California Installs 'TrapWire' Surveillance Face Recognition

by george - RT *Wednesday, Nov 21 2012, 8:41pm*
international / prose / post

> Alarm bells recently sounded regarding a software package that could be hooked into the ubiquitous street and other surveillance camera systems of the world. Its primary capability is to RECORD in a data base (illegally in most nations) every face in its multiple view finders and then almost instantly recognise (and monitor) a face among millions in real time! This is surveillance and privacy intrusion gone mad!

One unstated factor is CLEAR, nobody asked the people, and we can be sure that the masses would not be inclined to be illegally recorded and monitored by perverts or other creeps as they went about their daily business -- the system is open to such horrendous abuse it must never be allowed to be installed. It is far too intrusive to be used by any covert group of proven sickos or fascist regulators; remember we already have indefinite detention without charge or trial passed in to law! Yes indeed, who is watching the (sick) watchers, there is no justifying the use and obvious abuse of such a system? Furthermore, all digital systems are vulnerable to hackers and corrupt operators -- the uninitiated could not imagine the boon and benefit these technologies offer State and non-State criminals.

Report from RT follows:

> **California gets face scanners to spy on everyone at once**
>
> In a single second, law enforcement agents can match a suspect against millions upon millions of profiles in vast detailed databases stored on the cloud. It’s all done using facial recognition, and in Southern California it’s already occurring.
>
> Imagine the police taking a picture: any picture of a person, anywhere, and matching it on the spot in less than a second to a personalized profile, scanning millions upon millions of entries from within vast, intricate databases stored on the cloud.
>
> It’s done with state of the art facial recognition technology, and in Southern California it’s already happening.
>
> At least one law enforcement agency in San Diego is currently using software developed by FaceFirst, a division of nearby Camarillo, California’s Airborne Biometrics Group. It can positively identify anyone, as long as physical data about a person’s facial features is stored somewhere the police can access. Though that pool of potential matches could include millions, the company says that by using the “best available facial recognition

algorithms” they can scour that data set in a fraction of a second in order to send authorities all known intelligence about anyone who enters a camera’s field of vision.

“Live high definition video enables FaceFirst to track and isolate the face of every person on every camera simultaneously,” the company claims on their website.

“Up to 4 million comparisons per second, per clustered server” — that’s how many matches a single computer wired to the FaceFirst system can consider in a single breath as images captured by cameras, cell phones and surveillance devices from as far as 100 feet away are fed into algorithms designed to pick out terrorists and persons of interest. In a single setting, an unlimited amount of cameras can record the movements of a crowd at 30-frames-per-second, pick out each and every face and then feed it into an equation that, ideally, finds the bad guys.

"I realized that with the right technology, we could have saved lives,” Joseph Rosenkrantz, president and CEO of FaceFirst, tells the Los Angeles Times. He says he dreamed up the project after the attacks of September 11, 2001 and has since invested years into perfecting it. Not yet mastered, however, is how to make sure innocent bystanders and anyone who wishes to stay anonymous is left alone as he expands an Orwellian infrastructure that allows anyone with the right credentials to comb through a crowd and learn facts and figures of any individual within the scope of a surveillance cam.

Speaking to reporters with Find Biometrics in August, Rosenkrantz said that the system is already in place in Panama, where computers there process nearly 20 million comparisons per second “using a FaceFirst matching cluster with a large number of live surveillance cameras on a scale beyond any other system ever implemented.”

“Within just a couple of seconds whoever needs to know receives an email containing all the evidence and stats about the person identified along with the video clip of them passing the camera so they may be approached then and there,” he says.

Earlier this year, RT broke the story of TrapWire, a surveillance system marketed by global intelligence firm Stratfor to law enforcement agencies across the world. Through investigation of TrapWire and its parent companies, it became apparent that surveillance devices linked to the system could be monitored from remote fusion centers with access to an endless array of cameras and databases. According to FaceFirst’s developers, their technology doesn’t need a second person to scour video feeds to find suspected terrorists. Complex algorithms instead make finding a match the job of a computer and positive IDs can be returned in under a second.

"It doesn't do me any good if I'm able to look at a face with a camera and five minutes later, there's a match," says Paul Benne, a security consultant who tells the Los Angeles Times that he recommended his clients use FaceFirst in high-security areas. "By then, the person's gone."

Rosenkrantz admits in his interview to the use of the technology at Panama’s Tocumen airport, as well as other border crossings along the perimeter of the country. The deployment of FaceFirst in the United States still begs questions concerning the relationship between security and privacy, though, and is likely to remain an issue of contention until agencies in San Diego and elsewhere explain what exactly they’re up to.

According to a report in Southern California's News 10 published this week, an unnamed law enforcement agency in San Diego County has been testing a handheld version of FacecFirst for about five months now. On the record, though, no agency in the US has been forthcoming with why it's using those specific facial scanners or even confirming it's in their arsenal of ever expanding surveillance tools.

"If they spot someone who doesn't have identification, they can take their picture with their phone and immediately get a result," Joseph Saad, business development director for FaceFirst, tells News 10.

