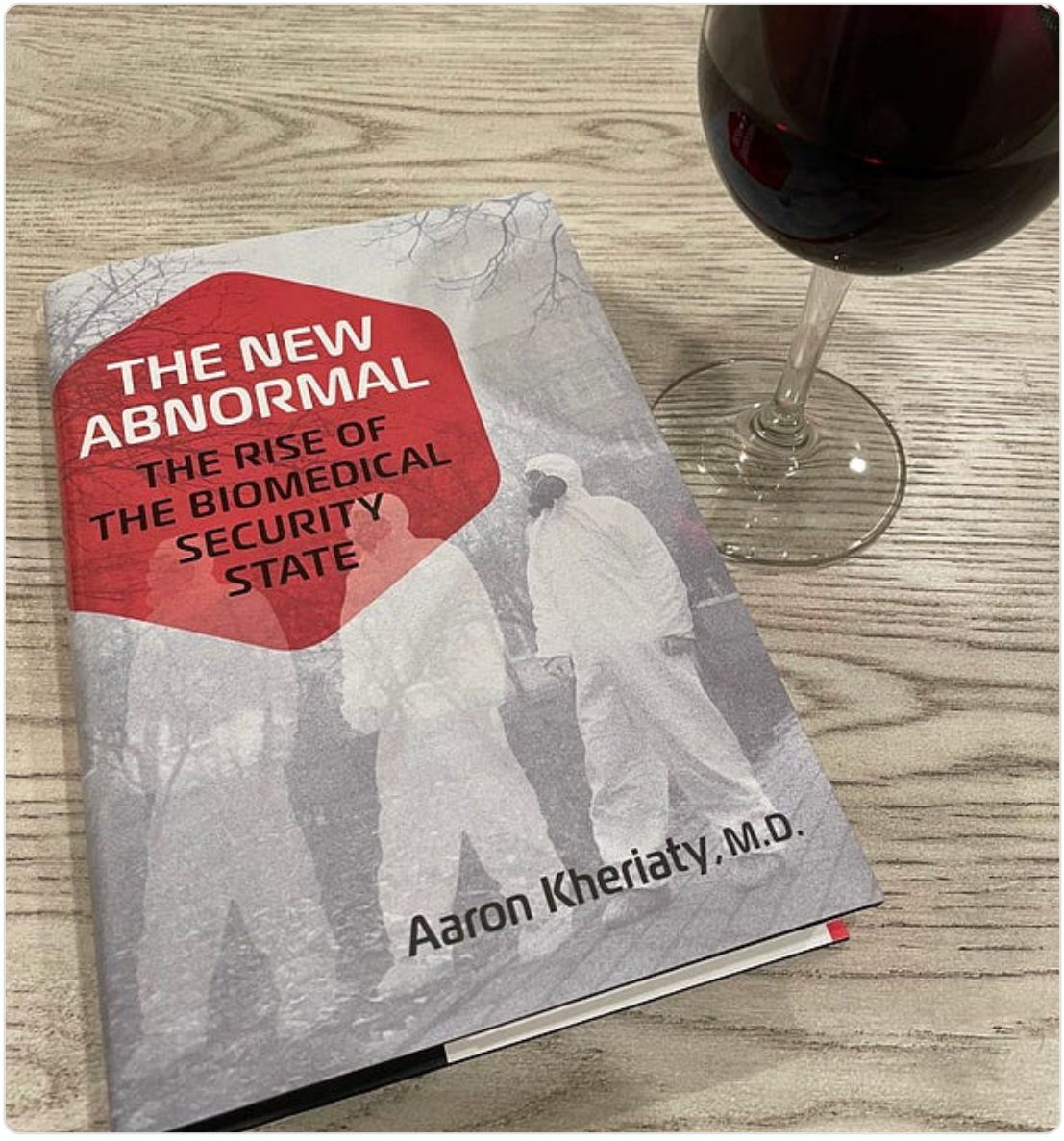
Compact Conversations: Aaron Kheriaty

Compact Podcast

Play See More ↗

Aaron Kheriaty, MD
@akheriaty

Better than Netflix... amazon.com/dp/1684513855/



1:31 AM • Oct 18, 2022

287Likes61Retweets