

RUNNER-UP

Privacy concerns prompt protests in California

Gabrielle Hodgson

The state's new law mandating neural-network-based screenings has driven workers statewide to vent their anger.

Public-sector employees across California have camped out in the tens of thousands to protest the state's new law requiring SAFE (Secure Assessment for Employment) screenings at all government workplaces. The screenings use a machine-learning algorithm developed by Brazil-based NeuroExpose to visually assess an employee's cognitive competence and level of stress on arriving at work (see figure 1). "Our technology is efficient, accurate, and discreet," says NeuroExpose spokesperson Julia Krieger. "The assessment process is no more invasive than walking through an airport scanner. And the data collected are automatically encrypted and secured." Governor Javier Powers, who fought for years to push the new law through, notes, "The screenings will save lives. This is about keeping workplaces safe from those who seek to cause harm."

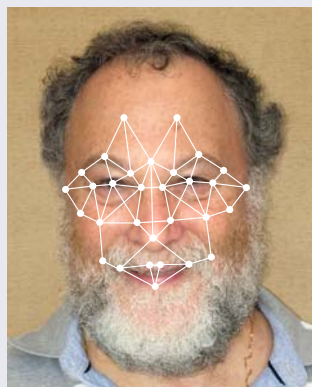


FIGURE 1. THE SAFE (Secure Assessment for Employment) screenings mandated by California rely in part on face-recognition technology. Eyebrow and lip shapes, for example, are used to assess a worker's state of mind. [Photo by Cynthia Cummings.]

Employees who will be subject to the screenings see things differently. "I'm a mother of three," says Bernadine Choi, who has spent the last four days protesting in front of the Los Angeles Employment Resource Center (figure 2 shows a similar gathering, at San Jose's Beckman Park). "Some days I may not have had enough sleep. I may look haggard. I may look like I want to kill someone. Should I have to lose my job because of that?" Others worry about the risk of racial profiling and point to the national overhaul of airport security systems that was implemented in 2111 after troubling statistics on machine-learning-triggered detentions had been revealed.

The governor's office has assured the public that protocols are in place to handle the sensitive data and minimize false positives. Unlike the systems in airports and concert halls, which are tuned to recognize imminent threats, the SAFE systems are designed around early detection. "The algorithms will analyze data from an individual employee over days, months, and years. They will pick up on changes in behavior and identify early warning signs. These systems will get people the help they need, early," Powers says.

Rise of the machine

The use of neural-network-based architectures to address public health and security concerns dates back to

Gabrielle Hodgson is a recent graduate of Harvard Law School in Cambridge, Massachusetts, and now works at White & Case in Palo Alto, California, where she assists companies with technology transitions.



FIGURE 2. PROTEST SCENES such as this one in San Jose played out across California after the legislature passed a law requiring state employees to submit to regular screenings at the workplace. The protesters regard the screenings as an unreliable invasion of privacy. The current craze for early 21st-century fashion is evident in the dress of the demonstrators. [Occupy Wall Street photo, 30 September 2011, by David Shankbone.]

the 2030s, when researchers at Caltech announced a system that could analyze body language to achieve a 30% reduction in false negatives for drug detection at border crossings.¹ Paired with facial-recognition technology, later developments based on that system eventually replaced human-conducted screenings at airports and immigration checkpoints—though not without setbacks, as the 2111 revelations showed. A team of physicists at the Perimeter Institute for Theoretical Physics, the facility that now hosts the annual International Summit on Global Data Sharing and Protection, adapted the Caltech system in 2049 in their pioneering application of quantum machine learning to screen blood for contagious diseases.² Their innovations quickly developed into the elaborate global network for disease tracking and containment that exists today.

Indeed, critics of the SAFE protests point to the hysteria around the first body scanners empowered to issue quarantine warrants and deny access to public spaces to people identified as disease carriers. “Back in the 2050s, there was a lot of fear of those scanners. People thought they wouldn’t be allowed onto flights because of a runny nose,” writes historian Angela Fazel in her

book *Quantum Machine Learning and the Rise of the World Nation* (MIT Press, 2113). “The technology had a rocky start, but in the end none of the fears held up. People found that they were less sick and they liked the fact that ‘someone’ was looking out for their health.” Fazel observes that tracking health and contagion trends also ushered in a revived attention to public health in the US. “There was fresh evidence to show that each individual is healthier when the population as a whole is healthier,” she notes. “Absent machine learning, universal health care in this country may never have been achieved.”