Saad says his company predicts that "facial recognition will be in every day society" soon, perhaps before many Americans want to admit. According to filings available online, Airborne Biometrics was already cleared by the Government Services Administration (GSA) last year to have FaceFirst sold to any federal agency in the country.

"The ability to apply our technology for the advancement of our country has always been my number one goal," Rosenkrantz said in April 2011 when Airborne was awarded an IT 70 Schedule contract for FaceFirst by the GSA. Because that contact has since been signed with Uncle Sam, Rosenfratz and company can see that goal through, at least until its up for renewal in 2017, through a deal that lets them sell FaceFirst to "all federal agencies and other specified activities and agencies."

In a demonstration video on the FaceFirst website, the company touts their product as being a great addition to any acquisition device, specifically suggesting that clients consider integrating the software with tactical robots, mobile phones and surveillance drones. Coincidently, just last month the sheriff of Alameda County, California asked the US Homeland Security department for as much as $100,000 in order to have an unmanned aerial vehicles — a drone — in his agency's arsenal for the sake of protecting the security of his citizens.

Weeks earlier, Homeland Security Secretary Janet Napolitano told congressional lawmakers that she endorses the idea of sending drones to California to aid with law enforcement efforts. Pleads like the one out of Alameda have been occurring across the country in a rate considered alarming by privacy advocates, but rarely has that opposition brought into the spotlight the scary surveillance capabilities that any police agency may soon have in their hands. While the issues of Fourth Amendment erosions and privacy violations have indeed emerged, the actual abilities of surveillance devices — snagging faces from large crowds in milliseconds and sending info to the authorities — have not.

"Facial characteristics become biometric templates compared against multiple watch lists created from customer photos or massive criminal databases," the promo explains. Those lists can be custom created by law enforcement agencies to track a 'most-wanted' roster of suspected criminals but can pull from databases where any biometric information is already available or can be inputted on the fly.

Discovery of San Diego's use of FaceFirst comes just two months after the FBI announced it had already rolled out a program to upgrade its current Integrated Automated Fingerprint Identification System (IAFIS) that keeps track of citizens with criminal records across the country with one that relies on face recognition. The FBI

expects the Next Generation Identification (NGI) program will include as many as 14 million photographs by the time the project is in full swing in just two years, relying on digital images already stored on federal databases, such as the ones managed by state motor vehicle departments. In the state of New Jersey, the DMV has recently told drivers that they are not allowed to smile for driver's license photos because it could cause complications in terms of logging biometric data in their own facial recognition system.

The FBI said that, by rolling out NGI, they "will be able to provide services to enhance interoperability between stakeholders at all levels of government, including local, state, federal and international partners." The unnamed San Diego law enforcement agency already with the ability to match millions of faces in a single moment may be relying right now on that connectedness to keep track of anyone they wish.

According to an article in the Los Angeles Times last week, 70 percent of biometrics spending comes from law enforcement, the military and the government. The private sector is scooping up that scanning power too, though, with FaceFirst having already cut deals with Samsung to provide them with technology for use in closed-circuit surveillance cameras marketed to businesses. But while the Federal Trade Commission has informed companies and corporations that they need to be more transparent about how personally identifiable information is stored on their servers, the Times notes that no guidelines like that exist for law enforcement agencies, who may very well sit on mounds of intelligence without good reason.

"You don't need a warrant to use this technology on someone," Sen. Al Franken (D-Minnesota) said last year during a congressional hearing about the use of expanding surveillance technology. "You might not even need to have a reasonable suspicion that they're involved in a crime."

Aside from FaceFirst, law enforcement is using that excuse to pull data on persons — of interest and otherwise — even when their faces are protected. As RT reported recently, an ever-growing number of police departments are investing in license plate scanners that let officers identify as many as 10,000 vehicles and their registered owners in a single shift. Much like how FaceFirst can pick out dozens of suspects from a single photograph and send data to custom servers, those license plate readers can pick up the precise location of persons never suspected of a crime, making rampant invasion of privacy just collateral damage as the surveillance monster state grows larger

"The cameras will catch things you didn't see, cars you wouldn't have run, and the beauty of it is that it runs everything," Lieutenant Christopher Morgon of the Long Beach, California Police Department says in promotional material for an automated license plate recognition device manufactured by PIPS Technology.

The Federal Trade Commission has offered the security industry best practice suggestions about how long to hold onto data picked up by surveillance cameras, but safeguards for law enforcement agencies are largely absent. In the case of the scanners used to find license plates on the streets of Southern California, Jon Campbell of LA Weekly writes, "The location and photo information is uploaded to a central database, then retained for years — in case it's needed for a subsequent investigation."

Rosenkrantz says FaceFirst is experiencing triple digit growth in 2012 and expects sustainable expansion to continue throughout the next five years. By 2020, the Federal

Aviation Administration expects that as many as 30,000 drones will be operating in US airspace.

[Input 'trapwire' in search box for additional information.]

http://rt.com/usa/news/california-facefirst-surveillance-recognition-908/
