YOUR FACE BELONGS TO US: A SECRETIVE STARTUP'S QUEST TO END PRIVACY AS WE KNOW IT

Written by Kashmir Hill, Reviewed by Marc D. Alexander*

"Creepy" and "scary" are acrid words appearing in Kashmir Hill's book Your Face Belongs to Us (2023), about facial recognition software. The nightmarish scenarios Hill presents reveal a dystopian present, made possible by existing technology. The prototypical example is the weirdo at a bar snapping a photo of a woman with his smart phone. He does not know her, but with facial recognition software, he will be able to identify her, explore the web with her name and image, find her address, age, education, place of employment, lawsuits, marriages, divorces, friends, relatives — and still more images, linked to more information. Now, she is no longer an anonymous stranger.

More gravely, countries with troublesome human rights records can now photograph protesters, and instantly identify them. Those at greatest risk of losing their anonymity will be persons at the margins of what is considered to be politically or socially acceptable.

During the Occupy Wall Street protests, some protesters wore Guy Fawkes masks, appropriating the comically sinister image of the rebel with the upturned mustache who unsuccessfully tried to blow up the British Parliament in 1605. In the television series Mr. Robot, the hacktivists seeking to destroy the records of Evil Corp also wore Guy Fawkes masks. While the mask is a symbol of rebellion, it has also become a way to recover anonymity. Today, masks and reflectacles may be used in an attempt to thwart facial recognition software.

When Madison Square Garden experimented with facial recognition in 2022, lawyers with law firms that had sued its owner MSG Entertainment discovered they were on an exclusion list designed to keep them out of concert and sporting events. Kelly Conlon, a lawyer at such a firm who was shepherding a Girl Scout Troop to a Christmas Spectacular, discovered she was on the exclusion list when she entered the venue and was instantly identified.

It is technologically feasible to create a billboard that looks at you when you look at it in public. If it can instantly identify you through facial recognition, it could then tailor advertisements to your appetites and desires, through information shared with it from the sites where you shop on the Internet. In this scenario, Big Brother is a corporation not just looking at you, but interacting with you. We are already bombarded with targeted advertisements on the Internet, so perhaps you wouldn't care about being bombarded with targeted advertisements as you walk across Times Square, Union Square, or Pershing Square.

While we may want a zone of privacy to protect us from an overreaching government, as some of these examples illustrate, the erosion of privacy through facial recognition by the private sector may present an even greater problem.

The famous article by Samuel Warren and Louis Brandeis, *The Right to Privacy* (1890) 4 Harv. L.Rev. 193, advocated for the existence and protection of the right to privacy. Beyond the concern with privacy, the article is relevant to the subject of facial recognition in two ways. First, Warren and Brandeis were concerned about galloping technology, writing, "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" (*Id.* at p. 195.) Second, their concern about "mechanical devices" was galvanized by the development of the portable camera, making it possible to capture images of faces, and of persons in compromising situations.

Other historical examples chosen by Hill are rather hit or miss, as relevant for contrast as for comparison to facial recognition technology. Charles Darwin's cousin Francis Galton measured skulls, hoping to identify criminal types. A devotee of phrenology and eugenics, he veered into racist junk science. Alphonse Bertillon developed a system of measurements to keep track of a criminal, useful when combined with his signal contribution, the front and profile mugshot. Cesare Lombroso, the Italian criminologist, sought to connect physical defects to born criminals. Herman Hollerith, a statistician and United States census worker, developed a tabulating machine for punch cards, useful for processing vast amounts of information about individuals. Hollerith's punch card tabulating system became a foundational block for IBM's business.

Those antecedents were directed to discovering a criminal type, pinning down the description of a known criminal with measurements, or processing large amounts of information. But none promised the power of current facial recognition: the power to identify a stranger with the aid of a photograph, and link to all the personal information collected about that person on the Internet and in electronic databanks, stripping away the stranger's anonymity.

Hill enters the strange world of facial recognition through her reporting about Clearview AI. Clearview combined the technological brilliance of a software designer, Hoan Ton-That, the connections of Richard Schwartz, a former aide to Rudolph W. Giuliani, and financial backing from conservative libertarian Peter Thiel and others. Facial recognition has a potentially enormous market as a crime-fighting tool, and thus can be pitched to law enforcement as necessary for security.

Thiel is an interesting person to have backed the development of a software tool that can be used to eliminate anonymity and destroy privacy. After Gawker outed the very private Thiel, he provided financial backing to Hulk Hogan in his lawsuit against Gawker for invasion of privacy and other torts, because Gawker posted sections of a sex tape involving the Hulk and the wife of Bubba the Love Sponge. "I refuse to believe that journalism means massive privacy violations," said Thiel. "I think much more highly of journalists than that." Evidently, Thiel was jealous to protect his privacy and that of the Hulk.

Hill's reporting about Clearview, originally appearing in The New York Times, is sensational. At first, Clearview kept a low profile, creating obstacles to her reporting. Clearview is the "secretive startup" of the book's title. Discovering where it was located, who was involved, and the nature of its business, as well as getting the trust of participants Hill could interview proved to be a daunting project. When she finally interviewed a founder of the company, David Scalzo, he told her, "You can't ban technology. Sure, that might lead to a dystopian future or something, but you can't ban it." Explains Hill, "technical sweetness" is a term used "to describe the delight that scientists and engineers feel when they push innovations forward, which may overpower any concerns they feel about that progress."

Your Face Belongs to Us presents issues sure to trigger legal concern.

When people talk about protecting privacy, they have been concerned about protecting it from government overreach. But Hill reports that when former Senator Al Franken became interested in protecting privacy, he observed: "The Fourth Amendment doesn't apply to corporations and the Freedom of Information Act doesn't apply to Silicon Valley." Yet today information gathered by Clearview, companies such as Facebook, Amazon, and Google, is information gathered by the private sector.

