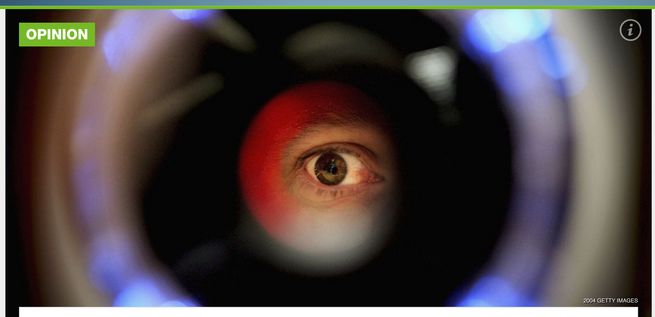
OPINION



2014 GETTY IMAGES

Biometrics are coming for you

How blue is your iris? How brisk is your walk?

July 6, 2014 12:00AM ET

by **Jathan Sadowski** - @jathansadowski

Biometrics are on the rise — and they're coming to a store, street and office near you.

The private sector is funneling billions of dollars into researching and developing biometric surveillance, for facial recognition and analysis technologies. And lawmakers are beginning to take notice. At the end of June the U.S. Department of Commerce convened a "multistakeholder process" charged with developing a "voluntary, enforceable code of conduct that specifies how the Consumer Privacy Bill of Rights applies facial recognition technology in the commercial context."

There's a lot to be worried about on the personal privacy front. But many of the risks of corporate-controlled biometrics extend beyond the usual privacy and security concerns. They include the potential for manipulating consumer behavior, turning people into commodities for profit, taking personal information about people out of context and using it to discriminate against individuals with impunity.

Biometric basics

Biometrics identify, measure and collect a biological trait or group of traits. There is a wide variety of types of existing biometrics, with more in development. Some of the most common focus on physical traits, like faces, fingerprints, irises, retinas and DNA. Others focus on behavioral elements such as voice, signature, gait and keystrokes.

In practice, biometric technologies employ a standard process across different types. A sample of the biological trait is collected using a sensor of some kind, such as a camera for faces or a recorder for voices. Through the use of an algorithm that extracts information from the biometric sample, the trait is then converted into a digital representation called a template, which can be stored in a database.

The larger the database, the more templates there are to verify or identify subjects. The key component is the algorithm used to construct the template; this is the feature that distinguishes a biometric recognition system from (and makes it better or worse than) others.

Strip-mining the body

The potential role of biometrics in the information economy is huge — especially for the massive data brokerage industry. During a 2013 U.S. Senate hearing, John D. Rockefeller IV, chairman of the Committee on Commerce, Science and Transportation, said, "In 2012 the data broker industry generated $156 billion in revenues. That's more than twice the size of the entire intelligence budget of the United States government — all generated by the effort to learn about and sell the details about our private lives."

Big Data equals big money, and biometrics present new ways to turn people's traits into profit. Think of biometrics as akin to strip-mining the body so that ever more data can be extracted. This analogy captures the degree of intrusiveness that biometrics have when they hone in on particular biological traits and pull them out of the context of the body, person and environment.

> "Biometric data would be gold to data brokers, enabling these companies to significantly fine-tune the ways they target potential customers."

Biometric data would be gold to data brokers, enabling these companies to significantly fine-tune the ways in which they target potential customers. In May the Federal Trade Commission released a report showing the extent to which data brokers have already built consumer profiles that include a slew of private information based on consumer trackable behavior. As FTC Chairwoman Edith Ramirez says, these data brokers "know as much — or even more — about us than our family and friends." Coupled with biometric algorithms and databases, these brokers and, crucially, their clients would be able to identify us in much the same way our family and friends can.

Some high-end stores already use facial recognition software to alert clerks and salespeople that a VIP or a celebrity is in the store. With large enough databases, what's to prevent stores from identifying even non-VIP customers who walk in the door? In that case, your consumer profile and reputation become far more significant.

