How Taylor Swift works for the NSA and Facebook spy groups with the scary future of her facial recognition tech

Surveillance at concerts is just the beginning, as fears grow around an unregulated, billion-dollar industry

Gabrielle Canon in San Francisco

@GabrielleCanon

⤢

▲ Taylor Swift has used facial recognition software for safety at events – but how far should the technology go? Photograph: Matt Winkelmeyer/TAS18/Getty Images for TAS

Taylor Swift raised eyebrows late last year when Rolling Stone magazine revealed her security team had deployed facial recognition recognition technology during her Repudiation tour to root out stalkers. But the company contracted for the efforts uses its technology to provide much more than just security. ISM Connect also uses its smart screens to capture metrics for promotion and marketing.

Facial recognition, used for decades by law enforcement and militaries, is quickly becoming a commercial tool to help brands engage consumers. Swift's tour is just the latest example of the growing privacy concerns around the largely unregulated, billion-dollar industry.

Surveillance fears grow after Taylor Swift uses face recognition tech on fans

Read more

ISM Connect uses “smart screens” to simultaneously enhance security, advertise and collect demographic data for brands. “When fans attend events they are their most passionate selves, and it is at these pinnacle and personal moments that they are open to new ideas” the company says on its website. “Our products enhance and ensure security at immense and highly visible events, while providing advertisers with a seamless, immersive platform to connect to their brand advocates.”

At Swift’s shows, ISM installed cameras behind kiosks marked as “selfie stations”, drawing concert-goers in with Swift trivia and behind the scenes footage. Their hidden cameras scanned the facial features of fans interacting with the screens, the company explained in a series of posts on its website. They also outlined how this helped generate metrics used to enhance the tour, in a post that has since been removed.

It’s unclear what exactly happened with the data next. A security contractor told Rolling Stone that the data was sent to a central command team in Nashville to be checked against a database of known Swift stalkers. The Guardian has not independently confirmed the report. Rolling Stone’s source could not be reached for comment, despite several attempts.

But ISM’s trademark for its “FanGuard” technology confirms it uses “facial recognition to identify persons of interest for security purposes”, and includes protections for the “design and development of electronic data security systems”.

And its website says, it uses those same smart screens to deliver demographic information and metrics to help educate promotors on how best to direct their marketing efforts. Both ISM and Swift’s team declined to provide further details on how the data was used.

ISM’s “data metric smart cameras” have been used at Nascar tracks, Daytona Beach’s luxury mall and at the Redskins’ FedEx field. Soon they will be at Minor League Baseball stadiums, and ISM hopes to integrate them into “smart cities”. Already, the company’s screens have captured engagement and demographic data on over 110 million event-goers at more than 100 venues, according to their website.

Like the technology itself, the industry is expanding rapidly as it becomes a profitable tool for retail and marketing companies.

Facebook Twitter Pinterest

▲ A facial recognition verification system in Dulles international airport, Virginia. Photograph: Jim Watson/AFP/Getty Images

In the next two years, facial recognition is expected to become a $9.6bn market, according to a 2015 report from Allied Research. But regulation in the burgeoning industry has failed to keep pace. Companies are expected to police themselves, and aren't hold to account for how they collect, use, and store the data.

Privacy advocates, researchers, and industry experts have all begun to sound the alarm about the lack of governmental oversight with this type of technology and the stealthy way it can be used to collect data on crowds of people. And, they warn, the industry is growing exponentially, becoming far more widely used than most people realize.

ISM says on its website that it doesn't keep the information it collects, and that biometric cameras don't produce an actual, identifiable image of someone. The company also emphasizes that signs inform crowds that they "might be filmed".

More than half of all American adults have had their likeness cataloged in databases used for facial recognition matching, according to a 2016 Georgetown law study, and a quarter of law enforcement agencies across the country have access to those databases. Mass surveillance has only gotten more pervasive since then, said Clare Garvie, a senior associate at the center on privacy and technology and one of the authors on the study.

We underestimate the threat of facial recognition technology at our peril | Cynthia Wong

→

Read more

“We knew when we were writing in late 2016 that facial recognition technology would only become more common,” she said, adding that advancements have made it even easier for law enforcement agencies or companies to collect real-time data on crowds of people without their knowledge.

“It is going to become more widespread and more advanced, especially in the absence of common sense legislation governing how it can and more importantly – how it can’t – be used,” she said. “A company such as Walmart, or Saks Fifth Avenue, or a venue or a law enforcement agency can adopt this technology and provide no notice to the public.”

“If every shopping mall, and baseball game, and convenient store is tracking every move, knows who you are, and recording what you are doing and buying and that’s all being sent to some corporate repository, that could still have serious consequences and change what it feels like to live in America” the American Civil Liberty Union’s (ACLU) senior policy analyst Jay Stanley told the Guardian in December.

Illinois is the only state with laws requiring companies and agencies to have opt-in consent before they can collect biometric information. It’s also the only state mentioned by ISM Connect

where it doesn’t offer its technology. In January, San Francisco introduced legislation that would make it the first city in the country to ban its police department from using the technology.

Facebook Twitter Pinterest

▲ At Swift’s shows, kiosks marked as ‘selfie stations’ scanned fans’ faces. Photograph: Matt Sayles/Invision/AP

In the rest of the country, companies have been left to police themselves – and many don’t consider it to be a problem. Only a quarter of Americans believe facial recognition technology should be regulated or restricted by the government, a recent survey from the Center for Data Innovation found. The number drops even more when public safety is cast as a tradeoff. Garvie says that’s likely because Americans perceive the technology largely as a convenience tool. It makes it easy to tag friends in photos on Facebook or speed through lines at TSA checkpoints.

Kelly Gates, a professor at the University of California, San Diego, and author of Our Biometric Future, a book on facial recognition and the culture of surveillance, says this attitude may come at a price.

“People’s lives – everything we do – is online,” she said. “So much data is collected all the time and automation and machine learning algorithms are coming up with ways to do things with that data, and it will affect our lives going forward.”

Mary Haskett, the co-founder of the facial recognition company Blink Identity, compared the public’s lack of understanding of the impact of facial recognition technology to Facebook’s Cambridge Analytica scandal. “[Users] didn’t realize how much in-depth information Facebook had, and more importantly how that information was being used to manipulate them,” she said. Only now, she added, these issues are quickly making their way into the physical world.

Haskett spent over a decade working for the US Department of Defense doing what she describes as “large scale national identity systems” and other programs “installed into foreign governments”. But these days, development of the tech is increasingly aimed at consumers.

“The problem is that what the technology can do is far more invasive and personal than people realize, and this will only get worse as AI technology continues to grow in capability.”