Federal Trade Commission
Title: Comments on Facial Recognition Technology
Subject Category: Face Facts: A Forum on Facial Recognition Technology; Project No. P115406
Published: To Be Added
Comments Due: Tuesday, January 31, 2012

Comments on Facial Recognition Technology from Abine, Inc.

We're Abine, an online privacy startup composed of privacy advocates and experts who are worried by the emerging privacy issues associated with facial recognition. We believe that the collection, surveillance, and visibility of what used to be private information online has gotten out of hand. Invisible advertising networks and tracking technologies follow consumers across the web, building profiles of them and their activities in order to target them with ads. When consumers sign up for online accounts, websites sell their personal information to third parties. Spam emails, inclusion in harmful information databases, and identity theft often follow. From Facebook to forums, almost everything consumers do online is bought and sold to the highest bidder. We are concerned that facial recognition will become yet another avenue for privacy violations.

To empower consumers and give them more control over their online privacy, we offer several privacy solutions in an expanding collection of products and services. Our software tools block online tracking and targeted advertising, and our DeleteMe service removes our customers' personal information from public databases.

Facial recognition technology is growing quickly, often without the public's knowledge or understanding. We want to express our multi-faceted concerns about facial recognition, specifically its contribution to an ever-growing database of personal information on all of us, its ability to facilitate identity theft, and its likely chilling effects on free speech and association.

Risk 1: Even More Personal Information and Tracking Means a Greater Risk of Identity Theft

Take the massive amount of information that Google, Facebook, ad networks, data miners, and people search websites are collecting on all of us; add the info that we voluntarily provide to dating sites, social networks, and blogs; combine that with facial recognition software; and you have a world with reduced security, privacy, anonymity, and freedom. Carnegie Mellon researchers predict that this is "a world where every stranger in the street could predict quite accurately sensitive information about you (such as your SSN, but also your credit score, or sexual orientation) just by taking a picture.

Think of your personal information—name, photos, birthdate, address, usernames, email addresses, family members, and more—as pieces of a puzzle. The more pieces

a cyber criminal has, the closer he is to solving the puzzle. Maybe the puzzle is your credit card number. Maybe it's the password you use everywhere. Maybe you're your Social Security Number.

Facial recognition software is a tool that can put all these pieces together. When you combine facial recognition software with the wealth of public data about us online, you have what's called "augmented reality:" "the merging of online and offline data that new technologies make possible." You also have a devastating blow to personal privacy and an increased risk of identity theft.

Once a cyber criminal figures out your private information, your money and your peace of mind are in danger. Common identity theft techniques include opening new credit cards in your name and racking up charges, opening bank accounts under your name and writing bad checks, using your good credit history to take out a loan, and draining your bank account. More personal attacks may include hijacking your social networks while pretending to be you, reading your private messages, and posting unwanted or embarrassing things "as" you.

Carnegie Mellon researches performed a 2011 facial recognition study using off-the-shelf face recognition software called PittPatt, which was recently purchased by Google. By cross-referencing two sets of photos—one taken of participating students walking around campus, and another taken from pseudonymous users of online dating sites—with public Facebook data (things you can see on a search engine without even logging into Facebook), they were able to identify a significant number of people in the photos. Based on the information they learned through facial recognition, the researchers were then able to predict the social security numbers of some of the participants.

They concluded this merging of our online and offline identities can be a gateway to identity theft:

> If an individual's face in the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her, once her name has been (probabilistically) inferred.

We don't want to live in a world where the only way to opt-out of data collection is to live in self-imposed solitude. We shouldn't have to stay at home to avoid cameras and surveillance that will record, store, and possibly sell data about our faces.

Some statistics on identity theft from the Identity Theft Assistance Center (ITAC):

- 8.1 million adults in the U.S. suffered identity theft in 2011
- Each victim of identity theft loses an average of $4,607

- Out-of-pocket losses (the amount you actually pay, as opposed to your credit card company) average $631 per victim
- New account fraud, where thieves open new credit card accounts on behalf of their victims, accounted for $17 billion in fraud
- Existing account fraud accounted for $14 billion

We don't want to live in a world where the only way to opt-out of data collection is to live in self-imposed solitude.

