SRILANKA Guardian ENGLISH

We See It All : A perfect architecture of control

Jon Fasman

February 1, 2021

What the War on Drugs has done for police militarization, the War on Terror is now doing for police intelligence gathering, and the privacy of millions of Americans is at risk. — **Adam Bates, CATO INSTITUTE**

Sometimes the future reveals itself as the present.

On February 10, 2020, I flew from New York to Las Vegas. The Democratic primary campaign had begun in earnest. As The Economist's Washington correspondent and a co-host of our new American politics podcast, Checks and Balance, I was on the road nearly every week from just after New Year's Day until Covid-19 shut everything down. I had been in New Hampshire the previous week and Iowa before that, and I was about to spend three days in Nevada, followed by five in South Carolina—after a brief stop at home to do some laundry and make sure my wife and kids still recognized me and hadn't changed the locks.

Delta's cross-country and international flights both leave from the same terminal at JFK. Nearly all the gates had a placard advertising Delta's facial-recognition boarding—blue, tall, and thin, with an outline of a face captured by the four corners of a digital camera's viewfinder. "ONE LOOK AND YOU'RE ON," it blared above the picture. A banner just below read, "You can now board your flight using Delta Biometrics, a new way to more seamlessly navigate the airport." And, in tiny type at the bottom, down at foot level: "Boarding using facial recognition technology is optional. Please see an agent with any questions or for alternative procedures. Visit delta.com to view our Privacy Policy."

About eight months earlier I had flown to Quito through Delta's biometric terminal in Atlanta. Facial recognition was a strange novelty: the cameras weren't working; most people boarding my flight, including me, walked right past them and had their tickets checked by a flight attendant. But apparently it worked well enough—or soon would work well enough—for Delta to roll it out more aggressively. I had noticed facial-recognition gates in Minneapolis and Detroit; in late 2019, Delta announced it would install them in Salt Lake City. Some 93 percent of customers boarded without issue, Delta said in a press release, and 72 percent preferred it to standard boarding.

Signs of Delta's ambition can be found in the banner text below the picture, which mentions not just boarding, but the ability to "more seamlessly navigate the airport." And indeed, Delta's press release touted its "curb-to-gate facial recognition": you can use your face to check in for your flight, check luggage, go through security, and board your plane. It's all very convenient. If you've traveled internationally, the airlines already have your passport picture on file—either in their own database or accessible in one built by Customs and Border Protection.

My feeling about this program is clear: I opt out, and I hope, after reading this book, that you will too. Facial recognition imperils our civil liberties. Volunteering to use it normalizes it. The more you choose to use it, the more it will be used in ways and places that you do not choose. Whenever you have the option to avoid using it, you should take that option; you should do everything you can to slow facial recognition's spread.

After I posted a picture of Delta's placard online, a friend commented that at least Delta gave passengers the choice: he had flown Singapore Airlines to Tokyo and was required to board using facial recognition. That was relatively new: until July 2017, I was based in Singapore for The Economist and flew Singapore Airlines several times each month. They did not then use facial recognition. Future as present.

When I landed in Las Vegas, I found messages from several friends asking me what I thought of that day's episode of The Daily, the New York Times's daily news podcast. I hadn't heard it, but on their advice I listened as I drove between meetings. It was the audio version of a terrific, terrifying story that Kashmir Hill had broken a couple of weeks earlier.1 Hill has been reporting on tech and privacy for about a decade; she is a perceptive, thoughtful, and engaging writer and a terrific reporter—one of the rare few whose stories tend to get better as they get longer.

This particular piece concerned a company called Clearview AI that had developed a facial-recognition app. When a user snaps and uploads a picture of anyone they see, the app tells them who that person is, thanks to Clearview's database of more than three billion images scraped from the public domain, including Facebook, YouTube, and other widely used sites. That's more than seven times as big as the FBI's facial-recognition database.

To put it another way, if you are an American, there is a one in two chance that you're in an FBI-accessible database. If you are a person in a first-world country, you're probably in Clearview's. Anyone who has Clearview's app on their phone can learn in just a few seconds who you are, and with a little sleuthing they can find out much more: your address, employer, friends, family members, and any other information about you that may be online.

As I write, hundreds of law enforcement agencies use it, as do some private companies (Clearview declined to say which ones). Some of Clearview's investors—and their friends—have used it as well: John Catsimatidis, a grocery-store magnate, happened to see his daughter on a date with someone he didn't recognize.2 He asked a waiter to take the guy's picture, which he then ran through Clearview. Within seconds, the app told him who his daughter was eating dinner with—a venture capitalist from San Francisco. Catsimatidis also used it in his stores to identify ice-cream thieves. ("People were stealing our Haagen-Dazs," he complained. "It was a big problem.")

