Amazon's Facial Recognition Software Is 'Flawed, Biased and Dangerous'

After identifying 28 members of Congress as police suspects, Amazon's facial recognition AI seems to work only about 80% of the time, and yet it is being sold en masse to governments and police agencies. Even if it worked 95% of the time, the 5% who are wrongly identified are at risk of having their lives destroyed for nothing. TN Editor

A facial recognition tool that Amazon.com Inc sells to web developers wrongly identified 28 members of Congress as police suspects, in a test conducted by the American Civil Liberties Union (ACLU), the organization said on Thursday.

Amazon, in a response, said it took issue with the settings of its face ID tool during the test. The findings nonetheless highlight the risks that individuals could face if police use the technology in certain ways to catch criminals.

Since May, the ACLU and other civil rights groups have pressured Amazon to stop selling governments access to Rekognition, a powerful

image ID software unveiled in 2016 by the company's cloud-computing division.

The groups cited use of Rekognition by law enforcement in Oregon and Florida and warned that the tool could be used to target immigrants and people of color unfairly.

Their activism has kicked off a public debate. The president of Microsoft Corp, Amazon's rival which also uses facial recognition technology, called on Congress earlier this month to study possible regulations.

The ACLU said it wants Congress to enact a moratorium on use of the technology by law enforcement.

Facial recognition is already widely used in China for police purposes, and a number of start-up companies there – some valued at billions of dollars – are aggressively pursuing the technology.

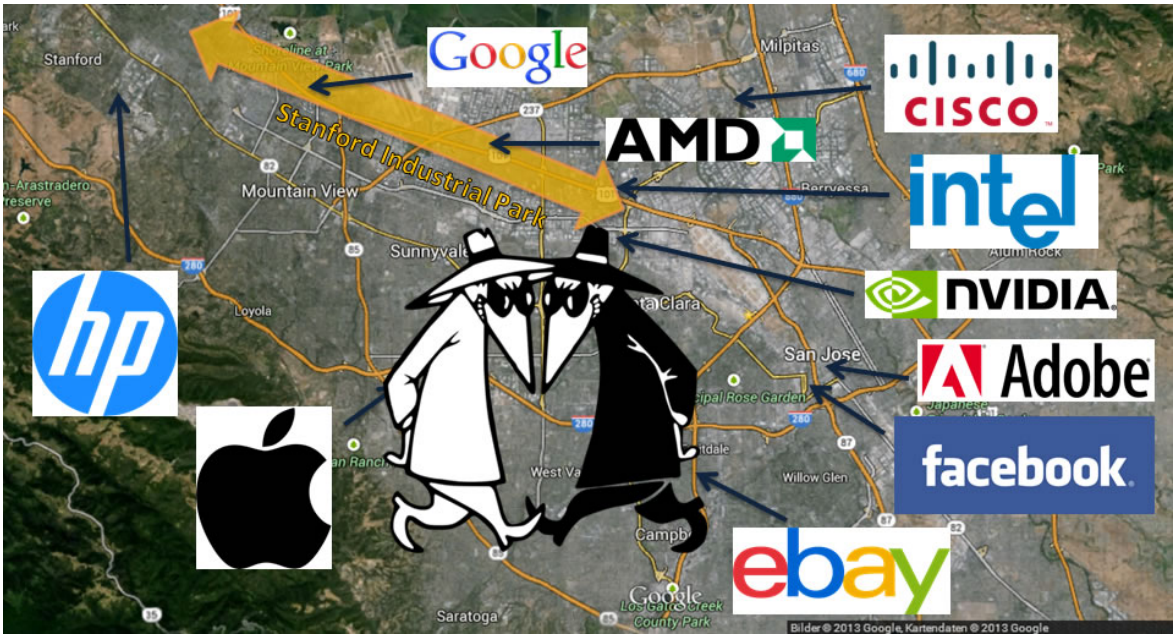
Amazon has touted a range of uses for Rekognition, from detecting offensive content online to identifying celebrities.

"We remain excited about how image and video analysis can be a driver for good in the world," a spokeswoman for Amazon Web Services said in a statement, citing its help finding lost children and preventing crimes. She said Rekognition was normally used to narrow the field for human review, not to make final decisions.