Great power, great responsibility

Ernesto Gregory, at the Center for Policy and Human Studies, says the fact that personal data are being

collected by governments to control and regulate society is not itself a problem. The issue is the use and safeguarding of that data. "Data will always be collected," says Gregory. "What is done with that power of information is what matters. Power can be used for good or evil. Often, we can only tell the good from the evil in hindsight." In Gregory's view, a legal system built on safeguarding against abuse of discretionary power is key. "Data collected about people should be used for the good of the people," he insists. "This means open access to government protocols on the macro scale and anonymity on the micro scale."

In a speech to the US Congress last month on statistical thresholds for obtaining warrants to access individualized data, Gregory used self-driving cars to make his point about macro and micro accessibility. "One hundred years ago, the government was required to obtain a warrant if it wanted to put a tracking mechanism on someone's car. Now it's preposterous to think that your car is not always being tracked." After all, cars require 24/7 tracking technology to communicate with other cars on the road, to receive traffic and hazard updates, and to provide the data necessary for future planning of infrastructure and transportation routes. "These macro collections of data are available for everyone to see," Gregory concluded. "For the government to access the data on any one car, however, still requires a warrant."

A balancing act

Ensuring the protection of individualized data is the cornerstone of the 2042 International Convention on the Integrity of Privacy (ICIP), which has 156 signatories to date. The goal of the ICIP is to recognize governments' need for security and regulation programs while protecting individuals from unwarranted government intrusion.

The ICIP, however, is only a tool to help guide countries in developing their own bodies of law. "The US Supreme Court cases of the last decade have actually gone further than the convention in favoring privacy rights over government interests," says University of Chicago Law School professor Larry Sherman. "The legality of California's SAFE screenings law will make for an interesting case if it is ever challenged." Sherman argues that it is one thing to protect the integrity of privacy at airports, where people are surrounded by strangers and where secondary screenings following a primary screening are routine. But it's a whole different story to protect the integrity of privacy at a small workplace, where coworkers will notice if someone is taken aside for additional screenings or treatment.

If a challenge to SAFE does reach the Supreme Court, it will be just one in a long line of cases that have arisen from the intersection of big data and privacy. In her book, Fazel chronicles the legal battles that have played out in that arena over the past century:

By the beginning of the twenty-first century, the world was already aware of the implications big data would have on personal medicine and the design of smart buildings. Also, there was a lot of unjustified hype about things like stock-market prices and weather predictions. But no one then could have foreseen the results of big data applied to global surveillance. When the network can track your location at every moment, anywhere in the world, the world really does become smaller. The old conceptions of borders and citizenship fall away. There is cross-pollination of law and culture at a fantastic rate.

The spark that lit the fire

Fazel points to the development of the first commercially viable quantum computers as the tipping point in the big-data revolution. By 2020 quantum annealing and quantum-dot manipulation had emerged as the two most promising methods to achieve large-scale commercialization. By the late 2020s, quantum dots had won out, "but we never would have gotten there so fast without the competition between the two technologies," says Fazel. "That decade saw a smorgasbord of spin-off companies from university labs, all fighting for funding from the technology giants of the day. It was an exciting time to be a young grad student in statistical mechanics or condensed-matter physics."

Governments quickly began using dot-based systems to find solutions to traffic congestion, control crime, and analyze population statistics. "By then," Fazel explains, "the camera and sensor technologies on drones had become sophisticated enough that the largest cities in North America were under near constant daytime surveillance." Such data, coupled with quantum machine learning, opened up whole new models for how to understand and predict human patterns. As Fazel puts it, "the network knew where you were going before you did. It was a messy time of negotiating what information the government was privileged to know and what it was not."

That negotiation is far from over. The patchwork of folding chairs and coffee cups that mark the camp of protesters in front of the California State Capitol is ample evidence of the tension still at play between privacy and government interests. "It's not even about protecting my anonymity," said one protester, who asked not to be named. "It's about protecting my autonomy. I don't want some algorithm, SAFE or not, dictating what thoughts I should and should not think. What is the point of science if not to encourage independent thought?" Asked to respond, NeuroExpose's Krieger had no comment.

REFERENCES

1. R. Whitehead et al., *Science* **420**, 239 (2033).
2. J. B. Rodriguez, S. L. Baldwin, *Nature* **927**, 694 (2049).