Risk 2: Chilling Effects on Free Speech & Association

Facial recognition software threatens to censor what we say and limit what we do, even offline. Imagine that you're known in your community for being an animal rights activist, but you secretly love a good hamburger. You're sneaking in a double cheeseburger at a local restaurant when, without your knowledge, someone snaps a picture of you. It's perfectly legal for someone to photograph you in a public place, and aside from special rights of publicity for big-time celebrities, you don't have any rights to control this photo. This person may not have any ill intentions; he may not even know who you are. If he uploads it to Facebook, and Facebook automatically tags you in it, you're in trouble.

The same goes for the staunch industrialist caught at the grassroots protest; the pro-life female politician caught leaving an abortion clinic; the CEO who has too much to drink at the bar; the straight-laced lawyer who likes to dance at goth clubs. If anyone with a cell phone can take a picture, and any picture can be tied back to us even when the photographer doesn't know who we are, we may stop going to these places altogether. We may avoid doing anything that could be perceived as controversial. And that would be a pity, because we shouldn't have to.

Risk 3: Incursions on Physical Safety and Due Process

Perhaps most importantly, facial recognition threatens our safety. It's yet another tool in stalkers' and abusers' arsenals. See that pretty girl at the bar? Take her picture; find out everything about her; pay her a visit at home. It's dangerous in its simplicity. (And revisit our discussion of the Carnegie Mellon study above to understand why this example isn't science fiction, but a realistic possibility.)

There's a separate set of risks from facial recognition that *doesn't* do a good job of identifying targets: false identifications. An inaccurate system runs the risk of identifying, and thus detaining or arresting, the wrong people. Let's say that an airport scans incoming travelers' faces to search for known terrorists. Their systems incorrectly recognize you as a terrorist, and you're detained, searched, interrogated, and held for hours, maybe even arrested. This is precisely why Boston's Logan Airport abandoned its facial recognition trials in 2002: its systems could only identify volunteers 61.4 percent of the time.

A Special Comment on Facebook

Facebook uses facial recognition. Every tag of your face gives Facebook a better idea of what you look like.

Its software examines photos as you upload them, comparing the faces in the photos to faces of your Facebook friends. If it thinks it's got a match, it will prompt you to tag the image. It also scans your uploaded photos for known images of child pornography using a program called PhotoDNA, reporting suspected violations to the government.

Facebook got in trouble with privacy advocates when it rolled out facial recognition by default. It's since dialed it back to "Tag Suggestions," which you can choose to disable. Even if you disable it, though, Facebook still collects information about your face whenever it's tagged. Every tag gives Facebook more information about your face: how you look in glasses and accessories, makeup, profile view, your good and bad sides, and different shadows and lighting. Even if *you* don't tag yourself, your friends are giving away your facial pattern whenever *they* do.

When you consider that Facebook's 600 million members upload over 250 million photos every day, you see that they're building an empire of facial data. Rumor has it they're building a way to search for people by picture alone.

There is also a question of whether Facebook scans & cross-references uploaded photos against criminal databases. Because of their use of PhotoDNA, it seems possible that they could use the same technology to identify known or suspected criminals. An often-cited article on this topic contains a quote from Facebook's Chief Security Officer, Joe Sullivan:

> Every picture uploaded by Facebook users is run through a program called "Photo DNA," he said, to look for possible matches with offenders. The company saves the data, he said, and makes referrals to law-enforcement agencies.

Mr. Sullivan's statement suggests that Facebook initiates referrals of people who download these images to law enforcement agencies.

Because the extent and nature of Facebook's use of facial recognition on user-submitted photos is not clear, we write publicly to ask that the FTC and the media look further into this matter.

Summary of our Views

We believe that facial recognition can have both positive and negative, and we aren't advocating a wholesale ban of the technology. Rather, we're suggesting that

advances in facial recognition be kept in line with privacy considerations, such as opt-out mechanisms, more consumer control, and transparency. We realize that the most powerful arguments in favor of facial recognition concern law enforcement and security needs. However, we assert that privacy and security are not mutually exclusive; that facial recognition technology could be used to further security needs without compromising privacy rights. The two interests should be weighed against one another to accomplish what's best for consumers.