



FEATURE

TECHNOLOGY

An Artist's Pioneering Masks Shield Us from Future Surveillance

Zach Blas explains why we should all be wary of the coming wave of biometric technology *by Tosten Burks*



📅 January 26, 2015

The ninth annual Biometrics for Government and Law Enforcement conference kicks off today in Arlington, Virginia, where the F.B.I., Department of Homeland Security, U.S. Army, California Border Patrol, and more gather to plot the future of snagging bad guys. This year's festivities showcase the F.B.I.'s new \$1.2 billion "Next Generation Identification" system (N.G.I.)—taken fully operational last September—a massive database and suite of tools (accessible by 18,000 federal, state, local, tribal, and international agencies) for capturing, storing, and analyzing fingerprints, palm prints, faces, and iris biometrics. The bureau calls it "a significant step forward for the criminal justice community in utilizing biometrics as an investigative enabler." In other words, the robocops are coming.

Biometrics, or ways of identifying individuals based on singular physical characteristics, have been used for criminal investigation since ancient imperial China began tracking citizens' fingerprints, but recent advancements have taken body and face quantification mainstream. Your thumb unlocks your iPhone, Japanese and Polish A.T.M.s come equipped with fingertip vein pattern recognition, Dubai police officers wear Google Glass with facial recognition software, and, as part of the N.G.I. rollout, 62 U.S. police departments are currently field-testing handheld iris and facial recognition devices. But how will this information be compiled, and what can these agencies presume to know about an individual from biometric identification? Critics point to experiments like gay face studies, and other data-driven attempts to standardize how we see large groups of people, as proof that biometrics can ultimately be as pseudoscientific as the 19th century pursuits of phrenology and anthropometry, which attempted to read into a person's identity based on say, the length of one's left foot or the shape of an individual's skull.

Concern for a world beyond the watch of government, free from systematically monitored and restricted public visibility, is the broad civil rights challenge tackled by artist and University of Buffalo Professor Zach Blas's work. Blas's mask projects, designed to visualize the way computers mathematically understand and read human faces, reject the safety of surveillance and propose a rebellion in the form of public opacity. These masks, built from facial biometric data, cast the insidious growth of visual

surveillance's technological capacity in stark relief. Some of the masks, like Blas' lumpy Facial Weaponization Suite series, are shaped so that they can't be identified as faces by biometric software, providing opacity to the wearer. Others, like his metal face cage masks, are made intentionally painful to wear, illustrating the discomfort in imposing quantified, presumptuous data onto the face of a specific individual.

Such are the capabilities of modern biometric technology that the *New Yorker* recently predicted an "emotion economy." Through the detailed, instant detection of human emotion, powered by camera technology backed by increasingly well-sourced algorithms, *attention* will soon be as quantifiably valuable as money and time. Aside from your new political identity, your face may also be your next wallet.

We talked to Blas about what it all means.

What was your first exposure to biometric technology? What was your reaction?

What captured my attention the most...were the problematics of digital standardization. I think that's what really captivated me the most. I wasn't initially focused on surveillance. And even though the work that I've done is very commonly talked about now in relation to surveillance and privacy and the NSA, that actually was not the focal point at all of the project. It was very much about how biometrics are standardizing how you account for identity at a global, technical scale. To do that, that requires certain processes of abstraction, certain kinds of averaging... I became really

interested in how that kind of standardization was effecting queer people, people of color, transgender people, broad sets of minoritarian populations.

The much more basic issue of identification standardization...is the precondition for surveillance to even happen because for global surveillance to ramp up, you have to have technical protocols that are congruent with one another. That's part of the standardization that biometrics are a part of, that standardizes the face, the iris, the fingerprint, etc., in a way that can be shared between global networks, between countries, private security companies, militaries.

What are the implications of biometric technologies being primarily implemented and advanced by security, law enforcement, and other government agencies and affiliates?

I get the sense that we're living in a culture now where more and more, we're interested in being able to fully quantify certain things in relation to identification, that historically have always remained open and vague. I think the face is a great example of that. As we move towards this belief in total quantification, what happens is you annihilate all alterity. All alterity ["otherness"] exists within the cracks and fissures of quantification...Now we're at a moment where biometrics have so deeply and broadly changed what a face means. All the different ways that the face is a quantitative surface permeates through the world today.