Are you part of the "urban scramble or "rural everlasting" (to use actual data broker categories)? Are you a big spender or shoplifter? Did you just receive a large tax refund or a job promotion? Well, thanks to biometric identification and a data broker's profile, a store manager can be sure to entice you into a larger purchase. Thanks to biometrics, just as you know the stores where you shop and frequent, the stores can know you too.

Technology and identity

These implications, among others, are consequences of the ways biometrics allow and encourage more intensive commodification of physical data. In "When Biometrics Fail: Gender, Race and the Technology of Identity," social scientist Shoshana Magnet writes, "The flimsy material body is rendered rugged as biometric technologies make bodies replicable, transmittable and segmentable — breaking the body down into its component parts (from retina to fingerprint) in ways that allow it to be marketed more easily in the transnational marketplace." We've heard of the data economy, but how about the face economy or iris economy or gait economy?

There are entire corporate sectors eager to mine that data and put it to use in any number of ways. Data brokers construct in-depth consumer profiles replete with biometric templates. Salespeople and store security departments can use biometric emanations to pull up your reputation from the database. Your identity can be pinned to your location, which is better tracked as you move through streets, public squares and shops. Insurance companies, for instance, are hungry for the somatic data provided by personal health and fitness monitoring devices. Imagine what they and others could do with the knowledge and power provided by diverse types of biometrics.

No fakers

It's not all about the consumers and clients, though. Employees, too, are subject to the watchful gaze of biometrics. New surveillance technologies provide methods for employers to establish amped-up management schemes that fall under what's called Digital Taylorism. The measures we might take, as consumers in the marketplace, to avoid biometric surveillance aren't as effective in the workplace. Especially when having a job, well paying or otherwise, is becoming a privilege and bad conditions must often just be tolerated.

Now in addition to tracking employees' locations, movements and actions, recent technological advances allow for accurate biometric analysis of our emotions. Faking your way through a job you hate won't be enough when managers can algorithmically know that your heart isn't really into selling shoes or entering data into a spreadsheet. What better way to control employees and ensure they are maximally productive and never slacking than to use biometrics? Then there's the the legion of commercial opportunities available for corporations that can fine-tune their monetizing schemes to account for your moods and feelings — and in the process change how we express those emotions.

> "Labor laws must account for the new, intensified ways in which employers manage and subsequently dehumanize their employees."

The troubling implications of biometrics have inspired artists such as Zach Blas and Adam Harvey to protest them in creative ways. Harvey is behind a project called CV Dazzle, which uses "avant-garde hairstyling and makeup designs to break apart the continuity of a face" in order to evade facial recognition algorithms. Blas has created "face cages," which represent the shapes and structures that facial recognition algorithms look for so they can identify, track, and "see" human faces. He intends the face cages to be a "dramatization of the abstract violence of the biometric diagram."

Of course, there's also a counterindustry of companies ready to capitalize on anti-surveillance sentiments by providing you with gadgets to detect and jam these technologies — such as an expensive, 3-D-printed mask called the URME Personal Surveillance Identity Prosthetic created by another artist, Leo Selvaggio.

That artists are reacting to biometrics signals how these technologies have hit a social nerve. These projects draw attention to technologies that are implemented on the sly. But ultimately, political action is required to shift the balance of power; after all, resistance and reform is what keeps our bodies from being reduced to just more templates in a database.

We need stronger legislation that not only recognizes that our privacy is at risk but also takes seriously the ways in which such data are used to manipulate and control people. Consumer protection regulations should account for biometrics on their own terms rather than subsuming it under already outdated laws about data security and privacy. Labor laws must also consider the new, intensified ways in which employers manage and subsequently dehumanize their employees.

Finally, we must raise awareness about of the ever-increasing surveillance we're placed under and make it known — with our voices, votes and dollars — that it's not acceptable.

Jathan Sadowski is a freelance writer and Ph.D. student in the Consortium for Science, Policy and Outcomes at Arizona State University. He writes about social justice and political economy of technologies.

The views expressed in this article are the author's own and do not necessarily reflect Al Jazeera America's editorial policy.