Police love it; they say it helps them identify suspects quickly. But that convenience alone should not determine a product's worth or legality. There are many things—such as indefinite detention without charge and repealing habeas corpus—incompatible with a free and open society that would make the job of law enforcement easier.

And while police are the main customers now, nothing is stopping Clearview from selling its app to anyone who wants to buy it. Indeed, the founder of a firm that was one of Clearview's earliest investors seems resigned to this possibility. He told Hill, "I've come to the conclusion that because information constantly increases, there's never going to be privacy.… Laws have to

determine what's legal, but you can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it." If backing a technology that produces "a dystopian future or something" for everyone on earth makes him richer, then bring on the dystopian future.

Facebook and other social media sites ban others from scraping their images; Clearview did it anyway. Eric Schmidt, Google's former chairman, said in 2011 that facial recognition was "the only technology that Google has built and, after looking at it, we decided to stop," because it could be used "in a very bad way."3

Clearview's founder, Hoan Ton-That, displayed no such qualms. On The Daily, he did not sound evil; he sounded smug, callow, and indifferent. When Hill asked him about the implications of creating technology that "would herald the end of public anonymity," she wrote, he "seemed taken aback": "I'll have to think about that," he replied. One would have hoped he had done so before he invented his nightmare app.

Today, too much of our privacy, and too many of our civil liberties, depend on the whims of people like Ton-That. I'm sure that Mark Zuckerberg did not sit in his dorm room at Harvard dreaming of building a platform to help Russia undermine American democracy, but that's what he did. He more likely dreamt of building something great, and world-changing—of being successful, of making his mark on the world. He did all that too. And today, he has a fiduciary responsibility to his investors to maximize their returns. He has no such obligation to the rest of us. If our civil liberties imperil the profits of tech entrepreneurs and firms that sell surveillance technology, they are free to choose the profits every time.

That is not because they are bad people. After all, even the CEOs of crunchy, green companies probably also care more about maximizing returns than about strangers' civil liberties. But Clearview AI's technology, and the panoptic powers of modern surveillance technology more broadly, when combined with low-cost and permanent digital storage—particularly in an era of resurgent authoritarianism and institutional weakness in developed countries—imperil our democracy in a way that we've never before seen. To put it another way: our liberty isn't threatened by people buying more ethically produced yogurt or BPA-free water bottles; it is by people buying more of what Clearview is selling.

It is our responsibility to speak up for ourselves, our civil liberties, and the sort of world we want to see. Is it one in which any stranger can snap a picture of us and know everything about us? If not, it is up to us to prevent that world from emerging. In the coming chapters,

I hope to show you why and how.

This book grew out of a series of articles I reported and wrote for The Economist in the first half of 2018 about how technology is changing the justice system—in particular, police work, prisons, and sentencing.4 I chose to focus on police and tech because police are perhaps the most tangible and familiar representatives of state power. If I told you that the National Security Agency, or the Chinese government, had surveillance technology that could overhear and store every conversation we had on our cellphones, or track all of our movements, you might be outraged, but you would probably not be surprised. I hope it would both outrage and shock you, however, to learn that every police department has that ability, with virtually no oversight about how it's used. By writing about the police, I am really writing about state power.

When I was reporting, facial recognition was still largely theoretical to most people—it was not part of their lived experience. Some police departments had launched modest trial programs. A few small ones used it for limited purposes—Washington County, Oregon, began using it in 2017 to identify suspects. Today it's in airport terminals. Even if Clearview were to fold tomorrow, another firm would probably do what they are doing.

Some critics argue the technology is unreliable, and it is—particularly, in America and Europe, for people of color. But that's not really the point. Yes, facial recognition is dangerous when it's unreliable, because it risks getting innocent people arrested. But it's dangerous when it's reliable, too, because it lets governments track us in public anytime. And it is getting more and more reliable.

License plate readers can track our cars, and they can go on as many police cars and city-owned light and telephone poles as political whim and budgets will allow. Devices that mimic cellphone towers, tricking our phones into revealing who we've called, what we've texted, and what websites we've searched, can now fit in the trunk of a car.

The architecture and infrastructure of a surveillance state are here. We've seen what it looks like in China, which now has more state-owned surveillance cameras than America has people. It has used its capacity to repress free speech and expression, monitor dissidents, and keep more than a million Muslims in modern-day concentration camps—and, when not locked up, under permanent, crushing surveillance.

The single most incisive and unsettling question I heard in the year I spent reporting for this book came from Catherine Crump, a law professor at the University of California, Berkeley, who directs the school's Samuelson Law, Technology and Public Policy Clinic and codirects the Berkeley Center for Law and Technology. "We can now have a perfect architecture of control," she told me—as China does. "What democratic practices do we need to not become China?" This book is a modest effort to answer that question.