Infosurhoy

As facial recognition use grows, so do privacy fears

Marta Subat

July 11, 2018

The unique features of your face can allow you to unlock your new iPhone, access your bank account or even “smile to pay” for some goods and services.

The same technology, using algorithms generated by a facial scan, can allow law enforcement to find a wanted person in a crowd or match the image of someone in police custody to a database of known offenders.

Facial recognition came into play last month when a suspect arrested for a shooting at a newsroom in Annapolis, Maryland, refused to cooperate with police and could not immediately be identified using fingerprints.

“We would have been much longer in identifying him and being able to push forward in the investigation without that system,” said Anne Arundel County police chief Timothy Altomare.

Facial recognition is playing an increasing role in law enforcement, border security and other purposes in the US and around the world.

While most observers acknowledge the merits of some uses of this biometric identification, the technology evokes fears of a “Big Brother” surveillance state.

Heightening those concerns are studies showing facial recognition may not always be accurate, especially for people of color.

A 2016 Georgetown University study found that one in two American adults, or 117 million people, are in facial recognition databases with few rules on how these systems may be accessed.

A growing fear for civil liberties activists is that law enforcement will deploy facial recognition in “real time” through drones, body cameras and dash cams.

“The real concern is police on patrol identifying law-abiding Americans at will with body cameras,” said Matthew Feeney, specialist in emerging technologies at the Cato Institute, a libertarian think tank.

“This technology is of course improving but it’s not as accurate as science fiction films would make you think.”

‘Aggressive’ deployments

China is at the forefront of facial recognition, using the technology to fine traffic violators and “shame” jaywalkers, with at least one arrest of a criminal suspect.

Clare Garvie, lead author of the 2016 Georgetown study, said that in the past two years, “facial recognition has been deployed in a more widespread and aggressive manner” in the US, including for border security and at least one international airport.

News that Amazon had begun deploying its Rekognition software to police departments sparked a wave of protests from employees and activists calling on the tech giant to stay away from law enforcement applications.

Amazon is one of dozens of tech firms involved in facial recognition. Microsoft for example uses facial recognition for US border security, and the US state of Maryland uses technology from German-based Cognitec and Japanese tech firm NEC.

Amazon maintains that it does not conduct surveillance or provide any data to law enforcement, but simply enables them to match images to those in its databases.

The tech giant also claims its facial recognition system can help reunite lost or abducted children with their families and stem human trafficking.

‘Slippery slope’

Nonetheless, some say facial recognition should not be deployed by law enforcement because of the potential for errors and abuse.

That was an argument made by Brian Brackeen, founder and the chief executive officer of the facial recognition software developer Kairos.

“As the black chief executive of a software company developing facial recognition services, I have a personal connection to the technology, both culturally and socially,” Brackeen said in a blog post on TechCrunch.

“Facial recognition-powered government surveillance is an extraordinary invasion of the privacy of all citizens—and a slippery slope to losing control of our identities altogether.”

The Georgetown study found facial recognition algorithms were five to 10 percent less accurate on African Americans than Caucasians.

Policy questions

Microsoft announced last month it had made significant improvements for facial recognition “across skin tones” and genders.

IBM meanwhile said it was launching a large-scale study “to improve the understanding of bias in facial analysis.”

While more accurate facial recognition is generally welcomed, civil liberties groups say specific policy safeguards should be in place.

In 2015, several consumer groups dropped out of a government-private initiative to develop standards for facial recognition use, claiming the process was unlikely to develop sufficient privacy protections.

Cato's Feeney said a meaningful move would be to "purge these databases of anyone who isn't currently incarcerated or wanted for violent crime."

Jennifer Lynch, an attorney with the Electronic Frontier Foundation, said that the implications for police surveillance are significant.

"An inaccurate system will implicate people for crimes they did not commit. And it will shift the burden onto defendants to show they are not who the system says they are," Lynch said in a report earlier this year.

Lynch said there are unique risks of breach or misuse of this data, because "we can't change our faces."

Evan Selinger, a philosophy professor at the Rochester Institute of Technology, says facial recognition is too dangerous for law enforcement.

"It's an ideal tool for oppressive surveillance," Selinger said in a blog post.

"It poses such a severe threat in the hands of law enforcement that the problem cannot be contained by imposing procedural safeguards."