I think one of the things that

I think one of the things that
you're seeing, when you ask
about the potential

ramifications of this, is you're seeing a really odd return to
pseudo-scientific endeavors of the 19th century. Things like
anthropometry, physiognomy, phrenology, methods that were
popularized by Alphonse Bertillon, Cesare Lombroso, Francis
Galton, certain criminologists who would measure criminal skulls
to say, "Here's what the average criminal skull looks like."

You're seeing a really weird history-repeating-itself moment with
things like that coming back, but of course they're executed under
the guise of high-tech biometrics, so they're not as questioned
because there's this high-tech sheen to these technologies that I
think a lot of people believe are utterly scientifically objective. I
think that's one of the central problems, that biometrics propagate
a certain way of understanding identity where you can scan the
surface of the body digitally, fully quantify it, and gain some kind
of core truth about a person. And you now see that permeating in
a lot of different ways.

I'm finishing a book right now that's on all of this, called
Informatic Opacity...Opacity is a philosophical concept that was
developed by the Caribbean philosopher and poet Édouard
Glissant. He has a really beautiful passage, "We must clamor for
the right to opacity for everyone." He's writing from Martinique in
this post-colonial context. His argument is about maintaining the
opacity of the other, respecting the opacity of the other person,
not thinking that another person could ever be fully transparent to

you, that, for Glissant, is a deeply anti-imperialist political project.

How has opacity grown more and more difficult to protect under the continued growth of visual and information surveillance?

Certain countries around the world implement biometric programs for all citizens. India was one of the first countries to do this. Another could just be living in an urban environment, where you feel like surveillance is totalized. London is a good example of that. There are so many networks of machines and humans capturing our data. We're being told by various governments what it means in particular ways. That has consequences. Some people choose to believe that and some people don't.

I think it's a lot harder to actually try to maintain that opacity that Glissant is talking about, more than ever. But at the same time, you just have to look to social movements for very clear articulations of opacity as a political project. That's why I was so personally interested in the masks, and why I worked with protest masks in my project, because the protest mask today--whether it's the Zapatistas, or Anonymous, or Pussy Riot, or Black Bloc--that to me is such a clear, powerful, popular example of investing in opacity.

And opacity for me means something very different than privacy. I was interested in how those collectives, those social movements, were wearing masks, on the one hand to evade individual detection, possibly by things like cameras, police forces, etc., but

at the same time, it's not just about preserving individuality. With social movements and collective protests with masks, there's also something very much about collective transformation. There's something positive that's happening in those moments that's not just about the negative refusal. It's also about coming together and transforming beyond the quantificative gaze of biometrics.

Is it fair to be skeptical that law enforcement's increasing willingness to implement body camera infrastructure is solely for the sake of accountability, as opposed to expanding the capacity of biometric policing and security?

I would never, ever trust the expansion of tools of visibility into the hands of the oppressors. I am so deeply against the police. That to me inspires the deepest of deepest of suspicion. A great example is the fact that with the Eric Garner case, someone did record his murder, and nothing happened with that footage. Why is it that the footage has to be somehow produced by the police for that footage to count in an official way in the criminal justice system? It just doesn't make sense to me. It puts so much agency and control over the video feed with the police officer. And there's also been incidents where they haven't had it turned on...

Of course, I would never expect the police or our governments to actually get to the root and address the baseline problematics. But it just seems to me a half-hearted gesture. Also you can read it as this gesture of, "Oh, this is going to be good for the public. We can see police encounters with people and hold them accountable."

But I think you can also read it in a cynical way: “Now, the police state just go to extend its surveillance capabilities.” I also read statistics about how less people are willing to file a complaint if an incident has been recorded. It just seems very clearly to be not necessarily about protecting citizens, but about increasing surveillance.

Does anyone benefit from a society that universally polices biometrically?

The short-handed answer would be the oppressors. To be a bit more specific, private security companies benefit because, of course, biometrics is a perfect neoliberal technology. Its development is not just happening with the state and the military. There’s a lot of commercial interest and investment in developing biometric technologies. Biometrics have also spilled out into the domestic realm. You have biometrics in computer games. You have creative biometric software platforms that are emerging.

There’s a lot of money to be made in the biometrics industry. At this point, it’s a multi-billion dollar industry. You’re either going to make money off of it in the private commercial sector, or you believe in some kind of imperial surveillance agenda and you feel like you’re gaining something from it by turning the world into a totalized surveillance society. ●

#surveillance #biometrics #masks #pseudoscience