The ACLU said it paid just $12.33 to have Amazon Rekognition compare official photos of every member of the U.S. House and Senate against a database of 25,000 public arrest photos.

The technology identified "matches" for 28 members of Congress with at least 80 percent accuracy, Amazon's default setting, the ACLU said.

Read full story here…



Spy vs. Spy – Silicon Valley Is Destination Of Choice For Espionage

Just as regular citizens have no expectation of privacy for personal information, Big Tech has no expectation of privacy for their technology secrets. Why? Because its entire culture is riddled with working spies from foreign actors that feel they have as much right to technology as the ones who invented it in the first place, even if they have to steal it. TN Editor

In the fall of 1989, during the Cold War's wan and washed-out final months, the Berlin Wall was crumbling—and so was San Francisco. The powerful Loma Prieta earthquake, the most destructive to hit the region in more than 80 years, felled entire apartment buildings. Freeway overpasses shuddered and collapsed, swallowing cars like a sandpit. Sixty-three people were killed and thousands injured. And local Soviet spies, just like many other denizens of the Bay Area, applied for their share of the nearly $3.5 billion in relief funds allocated by President George H.W. Bush.

FBI counterintelligence saw an opening, recalled Rick Smith, who

worked on the Bureau's San Francisco-based Soviet squad from 1972 to 1992. When they discovered that a known Soviet spy, operating under diplomatic cover, had filed a claim, Smith and several other bureau officials posed as federal employees disbursing relief funds to meet with the spy. The goal was to compromise him with repeated payments, then to turn him. "We can offer your full claim," Smith told the man. "Come meet us again." He agreed.

But the second time, the suspected intel officer wasn't alone. FBI surveillance teams reported that he was being accompanied by a Russian diplomat known to the FBI as the head of Soviet counterintelligence in San Francisco. The operation, Smith knew, was over—the presence of the Soviet spy boss meant that the FBI's target had reported the meeting to his superiors—but they had to go through with the meeting anyway. The two Soviet intelligence operatives walked into the office room. The undercover FBI agents, who knew the whole affair had turned farcical, greeted the Soviet counterintelligence chief.

"What," he replied, "You didn't expect me to come?"

We tend to think of espionage in the United States as an East Coast phenomenon: shadowy foreign spies working out of embassies in Washington, or at missions to the United Nations in New York; dead drops in suburban Virginia woodlands, and surreptitious meetings on park benches in Manhattan's gray dusk.

But foreign spies have been showing up uninvited, to San Francisco and Silicon Valley for a very long time. According to former U.S. intelligence officials, that's true today more than ever. In fact, they warn—especially because of increasing Russian and Chinese aggressiveness, and the local concentration of world-leading science and technology firms—there's a full-on epidemic of espionage on the West Coast right now. And even more worrisome, many of its targets are unprepared to deal with the growing threat.

Unlike on the East Coast, foreign intel operations here aren't as focused on the hunt for diplomatic secrets, political intelligence or war plans. The open, experimental, cosmopolitan work and business culture of

Silicon Valley in particular has encouraged a newer, "softer," "nontraditional" type of espionage, said former intelligence officials—efforts that mostly target trade secrets and technology. "It's a very subtle form of intelligence collection that is more business connected and oriented," one told me. But this economic espionage is also ubiquitous. Spies "are very much part of the everyday environment" here, said this person. Another former intelligence official told me that, at one point recently, a full 20 percent of all the FBI's active counterintelligence-related intellectual property cases had originated in the Bay Area. (The FBI declined to comment for this story.)

Political espionage happens here, too. China, for example, is certainly out to steal U.S. technology secrets, noted former intelligence officials, but it also is heavily invested in traditional political intelligence gathering, influence and perception-management operations in California. Former intelligence officials told me that Chinese intelligence once recruited a staff member at a California office of U.S. Senator Dianne Feinstein, and the source reported back to China about local politics. (A spokesperson for Feinstein said the office doesn't comment on personnel matters or investigations, but noted that no Feinstein staffer in California has ever had a security clearance.) At the Aspen Security Forum last week, FBI director Chris Wray acknowledged the threat Chinese spying in particular poses, saying, "China from a counterintelligence perspective represents the broadest, most pervasive, most threatening challenge we face as a country."

