UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

Prepared Remarks of
Commissioner Rohit Chopra[1]

Asia Pacific Privacy Authorities
54th APPA Forum

December 7, 2020

Thank you to the Asia Pacific Privacy Authorities forum for inviting me today to discuss law enforcement remedies for facial recognition abuses. I'll begin by saying that I believe the current state of facial recognition is flawed and dangerous. I support the actions taken by many cities in the United States that have instituted outright bans and moratoria. In addition, states have enacted specific protections for commercial misuse of biometric info.

While there is much more to do when it comes to reining in facial recognition, there are some laws currently on the books. So what should we do when companies violate the laws that we have?

I want to discuss two potentially unlawful practices when to facial recognition: improper collection and use of biometric information, and deceptive accuracy rates that can disproportionately harm minority groups.

It's clear that disclosure remedies and small fines will do little to deter wrongdoing given the structure of existing business model incentives. We will need to look to other remedies to advance the goal of deterrence and ensure fairness for individuals and businesses.

Improper Collection and Use of Biometric Information

Jurisdictions around the world have strengthened laws and regulations that forbid companies from using an individual's face or other biometric identifier, absent requirements such as express individual consent. While I have serious reservations about the adequacy of consent as a safeguard, it is a key feature of many laws that must be enforced.

It is important to step back and assess the incentives of their business model and why it can pay off to steal images of the faces of individuals.

[1] The views expressed below are my own and do not necessarily reflect those of the Commission or of any other Commissioner.

For some facial recognition software firms, individuals are not the customer, they're what's for sale. One typical model is to collect images of faces and then license any software to other commercial entities and law enforcement agencies.

These firms know that they can refine their algorithm by training it with more and more photos. Like a search engine, the more inputs it gets, the better it becomes. It's a race to become dominant. That means that there's a strong incentive to move as quickly as possible and amass more and more photos.

So what should regulators do when they catch them? Some agencies may seek – on a go-forward basis – to ensure that the firms actually obtain consent. But I fear this is not really a penalty, since they should have been doing that in the first place. If anything, even after the so-called sanction, they gain something valuable: an algorithm enhanced by ill-gotten data, which is theirs to keep.

One equitable path is to require forfeiture or deletion of any algorithm developed with ill-gotten images, given that it is tainted by the misconduct. While in some cases it may be technically feasible to "rewind" any development to a version prior to the misconduct, this will not always be the case. Ultimately, forfeiture or deletion is one of the few sanctions that might actually deter the incentive to engage in unlawful collection and surveillance. Given that the algorithm would be forfeited or deleted, any customers of the wrongdoer should also be released from any licensing or contractual obligations.

But what about the individuals whose biometric information was stolen? In the United States, Illinois – where Chicago is located – enacted one of the nation's first biometric data protection laws that include such requirements.

Under this law, Facebook was accused of improperly collecting and analyzing user photographs as part of their facial recognition technology development in a private class action lawsuit filed on behalf of Illinois users. Facebook settled the matter for $550 million, which will be distributed to Illinois users.

Each individual user will likely receive hundreds of U.S. dollars. It's important to redress individuals, particularly those who are more likely to experience harm. But at the same time, we must remember that Facebook retains many of the benefits from the algorithm which it can utilize across the country and potentially the whole world.

Deceptive Accuracy Claims and Harmful Discrimination

Many facial recognition software providers make claims about the accuracy of their matching algorithm. Even if they have some substantiation for accuracy, inaccuracy can be very high for particular groups leading to harmful discrimination.

Here's one example: Robert Julian-Borchak Williams was called by the Detroit Police Department. He was told he needed to report to the police station to be arrested. He thought the call was a joke. But he was soon greeted in his driveway by police officers who handcuffed him and he was taken away in front of his wife and daughters. He spent the night in jail awaiting formal charges for a crime he did not commit. As reported by Kashmir Hill of the New York Times, it turns out that Mr. Williams was falsely matched by facial recognition software. Mr. Williams is African-American.

This is not an isolated incident. In a groundbreaking analysis, the American Civil Liberties Union used Amazon's facial recognition software to compare the images of Members of the United States Congress to images collected by law enforcement when charging individuals with offenses. Twenty-eight Members of Congress were falsely matched, and were disproportionately people of color.

According to research by the U.S. National Institute of Standard and Technology, facial recognition software falsely matches individuals of Asian and African descent at ten to one hundred times the rate of false matches of those who are white. Other groups also demonstrate much higher false match rates, including for women.

The current state of facial recognition is just one of many examples where algorithmic decision-making and machine learning can reinforce harmful discrimination. Depending on the specific facts, selling facial recognition software with a misleading accuracy claim or with such a high false match rate for protected groups can constitute a violation of a number of federal and state laws.

In some cases, it can be unlawful practice to facilitate discrimination by baiting customers seeking to employ facial recognition technology that harms particular groups of citizens.

I do not believe that the answer is to simply require companies on a go-forward basis to improve their accuracy claims. This does little for affected customers and individuals, and it is difficult to verify accuracy claims and identify discriminatory effects at a point in time. Given the dangerous consequences stemming from unlawful facial recognition practices, one of the only practical remedies to address misconduct is to ban any future offering of that facial recognition technology.

Globally, we are at an inflection point when it comes to facial recognition and abuse of biometric information. Are we going to allow powerful technology firms to experiment on us without regard to invasion of privacy and harmful discrimination? When it comes to faulty matching with facial recognition, promises to do better in the future are inadequate to deter harmful conduct, and we will need to look at all of the legal tools we have to ensure meaningful accountability, so that sanctions are not simply the cost of doing business. Thank you.