

## Smile, the Government Is Watching: Next Generation Identification

Written by John W. Whitehead

Tuesday, 18 September 2012 13:22

---

*“You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement was scrutinized.” – George Orwell, 1984*

Brace yourselves for the next wave in the surveillance state’s steady incursions into our lives. It’s coming at us with a lethal one-two punch.

To start with, there’s the government’s integration of facial-recognition software and other biometric markers into its identification data programs. The FBI’s Next Generation Identification (NGI) system is a \$1-billion boondoggle that is aimed at dramatically expanding the government’s current ID database from a fingerprint system to a facial-recognition system. NGI will use a variety of biometric data, cross-referenced against the nation’s growing network of surveillance cameras, to not only track your every move but create a permanent “recognition” file on you within the government’s massive databases.

By the time it’s fully operational in 2014, NGI will serve as a vast data storehouse of “iris scans, photos searchable with face-recognition technology, palm prints, and measures of gait and voice recordings alongside records of fingerprints, scars, and tattoos.” One component of NGI, the Universal Face Workstation, already contains some 13-million facial images, gleaned from “criminal mug shot photos” taken during the booking process. However, with major search engines having “accumulated face-image databases that in their size dwarf the earth’s population,” it’s only a matter of time before the government taps into the trove of images stored on social-media and photo-sharing Web sites such as Facebook.

Also aiding and abetting police in their efforts to track our every movement in real time is Trapwire, which allows for quick analysis of live feeds from closed-circuit-TV (CCTV) surveillance cameras. Some of Trapwire’s confirmed users are the DC police, and police and casinos in Las Vegas. Police in New York, Los Angeles, Canada, and London are also thought to be using Trapwire.

Using Trapwire in conjunction with NGI, police and other government agents will be able to pinpoint anyone by checking the personal characteristics stored in the database against images on social-media Web sites and feeds from the thousands of CCTV surveillance cameras installed throughout American cities (there are 3,700 CCTV cameras tracking the public in the

## Smile, the Government Is Watching: Next Generation Identification

Written by John W. Whitehead  
Tuesday, 18 September 2012 13:22

---

New York subway system alone), as well as data being beamed down from the more than 30,000 surveillance drones taking to the skies within the next eight years. Given that the drones' powerful facial-recognition cameras will be capable of capturing minute details, including every mundane action performed by every person in an entire city simultaneously, soon there really will be nowhere to run and nowhere to hide, short of living in a cave, far removed from technology.

NGI will not only increase sharing between federal agencies, opening up the floodgates between the Department of Homeland Security, the State Department, the Department of Justice, and the Department of Defense, but states can also get in on the action. The system was rolled out in Michigan in February 2012, with Hawaii, Maryland, South Carolina, Ohio, New Mexico, Kansas, Arizona, Tennessee, Nebraska, and Missouri on the shortlist for implementation, followed by Washington, North Carolina, and Florida in the near future.

Going far beyond the scope of those with criminal backgrounds, the NGI data includes criminals and noncriminals alike – in other words, innocent American citizens. The information is being amassed through a variety of routine procedures, with the police leading the way as prime collectors of biometrics for something as nonthreatening as a simple moving violation. For example, the New York Police Department began photographing irises of suspects and arrestees in 2010, routinely telling suspects that the scans were mandatory, despite there being no law requiring defendants to have their irises scanned. Police departments across the country are now being equipped with the Mobile Offender Recognition & Information System, or MORIS, a physical iPhone add-on that allows officers patrolling the streets to scan the irises and faces of individuals and match them against government databases.

The nation's courts are also doing their part to "build" the database, requiring biometric information as a precursor to more lenient sentences. In March 2012, New York Governor Andrew Cuomo signed a law allowing DNA evidence to be collected from anyone convicted of a crime, even if it's a nonviolent misdemeanor. New York judges have also begun demanding mandatory iris scans before putting defendants on trial. Some Occupy Wall Street protesters who were arrested for trespassing and disorderly conduct were actually assigned bail based upon whether they consented to an iris scan during their booking. In one case, a judge demanded that an Occupy protestor, who was an unlikely flight risk, pay \$1,000 bail because she refused to have her iris scanned.

Then there are the nation's public schools, where young people are being conditioned to mindlessly march in lockstep to the pervasive authoritarian dictates of the surveillance state. It was here that surveillance cameras and metal detectors became the norm. It was here, too, that

## Smile, the Government Is Watching: Next Generation Identification

Written by John W. Whitehead  
Tuesday, 18 September 2012 13:22

---

schools began reviewing social-media Web sites to police student activity. With the advent of biometrics, school officials have gone to ever more creative lengths to monitor and track students' activities and whereabouts, even for the most mundane things. For example, students in Pinellas County, Florida, are actually subjected to vein-recognition scans when purchasing lunch at school.

Of course, the government is not the only looming threat to our privacy and bodily integrity. As with most invasive technologies, the groundwork to accustom the American people to the so-called benefits or conveniences of facial recognition is being laid quite effectively by corporations. For example, a new Facebook application, Facedeals, is being tested in Nashville, Tennessee, and enables businesses to target potential customers with specialized offers. Yet another page borrowed from Stephen Spielberg's 2002 *Minority Report*, the app works like this: Businesses install cameras at their front doors that, using facial-recognition technology, identify the faces of Facebook users and then send coupons to their smartphones based upon things they've "liked" in the past.

Making this noxious mix even more troubling is the significant margin for error and abuse that goes hand in hand with just about every government-instigated program, only more so when it comes to biometrics and identification databases. Take, for example, the Secure Communities initiative. Touted by the Department of Homeland Security as a way to crack down on illegal immigration, the program attempted to match the inmates in local jails against the federal immigration database. Unfortunately, it resulted in Americans being arrested for reporting domestic abuse and occasionally flagged U.S. citizens for deportation. More recently, in July 2012, security researcher Javier Galbally demonstrated that iris scans can be spoofed, allowing a hacker to use synthetic images of an iris to trick an iris-scanning device into thinking it had received a positive match for a real iris more than 50 percent of the time.

The writing is on the wall. With technology moving so fast and assaults on our freedoms, privacy and otherwise, occurring with increasing frequency, there is little hope of turning back this technological, corporate, and governmental juggernaut. Even trying to avoid inclusion in the government's massive identification database will be difficult. The hacktivist group Anonymous suggests wearing a transparent plastic mask, tilting one's head at a 15-degree angle, wearing obscuring makeup, and wearing a hat outfitted with infrared LED lights as methods for confounding the cameras' facial-recognition technology.

Consider this, however: While the general public, largely law-abiding, continues to be pried on, spied on, and treated like suspects by a government that spends an exorbitant amount of money on the security-intelligence complex (which takes in a sizable chunk of the \$80-billion

## Smile, the Government Is Watching: Next Generation Identification

Written by John W. Whitehead

Tuesday, 18 September 2012 13:22

---

yearly intelligence budget), the government's attention and resources are effectively being diverted from the true threats that remain at large – namely, those terrorists abroad who seek, through overt action and implied threat, to continue the reign of terror in America begun in the wake of the 9/11 attacks.

*Constitutional attorney and author John W. Whitehead is founder and president of The Rutherford Institute ( [Rutherford.org](http://Rutherford.org) ). His newest book, The Freedom Wars, is available at [Amazon.com](http://Amazon.com)*

*, and he can be reached at*

*[johnw@rutherford.org](mailto:johnw@rutherford.org)*

.