Making it even more complicated, said multiple former U.S. intel officials, many foreign intel "collectors" in the Bay Area are not spies in the traditional sense of the term. They aren't based out of embassies or consulates, and may be associated with a state-owned business or research institute rather than an intelligence agency. Chinese officials, in particular, often cajole or outright threaten Chinese nationals (or U.S. citizens with family members in China) working or studying locally to provide them with valuable technological information.

"You get into situations where you have really good, really bright, conscientious people, twisted by their home government," said a chief security officer at a major cloud storage company whose company

maintains sensitive government contracts. U.S.-based Chinese employees of this company have had Chinese government officials attempt to "leverage" these individuals' family members in China, this person told me. The company now requires employees working on certain projects to be U.S. citizens.

And yet, it's not clear that the Bay Area—historically famous for its liberalism, and now infamous for its madcap capitalism—is prepared to handle this escalation and these new tactics. Tech firms, especially start-ups, lack incentives to report potential espionage to U.S. officials;and businesses and universities are often ignorant about the espionage threat, or so attuned to local political sensitivities they may fear being accused of stereotyping if they attempt to institute more stringent defensive security and screening measures.

As Silicon Valley continues to take over the world, the local spy war will only get hotter—and the consequences will resonate far beyond Northern California. This story is based on extensive conversations with more than half a dozen former intelligence community officials with direct knowledge of, or experience with, U.S. counterintelligence activities in the Bay Area. All requested anonymity to discuss sensitive matters more openly. A few other individuals, all of whom worked counterintelligence in the Bay Area from the early 1970s through the mid-2000s, agreed to be interviewed on the record.

As one former senior intelligence official put it: "San Francisco is a trailblazer—you see the changes there in foreign counterintelligence first. Trends emerge there." If we want to understand a world where Russian and Chinese are ramping up their spy games against the United States, then we need to pay attention to what's happening in San Francisco.

Read full story here…

The Ridiculous Myth Of Powering The Nation With Renewable Energy

Technocrats should back up a few steps and look at the foolishness of their plans: To power America with 100% renewable enerty they propose 500,000 wind turbines, 18 billion square feet of solar panels, 75 million residential rooftop systems, 50,000 wind and solar farms. The projected cost is a minimum of $15.2 Trillion. However, we are already fully powered with enough oil, natural gas and coal resources to last another 200 years. TN Editor

There is a video where critics of a proposed 2015 plan to power the US with 100% renewables lay out their case.

They are not anti-renewables but they are pro-math. They worked out the issues of spacing of large scale solar panels and wind turbines.

Jacobson agreed with them that his base proposed system will cost $15.2 trillion. If there is need for 24 hour and not 4 hours of energy storage then the cost of the plan goes up to $22.8 trillion. This assumed various efficiency and other factors were granted as improvements to the 100% renewable plan.

These critics propose all nuclear options which would cost $3 to 6.7 trillion.

Jacobson's paper appeared in the Proceedings of the National Academy of Sciences. Bernie Sanders and others pushed the proposal as a solution to climate change. The PNAS journal published a lengthy critique by environmental scientist Christopher Clack and 20 co-authors. They questioned Jacobson's assumptions and methodology, appeared Feb. 24, 2017. Jacobson launched a $10 million lawsuit against Clack but then dropped the lawsuit in Feb 2018.

The baseline value for cost of capital in the Jacobson paper is one-half to one-third of that used by most other studies. Using more realistic discount rates of 6–9% per year instead of the 3–4.5% would double the estimate of a cost of 11 cents/kWh of electricity to 22 cents/kWh, even before adding in other unaccounted for capital costs.

Both hydroelectric power and flexible load were modeled in erroneous ways and that these errors alone invalidate the study and its results.

Using Jacobson's own numbers of how many hours per days they would be able to generate power and using the Jacobson numbers for pumped hydro backup power. The Jacobson 100% renewable plan will be short 90% power in the winter.

Read full story here…