To the Editor July 13, 2020

Facial Recognition is Evil

A **facial recognition system** is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. https://en.wikipedia.org/wiki/Facial_recognition_system

Evil [ee-vuhl] adjective
morally wrong or bad; immoral; wicked
harmful; injurious

So here, we go again, corporations and governments wanting citizens to trade our personal security and identity for an implied convenience. It is intrusive, dangerous, and it does not work.

Banning Facial Recognition Isn't Enough

Bruce Schneier, writing at New York Times:

Communities across the United States are starting to ban facial recognition technologies. In May of last year, San Francisco banned facial recognition; the neighboring city of Oakland soon followed, as did Somerville and Brookline in Massachusetts (a statewide ban may follow). In December, San Diego suspended a facial recognition program in advance of a new statewide law, which declared it illegal, coming into effect. Forty major music festivals pledged not to use the technology, and activists are calling for a nationwide ban. Many Democratic presidential candidates support at least a partial ban on the technology. These efforts are well intentioned, but facial recognition bans are the wrong way to fight against modern surveillance. Focusing on one particular identification method misconstrues the nature of the surveillance society we are in the process of building. Ubiquitous mass surveillance is increasingly the norm, in countries like China; a surveillance infrastructure is being built by the government for social control. In countries like the United States, it is being built by corporations in order to influence our buying behavior, and is incidentally used by the government.

In all cases, modern mass surveillance has three broad components: identification, correlation, and discrimination. Let us take them in turn:

Facial recognition is a technology that can be used to identify people without their knowledge or consent. It relies on the prevalence of cameras, which are becoming both more powerful and smaller, and machine learning technologies that can match the output of these cameras with images from a database of existing photos. That is just one identification technology among many. People can be identified at a distance by their heartbeat or by their gait, using a laser-based system. Cameras are so good that they can read fingerprints and iris patterns from meters away. And even without any of these technologies, we can always be identified because our smartphones broadcast unique numbers called MAC addresses. Other things identify us as well: our phone numbers, our credit card numbers, and the license plates on our cars. China, for example, uses multiple identification technologies to support its surveillance state.

Once we are identified, the data about who we are and what we are doing can be correlated with other data collected at other times. This might be movement data, which can be used to “follow” us as we move throughout our day. It can be purchasing data, Internet browsing data, or data about who we talk to via email or text. It might be data about our income, ethnicity, lifestyle, profession, and interests. There is an entire industry of data brokers who make a living analyzing and augmenting data about who we are — using surveillance data collected by all sorts of companies and then sold without our knowledge or consent.

There is a huge — and almost entirely unregulated — data broker industry in the United States that trades on our information. This is how large internet companies like Google and Facebook make their money. It is not just that they know who we are; it is that they correlate what they know about us to create profiles about who we are and what our interests are. This is why many companies buy license plate data from states. It is also, why companies like Google are buying health records, and part of the reason Google bought the company Fitbit, along with all of its data.

The whole purpose of this process is for companies — and governments — to treat individuals differently. We are shown different ads on the internet and receive different offers for credit cards. Smart billboards display different advertisements based on who we are. In the future, we might be treated differently when we walk into a store, just as we currently are when we visit websites.

The point is that it does not matter which technology is used to identify people. That there currently is no comprehensive database of heartbeats or gaits (Julian Assange put a stone in his shoe to beat this) does not make the technologies that gather them any less effective. And most of the time, it does not matter if identification is not tied to a real name. What is important is that we can be consistently identified over time. We might be completely anonymous in a system that uses unique cookies to track us as we browse the internet, but the same process of correlation and discrimination still occurs. It is the same with faces; we can be tracked as we move around a store or shopping mall, even if that tracking is not tied to a specific name. And that anonymity is fragile: If we ever order something online with a credit card, or purchase something with a credit card in a store, then suddenly our real names are attached to what was anonymous tracking information.

Regulating this system means addressing all three steps of the process. A ban on facial recognition will not make any difference if, in response, surveillance systems switch to identifying people by smartphone MAC addresses. The problem is that we are being identified without our knowledge or consent, and society needs rules about when that is permissible.

Similarly, we need rules about how our data can be combined with other data, and then bought and sold without our knowledge or consent. The data broker industry is almost entirely unregulated; there is only one law — passed in Vermont in 2018 — that requires data brokers to register and explain in broad terms what kind of data they collect. The large internet surveillance companies like Facebook and Google collect dossiers on us more detailed than those of any police state of the previous century. Reasonable laws would prevent the worst of their abuses.

Finally, we need better rules about when and how it is permissible for companies to discriminate. Discrimination based on protected characteristics like race and gender is already illegal, but those rules are ineffectual against the current technologies of surveillance and control. When people can be identified and their data correlated at a speed and scale previously unseen, we need new rules.

Today, facial recognition technologies are receiving the brunt of the tech backlash, but focusing on them misses the point. We need to have a serious conversation about all the technologies of identification, correlation, and discrimination, and decide how much we as a society want to be spied on by governments and corporations — and what sorts of influence we want them to have over our lives.