The United States Constitution, while protecting our houses from unreasonable searches and seizures, as well as the quartering of troops in our homes, is ill-equipped to preserve our privacy from the private sector. Indeed, as we know, the word "privacy" does

not appear in the Constitution, nor could the Founders have anticipated the world of the Internet and facial recognition technology. Some states, like California, provide constitutional privacy protection. But state-by-state regulation of facial recognition could lead to a patchwork of rules, though the Internet is national and world-wide in scope.

The rules that govern privacy do not just vary from state to state. The rules also vary from nation to nation. "If Clearview wanted to sell its facial recognition tool in Europe — which it was trying to do [in 2020] — it had to respect one of the fundamental rights of EU citizens: 'access to data which has been collected concerning him or her, and the right to have it rectified.' The right was reinforced and strengthened in 2018, when the European Union put into effect the world's most stringent privacy law …"

Hill explains the development of accurate facial recognition software requires access to a vast databank of images. However, companies developing facial recognition software were able to "scrape" images from the Internet before we even knew it was happening. Potentially enormous databanks of images exist, collected by Facebook, Flickr, Departments of Motor Vehicles, and law enforcement. When Facebook asked us to post a photograph and collected information about us, it then had the capacity to connect our images to the information we had voluntarily provided. How are image databanks protected and regulated?

Is our face public or private? For decades, it has been permissible to photograph someone in public. Using the image for commercial purposes raises legal issues. But using facial recognition to identify criminals does not raise the same issues as a photograph taken in public to be used for commercial purposes. Facial recognition software companies such as Clearview have argued they offer information in ways that do not invade protected privacy.

Because we appear in public where our image is not private, and because so much information about us is available on the Internet already, the superpower of facial recognition is that it destroys our anonymity. We are no longer a face lost in the crowd once our face becomes the key to unlocking our identity. In turn, our identity points to the information available about us in databanks and on the Internet.

Many persons may feel, because they are not criminals, they need not worry about facial recognition eroding their privacy. Instead, they worry about crime. They have nothing to hide. Major cities such as London, New York, San Francisco, Detroit, Atlanta, Delhi, and Taiyuan are heavily surveilled by cameras. Yet, many persons might feel deeply uncomfortable to know that their images on the Internet can be connected to much information they consider to be personal.

Early versions of facial identification made mistakes identifying persons of color, perhaps the result of training the facial recognition software with a databank not representative of the population. This defect led to wrongful arrests. In every case, the person wrongfully arrested was Black.

What notice do we get that our image may be used for facial recognition identification? Here, Hill explains the "Privacy Paradox." People claim to care about their privacy. But they do not understand what they need to do to protect it. A study of profiles of Carnegie Mellon University students revealed, "[m]ore than 90 percent shared their profile photos, but only 40 percent shared their phone numbers." In 2008, academics studying how long it would take to read all privacy policies the average American agrees to in a year, estimated more than 200 hours. Under the shield of a "privacy policy" providing a company with posterior protection, companies explain to users how their information can be shared and exploited.

While there have been some legislative efforts to get a handle on the legal problems presented by facial recognition, readers will not discover any comprehensive legal solution in Hill's book. In fact, some readers will reach a conclusion foreshadowed by the book's title: privacy as we knew it is dead.

The technology of facial recognition has simply outpaced regulatory efforts. Described as "pretty basic," the facial recognition app PimEyes allows a user with a photograph to do a reverse image search and find other photographs of the same person on the Internet. With images on the Internet and web page information, one can discover a considerable amount of information about a hitherto anonymous person. In fact, PimEyes was used to identify Daniela Klette, allegedly a member of the German terrorist Red Brigade, on the lam, but hiding in plain sight, for 30 years.

Does the tool erode privacy? PimEyes's online information states, "PimEyes operates within the boundaries of European standards, emphasizing that it is a facial search system, not a facial recognition system.

This distinction underlines the technology's purpose: to analyze and locate photographic material on the internet without storing biometric data." Does "without storing biometric information" mean that it is not used? And what exactly is the difference between a facial search system and a facial recognition system? One is left feeling queasy privacy has been eroded and anonymity is no longer possible. In our social media environment, it is unlikely that a person's face has not been captured on the Internet, if only in the background of a photo. We and our friends post photos on the Internet. We walk in public, attend family gatherings, meetings, conferences, and entertainment and sports events where we can be photographed. Interested in spying on friends, enemies, and strangers? A PimEyes subscription costs $30 per month.

Despite 104 references to algorithm, algorithms, or algorithmic in the book, Hill's explanations of facial recognition technology seem rather thin. We learn that there is a difference between logic-based AI systems and "think-for-itself" AI neural networks, and that the latter marked a breakthrough for facial recognition. We are told, "[a]nywhere a lot of data exists, a neural network can theoretically crunch it." Without a better understanding of the technology, it is impossible to understand how differences among facial recognition tools might impact privacy in different ways. It is probably too much to ask for a book to satisfy a wide audience and nerds.

Peter Steiner's 1993 cartoon of a dog at the computer speaking to his furry buddy, with the caption, "On the Internet, nobody knows you're a dog," could use an update. So much of our personal information is now discoverable once our face has unlocked our identity. Living in the past, a few of us may still wish that we were anonymous. Though we may be a needle in the haystack, if our dog face appears somewhere on the Internet with our master, a vast audience will now be privy to our canine qualities.

** Marc Alexander is a California attorney and a mediator affiliated with Alternative Resolution Centers. AlexanderDisputeResolution@gmail.com*