Q&A: The flip side of safety is an attack on privacy—regulating face recognition technology

March 27 2024, by Marie Claire Chelini

Credit: National Academies

If you bought a phone in the past few years, chances are you barely ever type your password anymore: your face unlocks not only your phone, but

also your social media, your Duke MyChart portal and even your banking app.

While extremely convenient, the popularization of face recognition technology (FRT) isn't without risks. For the past few years, Cynthia Rudin, Earl D. McLean, Jr. Professor of Computer Science, has been part of a DHS- and FBI-sponsored National Academies of Sciences, Engineering, and Medicine committee focused on FRTs.

This committee was composed of scientists and stakeholders from a range of specialties, tasked with gathering information on FRTs' current capabilities and discussing future possibilities, societal implications and the need for stronger regulations and governance. Their recommendations have been compiled in a Consensus Study Report published earlier this year.

We chatted with Rudin, who also holds appointments as a Professor of Electrical and Computer Engineering, Statistical Science and Biostatistics and Bioinformatics, to learn about some of the consensus' key recommendations.

This interview has been edited for clarity and length.

What are some of the most critical ethical issues associated with face recognition technologies?

Privacy (i.e., surveillance) is the most critical issue. Not just from our government, but from private actors and other governments. Some countries have cameras everywhere and monitor everyone. Racial and other biases are also an issue, not just with the technology itself, but also with the way it is used.

Sometimes it feels like we hear more about the dangers of face recognition than about its advantages. What are some good and ethical uses of this technology?

FRT is incredibly useful for keeping our borders safe and allowing people to clear passport control faster. It can help identify high-risk individuals quickly, for instance, making sure bad actors don't enter a concert or other crowded venue, and it is used for identifying leads at crime scenes. There have been a lot of cases where FRT has been instrumental in solving crimes that might not have been solved without it. It's also super useful for protecting access to your phone.

What were some of the consensus' key recommendations?

The first recommendation is that the government take prompt action to mitigate potential harms from FRT. There are some obvious recommendations, such that the National Institute of Standards and Technology (NIST) continue its FRT evaluation platform, which will ensure that we know about things like racial bias in the algorithms, and that there are standards established for performance, as well as for the quality of images that can even be used with FRT (people sometimes put low quality images into FRT systems, which they shouldn't do).

We also recommended training for law enforcement officers using this technology, limits on police surveillance and community oversight of FRT.

There are a lot of recommendations, so I can't list all of them here, but the one I'm the most proud of is Recommendation 4, which I insisted was important: "New legislation should be considered to address equity, privacy, and civil liberties concerns raised by facial recognition technology, to limit harms to individual rights by both private and public actors, and to protect against its misuse."

This would limit the collection and use of large databases of faces except for very specific purposes. I think this is extremely important and I hope the government acts on it soon. I don't see any reason why someone should be able to use FRT on you if it's not for a specific safety purpose. No advertisers, no fraudsters, no one who wants to limit access to a public or semi-public place like a store or concert venue, no one wanting to chill your legal right to protest, or your ability to access health care or go to a religious institution—none of them should have access to FRT.

Although the committee generally agreed on the overall need for further regulation and occasional outlawing of FRTs, it didn't reach a unanimous recommendation on some specific technologies. Can you give an example of face recognition usage where the committee didn't reach a unanimous consensus?

We were quite confused on exactly how someone or some entity would be certified to use FRT and where training materials would come from. We did, thankfully, include a recommendation stating that legislators should consider certification, we just weren't sure who would issue it. I personally think a new entity (or many) needs to be created to figure out a certification process.

There is precedence for this—you can't just open a restaurant; you need to be certified in food safety. It should be the same thing with FRT since it impacts safety for a lot of people if you mess up—particularly if you don't keep the database safe from hackers (or people who might just want to sell it).

Can you give an example of a usage that the committee agreed should be made illegal?

It became clear that being able to pull out your phone and identify the

person walking down the street because you are curious who they are is not a benign use of FRT. So, we agreed general surveillance should be illegal. We also agreed that FRT shouldn't be used as the sole reason for arrest—it's just a lead, and more evidence is needed.

One of the committee's recommendations was to ensure that when FRTs are employed there is always "a human in the loop," and you have strongly advocated for AI to not be treated as a black box. What are some of the challenges of adding a human back into the equation?

Automated systems make mistakes, and if there's no recourse when a decision is made, that's not good. However, as you mention, working with humans can be challenging, too. They have automation bias (overtrust), where they believe whatever the machine says. They need to be trained to use the technology. They are also slower than machines and make mistakes, too.

What takeaway message would you like people to get from this consensus?

FRT is both a really important and useful technology that we can't do without in the future, and it's also incredibly dangerous. We need it for our safety. This is the key to stopping and deterring criminals. However, if we don't do anything about this technology in terms of governance, we can say goodbye to our privacy as we know it today.

If cameras are cheap and FRT is cheap, it will be too tempting and too easy for anyone (our police, private actors, other governments) to place cameras all over our communities. Imagine hiring a private investigator—cheaply—who has a record of everyone's movements in a whole city, including yours.

Do we want that to exist? Imagine a foreign government having cameras all over NYC. That probably already exists. Imagine anyone going into a synagogue or mosque being filmed as they enter and their names posted on the internet. Do we want that? How about someone getting a legal abortion and their picture being sent back to their home state where abortion is illegal?

Imagine what would happen to the witness protection program if we allow facial recognition to proliferate—it's toast. So, we need to get a grip on it before it proliferates. That's what government regulations are for.

Provided by Duke University