The unique features of your face can allow you to unlock your new iPhone, access your bank account or even "smile to pay" for some goods and services.

The same technology, using algorithms generated by a facial scan, can allow law enforcement to find a wanted person in a crowd or match the image of someone in police custody to a database of known offenders.

Facial recognition came into play last month when a suspect arrested for a shooting at a newsroom in Annapolis, Maryland, refused to cooperate with police and could not immediately be identified using fingerprints.

"We would have been much longer in identifying him and being able to push forward in the investigation without that system," said Anne Arundel County police chief Timothy Altomare.

Facial recognition is playing an increasing role in law enforcement, border security and other purposes in the US and around the world.

While most observers acknowledge the merits of some uses of this biometric identification, the technology evokes fears of a "Big Brother" surveillance state.

Heightening those concerns are studies showing facial recognition may not always be accurate, especially for people of color.

A 2016 Georgetown University study found that one in two American adults, or 117 million people, are in facial recognition databases with few rules on how these systems may be accessed.

A growing fear for civil liberties activists is that law enforcement will deploy facial recognition in "real time" through drones, body cameras and dash cams.

“The real concern is police on patrol identifying law-abiding Americans at will with body cameras,” said Matthew Feeney, specialist in emerging technologies at the Cato Institute, a libertarian think tank.

“This technology is of course improving but it’s not as accurate as science fiction films would make you think.”

‘Aggressive’ deployments

China is at the forefront of facial recognition, using the technology to fine traffic violators and “shame” jaywalkers, with at least one arrest of a criminal suspect.

Clare Garvie, lead author of the 2016 Georgetown study, said that in the past two years, “facial recognition has been deployed in a more widespread and aggressive manner” in the US, including for border security and at least one international airport.

News that Amazon had begun deploying its Rekognition software to police departments sparked a wave of protests from employees and activists calling on the tech giant to stay away from law enforcement applications.

Amazon is one of dozens of tech firms involved in facial recognition. Microsoft for example uses facial recognition for US border security, and the US state of Maryland uses technology from German-based Cognitec and Japanese tech firm NEC.

Amazon maintains that it does not conduct surveillance or provide any data to law enforcement, but simply enables them to match images to those in its databases.

The tech giant also claims its facial recognition system can help reunite lost or abducted children with their families and stem human trafficking.

‘Slippery slope’

Nonetheless, some say facial recognition should not be deployed by law enforcement because of the potential for errors and abuse.

That was an argument made by Brian Brackeen, founder and the chief executive officer of the facial recognition software developer Kairos.

“As the black chief executive of a software company developing facial recognition services, I have a personal connection to the technology, both culturally and socially,” Brackeen said in a blog post on TechCrunch.

“Facial recognition-powered government surveillance is an extraordinary invasion of the privacy of all citizens—and a slippery slope to losing control of our identities altogether.”

The Georgetown study found facial recognition algorithms were five to 10 percent less accurate on African Americans than Caucasians.

Policy questions

Microsoft announced last month it had made significant improvements for facial recognition “across skin tones” and genders.

IBM meanwhile said it was launching a large-scale study “to improve the understanding of bias in facial analysis.”

While more accurate facial recognition is generally welcomed, civil liberties groups say specific policy safeguards should be in place.

In 2015, several consumer groups dropped out of a government-private initiative to develop standards for facial recognition use, claiming the process was unlikely to develop sufficient privacy protections.

Cato’s Feeney said a meaningful move would be to “purge these databases of anyone who isn’t currently incarcerated or wanted for violent crime.”

Jennifer Lynch, an attorney with the Electronic Frontier Foundation, said that the implications for police surveillance are significant.

“An inaccurate system will implicate people for crimes they did not commit. And it will shift the burden onto defendants to show they are not who the system says they are,” Lynch said in a report earlier this year.

Lynch said there are unique risks of breach or misuse of this data, because “we can’t change our faces.”

Evan Selinger, a philosophy professor at the Rochester Institute of Technology, says facial recognition is too dangerous for law enforcement.

“It’s an ideal tool for oppressive surveillance,” Selinger said in a blog post.

“It poses such a severe threat in the hands of law enforcement that the problem cannot be contained by imposing procedural safeguards.”