Bruce Schneier is a fellow at the Harvard Kennedy School and the author, most recently, of "Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World."

Weaknesses and Ineffectiveness

Compared to other biometric techniques, face recognition may not be most reliable and efficient. Quality measures are very important in facial recognition systems as large degrees of variations are possible in face images. Factors such as illumination, expression, pose and noise during face capture can affect the performance of facial recognition systems. Among all biometric systems, facial recognition has the highest false acceptance and rejection rates, thus questions have been raised on the effectiveness of face recognition software in cases of railway and airport security.

Face recognition is less effective if facial expressions vary. A smile or frown can render the system ineffective. This is why you are told not to smile for your driver's license photo.

Data privacy is the main concern when it comes to storing biometrics data in companies. Data stores about face or biometrics can be accessed by the third party if not stored properly or hacked.

Using crime fighting as an excuse can be disproved by the notion that when the public is regularly told that they are under constant video surveillance with advanced face recognition technology, this fear alone can reduce the crime rate, whether the face recognition system technically works or does not. Regardless of if the technology itself works, the user's perception of the technology does.

School bus companies cannot afford to put cameras in every bus, but the box that holds the camera _is_ in every bus. The kids never know if there is a camera in there or not.

Systems are often advertised as having accuracy near 100%; this is misleading as the studies often use much smaller sample sizes than would be necessary for large-scale applications. Because facial recognition is not completely accurate, it creates a list of potential matches. A human operator must then look through these potential matches and studies show the operators pick the correct match out of the list only about half the time. This causes the issue of targeting the wrong suspect.

https://en.wikipedia.org/wiki/Facial_recognition_system

Twitter Tells Facial Recognition Trailblazer To Stop Using Site's Photos

A mysterious company that has licensed its powerful facial recognition technology to hundreds of law enforcement agencies is facing attacks from Capitol Hill and from at least one Silicon Valley giant. Twitter sent a letter this week to the small start-up company, Clearview AI, demanding that it stop taking photos and any other data from the social media website "for any reason" and delete any data that it previously collected, a Twitter spokeswoman said. The cease-and-desist letter, sent on Tuesday, accused Clearview of violating Twitter's policies.

The New York Times reported last week that Clearview had amassed a database of more than three billion photos from social media sites -- including Facebook, YouTube, Twitter and Venmo -- and elsewhere on the Internet. The vast database powers an app that can match people to their online photos and link back to the sites the images came from. The app is used by more than 600 law enforcement agencies, ranging from local police departments to the F.B.I. and the Department of Homeland Security. Law enforcement officials told The Times that the app had helped them identify suspects in many criminal cases. It is unclear what social media sites can do to force Clearview to remove images from its database. "In the past, companies have sued websites that scrape information, accusing them of violating the Computer Fraud and Abuse Act, an anti-hacking law," notes the NYT. "But in September, a federal appeals court in California ruled against LinkedIn in such a case, establishing a precedent that the scraping of public data most likely doesn't violate the law."

https://yro.slashdot.org/story/20/01/23/0118250/twitter-tells-facial-recognition-trailblazer-to-stop-using-sites-photos

"Coded Bias": New Film Looks at Fight Against Racial Bias in Facial Recognition & AI Technology

A new documentary looks at the dangers of artificial intelligence and its increasing omnipresence in daily life, as new research shows that it often reflects racist biases. Earlier this month, Cambridge, Massachusetts, became the latest major city to ban facial recognition technology, joining a growing number of cities, including San Francisco, to

ban the artificial intelligence, citing flawed technology and racial and gender bias. A recent study also found that facial recognition identified African-American and Asian faces incorrectly 10 to 100 times more than white faces. The film “Coded Bias” begins with Joy Buolamwini, a researcher at the MIT Media Lab, discovering that most facial recognition software does not recognize darker-skinned or female faces. She goes on to uncover that artificial intelligence is not in fact a neutral scientific tool; instead, it internalizes and echoes the inequalities of wider society.

https://sundancefestival.net/coded-bias/

Facebook To Pay $550 Million To Settle Facial Recognition Suit (nbcnews.com) 22

Facebook has agreed to pay $550 million to settle a class-action lawsuit *(Warning: source may be pay walled; alternative source)* over its use of facial recognition technology in Illinois, "giving privacy groups a major victory that again raised questions about the social network's data-mining practices," reports The New York Times. From the report: *The case stemmed from Facebook's photo-labeling service, Tag Suggestions, which uses face-matching software to suggest the names of people in users' photos. The suit said the Silicon Valley company violated an Illinois biometric privacy law by harvesting facial data for Tag Suggestions from the photos of millions of users in the state without their permission and without telling them how long the data would be kept. Facebook has said the allegations have no merit. Under the agreement, Facebook will pay $550 million to eligible Illinois users and for the plaintiffs' legal fees.*

So what we have here is a personally intrusive technology, that is likely wrong, and can put people in compromising situations. Sounds good huh?