Written by **Warren Mass** on June 24, 2015

Facial Recognition Software Raises Privacy Concerns — Even in Church

Facial recognition software is now being used in an unexpected place — in churches.

Regular watchers of law-enforcement TV shows such as *NCIS* and *Criminal Minds* are familiar with the benefits of facial recognition software in apprehending criminals. A typical scenario involves the agency or bureau agents asking their computer experts (Abby in *NCIS* or Penelope in *Criminal Minds*) to access either private video surveillance footage or city traffic cam videos, and running the images of people found in them against master photo databases, usually from the state DMV.

The ease with which criminal or terrorist suspects are identified makes the viewer glad that such wonderful tools are available to keep us safe from serial killers and members of al-Qaeda who have infiltrated our country. However, there is a concern. While invading our citizens' privacy would always have made catching criminals easier, our forebears obviously believed that protecting the right to privacy of innocent citizens was more important than making law-enforcement's job easier. That is why they included the Fourth Amendment in the Bill of Rights, which reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

{modulepos inner_text_ad}

While the use of facial recognition software in conjunction with traffic cams and DMV databases by government agencies may evoke images from Orwell's *1984* of the government of Oceania using telescreens to keep its subjects under constant surveillance, many people are not nearly so alarmed by the use of such technology by private companies. Nevertheless, the ability of government agencies to access private databases may make people concerned even about being "tagged" in Facebook — a process in which a link is made from the photo to the person's profile.

However, an article posted online on June 23 by Kashmir Hill (a senior editor at *Fusion's Real Future*) explored an unexpected place where facial recognition software is being used — churches!

In her article, Hill reminds us that Facebook's facial recognition database is so good that it can identify you even when your face is hidden, that the FBI has entered a million photos into its facial recognition database, and that Google's new Photos app is so good at face recognition that it can identify people who are now adults in photos taken during their childhood.

And while people may expect the use of such software to identify criminals attending events at places

such as sports stadiums, perhaps the last place someone might anticipate such use is at church. Yet, notes Hill, that is exactly what is happening.

Hill quotes Moshe Greenshpan, the CEO of a facial recognition software company called Face-Six — based in Israel and Las Vegas — who says his Churchix technology is being used by 30 churches around the world. Greenshpan launched the service just four months ago and said churches are using it to identify their members and thereby keep track of attendance at church services and events. Such information would typically be used in targeting candidates for donations.

When Greenshpan declined to name any of the churches using his company's technology, Hill asked him if any of the churches are located in Texas or Illinois, the only two U.S. states that have laws requiring those using such software to obtain permission from the people being scanned, Greenshpan replied: "I prefer not to say."

In order for Churchix software to operate effectively, the church must first obtain and upload a high-quality photo of the member to enter into a master database, which the software uses to obtain a match.

When Hill asked Greenshpan if the churches let their members know how they will use the photos, he replied: "I don't think churches tell people. We encourage them to do so but I don't think they do."

On Face-Six's website, the company suggested uses for their software, including airports/border control, law enforcement, casinos, commercial use, and home security.

An article posted by *The New American* a week ago revealed how the Department of Homeland Security (DHS) is currently planning experiments using other types of video surveillance technology at airports.

The DHS plans to conduct its experiment at the Theodore Francis Green Memorial State Airport in Providence, Rhode Island, utilizing "Behavior Detection Officers (BDOs)" already employed at airports around the country. These BDOs observe passengers and "are trained to identify passengers exemplifying a discrete subset of behavioral indicators" of "malicious intent" — supposedly to prevent acts of terrorism and other crimes at our airports.

This is not a new program however. An article in CNS News on as far back as November 2013 noted that the TSA had spent approximately $900 million over the previous five years for BDOs to identify high-risk passengers but, as of that date, according to the General Accountability Office (GAO), only 0.59 percent of the passengers flagged had been arrested and among those not one was charged with terrorism.

While that report was concerned mainly with the inefficiency of the program, *The New American* article focused more on the privacy implications and the fact that the standards used to flag passengers as being suspicious were very subjective. The program also casts a very wide net in order to target very few suspects. The article noted:

> Any program that relies on spying on the behavior of all travelers to detect "malicious intent" by a few is rightly considered by many to be a breach of the proper province of government.

Those concerned about privacy object mostly to the program's videotaping of air passengers not only at security lines, but (quoting DHS's "Privacy Impact Assessment") "at designated areas throughout the airport, including a TSA security checkpoint, ticket counter, baggage claim, and airport entrance."

These videos would then be viewed by BDOs not only to identify people already suspected of criminal behavior, but anyone exhibiting "behaviors that suggest deception."

In an age when government is so intent on spying on its citizens, the ease with which personal images can be transmitted from private to government databases blurs the distinction between the two. Even those with nothing to hide might exercise caution, if they value their privacy.

Photo of facial recognition camera and infrared light: Maraparacc at en.wikipedia

Related articles:

DHS Admits to "Behavioral Detection" Video Surveillance Program at Airports

DHS, IRS, Debt Collectors Fight to Expand Use of License Plate Tracking Devices

Your Smart TV Is Spying on You

Snowden Warns Canadians About Proposed "Anti-terrorism" Law

New Police Radars Can See Through Walls

License Plate Trackers Send Passenger Photos to Police Databases

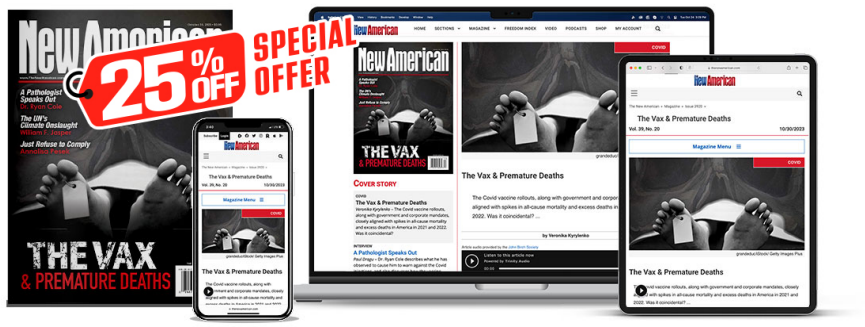
Pew Study Shows Bleak Future for Privacy Rights

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

24 Issues Per Year
Optional Print Edition
Digital Edition Access
Exclusive Subscriber Content
Audio provided for all articles
Unlimited access to past issues
Coming Soon! Ad FREE
60-Day money back guarantee!
Cancel anytime.

Subscribe