Feds are increasing use of facial recognition systems despite calls for a moratorium

September 2 2021, by James Hendler

Credit: Pixabay/CC0 Public Domain

Despite growing opposition, the U.S. government is on track to increase its use of controversial facial recognition technology.

The U.S. Government Accountability Office released a report on Aug. 24, 2021, detailing current and planned use of facial recognition technology by federal agencies. The GAO surveyed 24 departments and agencies—from the Department of Defense to the Small Business Administration—and found that 18 reported using the technology and 10 reported plans to expand their use of it.

The report comes more than a year after the U.S. Technology Policy Committee of the Association for Computing Machinery, the world's largest educational and scientific computing society, called for an immediate halt to virtually all government use of facial recognition technology.

The U.S. Technology Policy Committee is one of numerous groups and prominent figures, including the ACLU, the American Library Association and the United Nations Special Rapporteur on Freedom of Opinion and Expression, to call for curbs on use of the technology. A common theme of this opposition is the lack of standards and regulations for facial recognition technology.

A year ago, Amazon, IBM and Microsoft also announced that they would stop selling facial recognition technology to police departments pending federal regulation of the technology. Congress is weighing a moratorium on government use of the technology. Some cities and states, notably Maine, have introduced restrictions.

Why computing experts say no

The Association for Computing Machinery's U.S. Technology Policy Committee, which issued the call for a moratorium, includes computing professionals from academia, industry and government, a number of whom were actively involved in the development or analysis of the technology. As chair of the committee at the time the statement was

issued and as a computer science researcher, I can explain what prompted our committee to recommend this ban and, perhaps more significantly, what it would take for the committee to rescind its call.

If your cellphone doesn't recognize your face and makes you type in your passcode, or if the photo-sorting software you're using misidentifies a family member, no real harm is done. On the other hand, if you become liable for arrest or denied entrance to a facility because the recognition algorithms are imperfect, the impact can be drastic.

The statement we wrote outlines principles for the use of facial recognition technologies in these consequential applications. The first and most critical of these is the need to understand the accuracy of these systems. One of the key problems with these algorithms is that they perform differently for different ethnic groups.

An evaluation of facial recognition vendors by the U.S. National Institute of Standards and Technology found that the majority of the systems tested had clear differences in their ability to match two images of the same person when one ethnic group was compared with another. Another study found the algorithms are more accurate for lighter-skinned males than for darker-skinned females. Researchers are also exploring how other features, such as age, disease and disability status, affect these systems. These studies are also turning up disparities.

A number of other features affect the performance of these algorithms. Consider the difference between how you might look in a nice family photo you have shared on social media versus a picture of you taken by a grainy security camera, or a moving police car, late on a misty night. Would a system trained on the former perform well in the latter context? How lighting, weather, camera angle and other factors affect these algorithms is still an open question.

In the past, systems that matched fingerprints or DNA traces had to be formally evaluated, and standards set, before they were trusted for use by the police and others. Until facial recognition algorithms can meet similar standards—and researchers and regulators truly understand how the context in which the technology is used affects its accuracy—the systems shouldn't be used in applications that can have serious consequences for people's lives.

Transparency and accountability

It's also important that organizations using facial recognition provide some form of meaningful advanced and ongoing public notice. If a system can result in your losing your liberty or your life, you should know it is being used. In the U.S., this has been a principle for the use of many potentially harmful technologies, from speed cameras to video surveillance, and the USTPC's position is that facial recognition systems should be held to the same standard.

To get transparency, there also must be rules that govern the collection and use of the personal information that underlies the training of facial recognition systems. The company Clearview AI, which now has software in use by police agencies around the world, is a case in point. The company collected its data—photos of individuals' faces—with no notification.

Clearview AI collected data from many different applications, vendors and systems, taking advantage of the lax laws controlling such collection. Kids who post videos of themselves on TikTok, users who tag friends in photos on Facebook, consumers who make purchases with Venmo, people who upload videos to YouTube and many others all create images that can be linked to their names and scraped from these applications by companies like Clearview AI.

Are you in the dataset Clearview uses? You have no way to know. The ACM's position is that you should have a right to know, and that governments should put limits on how this data is collected, stored and used.

In 2017, the Association for Computing Machinery U.S. Technology Policy Committee and its European counterpart released a joint statement on algorithms for automated decision-making about individuals that can result in harmful discrimination. In short, we called for policymakers to hold institutions using analytics to the same standards as for institutions where humans have traditionally made decisions, whether it be traffic enforcement or criminal prosecution.

This includes understanding the trade-offs between the risks and benefits of powerful computational technologies when they are put into practice and having clear principles about who is liable when harms occur. Facial recognition technologies are in this category, and it's important to understand how to measure their risks and benefits and who is responsible when they fail.

Protecting the public

One of the primary roles of governments is to manage technology risks and protect their populations. The principles the Association for Computing Machinery's USTPC has outlined have been used in regulating transportation systems, medical and pharmaceutical products, food safety practices and many other aspects of society. The Association for Computing Machinery's USTPC is, in short, asking that governments recognize the potential for facial recognition systems to cause significant harm to many people, through errors and bias.

These systems are still in an early stage of maturity, and there is much that researchers, government and industry don't understand about them.

Until facial recognition technologies are better understood, their use in consequential applications should be halted until they can be properly regulated.

Provided by The Conversation

Citation: Feds are increasing use of facial recognition systems despite calls for a moratorium (2021, September 2) retrieved 28 April 2024 from https://techxplore.com/news/2021-09-feds-facial-recognition-moratorium.html