

DOOMED TO RELY ON THE MASK?

JONATHON W. PENNEY

Advances in facial recognition technology are raising questions about privacy, but they also tell us something about the health of our democracy.

Les progrès des technologies de reconnaissance faciale soulèvent autant de questions sur la protection de la vie privée que sur la santé de nos démocraties.

On November 15, 1977, several thousand Iranian students assembled before the White House to protest a visit by the Shah of Iran. The protesters wore rudimentary masks: paper bags with holes cut for the eyes, nose and mouth. They did so mainly to protect their identities and avoid retribution for themselves and their families. Student informants for the SAVAK, then Iran's intelligence agency, were known to conduct surveillance on Iranian students abroad.

Over the next year, masked Iranian students would stage similar protests across the United States and, over time, the mask came to symbolize Iranian student resistance to the Shah's regime. But by the end of 1978, as the overthrow of the Shah seemed more likely, the protesters began to take off their masks. They feared the SAVAK far less. Though the mask had come to symbolize resistance, it was the act of removing the mask that was the defiant statement of political freedom.

Today, another mask has come to symbolize political, social and economic protest and resistance. The Guy Fawkes mask, introduced by the American film *V for Vendetta* and popularized by the hacker group Anonymous, has been adopted by anti-establishment protesters around the world, from the Occupy Wall Street protests in the US to antiregime protesters in places like Australia, Thailand, Turkey, Egypt and Brazil.

But though no doubt chosen for its association with the antiauthoritarian message of *V for Vendetta*, the mask's central purpose was the same as it had been for the Iran-

ian students: to conceal and protect personal identities. Like the Iranian students and their paper masks, the Guy Fawkes mask allowed voices to be heard that might otherwise be chilled or deterred by a threat of retribution.

Unlike the Iranian students' paper bag faces, however, the Guy Fawkes profile may be with us for the foreseeable future. Exposing your face carries a much greater risk in an age when technology is exponentially more sophisticated in identifying, tracking, locating and conducting surveillance on dissidents. In particular, we are witnessing the widespread use of facial recognition technology (FRT), capable of identifying people by their unique facial patterns.

FRT is being deployed by oppressive and authoritarian states abroad. There were some reports that the Iranian protesters who took to the streets in 2009 to show opposition to this generation of Iranian leaders were subjected to a crude FRT (certainly many had their photos taken and posted online by the security services in an attempt at identification). Improved Iranian capabilities have since led to reports that Tehran was lending facial recognition technology to Syria's embattled government in that country's ongoing civil war.

But while the availability of FRT can send shivers down the spine of those taking to the streets to challenge authorities, the growing use and expanding capabilities of the technology raise privacy questions for all citizens, who may wonder what we surrender when we go about our lives unmasked.

When we read about FRT today, it is often invoked in seemingly benign situations, like its use by Facebook to identify people in photos posted online. But border officials in Canada and the US have used forms of FRT for years, and several US police departments are already testing or deploying FRT in the field. Moreover, FRT is quickly evolving and may soon offer law enforcement or any other state,

corporate or private users the capacity to dynamically identify people in "the field" in real time.

Combine these FRT developments with emerging drone robot spy technology — ubiquitous devices using regular airspace — and you have a chilling recipe for efficiently disrupting and suppressing dissent, disorder and protest with comprehensive identification and surveillance techniques. In this light, it is surprising not that we see masks being used out there, but that we don't see more.

The risks of FRT go beyond the possibility of abuse by state authorities. Data collected and retained for FRT purposes, in public or private databases, can also be leaked, lost or stolen. The Federal Bureau of Investigation, for example, is planning a national biometric database that includes stored facial patterns and will exploit FRT to identify suspects. No doubt Canadian law enforcement will eventually follow suit.

But just as law enforcement can get facial recognition IDs wrong (the FBI has often reported a 20 percent error rate), the database would be a rich target for cybercriminals, identity thieves or foreign cyber-espionage. Government databases are not immune to hacking or compromise, as our recent experience with the Heartbleed security vulnerability aptly showed.

The debate over what to do about FRT usually revolves around whether regulation is desirable or even possible. Some argue that regulation would squelch innovation and investment in a technology that can be put to good use in fighting crime or terrorism. They argue we need to adjust our privacy norms rather than stand in the way of a technological advance.

That's not a convincing argument. It relies on a form of what Evgeny Morozov calls "technological defeatism": the misguided notion that technological advancement is inevitable and therefore action to resist it is pointless. And while innovation should be encouraged, it does not obviate the potential benefits of regulatory action, nor should it trump the rights and interests of citizens. It just means that any regulatory action ought



SHUTTERSTOCK

Exposing your face carries a much greater risk in an age when technology is exponentially more sophisticated in conducting surveillance on dissidents.

JONATHON W. PENNEY

to be thoughtful and tailored to achieve balance between encouraging innovation and privacy rights.

The Electronic Frontier Foundation in San Francisco, which advocates for civil liberties in a digital world, has proposed warrant requirements for FRT use in the US. Some US lawmakers and the Electronic Privacy Information Center, another civil liberties research group, have called for a suspension or delay of FRT use until a regulatory framework can be better developed.

These are common sense ideas that can be easily advanced in Canada. Google, for example, previously banned FRT applications for some of its devices. Surely software vendors and developers could be encouraged to delay software release until a best practices regime, if not full regulatory measures, is in place.

Beyond regulation, technological countermeasures are also being

developed. These are products, devices and methods that can disrupt or circumvent FRT. Some researchers are developing forms of facial camouflage designed to fool the technology. Adam Harvey, an artist whose work focuses on surveillance technologies, has developed a product called CV Dazzle, which claims to use “avant-garde hair-styling and makeup designs to break apart the continuity of a face.” CV Dazzle’s website claims that “since facial-recognition algorithms rely on the identification and spatial relationship of key facial features like symmetry and tonal contours, one can block detection by creating an ‘anti-face.’”

Others have developed special glasses or goggles that do likewise. These solutions are important, but as with all technological arms races, there are concerns certain FRT applications may already be sophisticated enough to defeat such countermeasures. In the end, many

researchers suggest that the most effective technology out there to disrupt FRT operations is the old-fashioned face mask.

Since we have come full circle, this should make us examine the issues raised by facial recognition in the context of politics rather than technology. The proliferation and widespread use of masks in democratic protest to fool the technology of the authorities speaks to a deeper, perhaps more disturbing point about the state of our fundamental freedoms and open society. The notion that the guise of Guy Fawkes has come to symbolize struggles for justice, rights or freedom suggests we are moving in precisely the wrong direction. As the Iranian students taught us with their anti-Shah protests, true freedom is achieved not by donning masks in order to protest, but when the political environment is tolerant enough to allow us to take them off. ■



Professional Master in Public Administration

- Prepare for future leadership roles in policy-making and management
- Strengthen your analytic, communications and research skills
- Apply new learning immediately in your workplace
- Through part-time studies with leading academics, experienced practitioners and highly motivated peers from all sectors

