The New York Times

August 29, 2013

The Face Scan Arrives

By GINGER McCALL

WASHINGTON — THE future of technological surveillance is fast approaching — and we are doing far too little to prepare ourselves.

Last week, thanks in part to documents that I and the Electronic Privacy Information Center obtained under the Freedom of Information Act, the American public learned that the Department of Homeland Security is making considerable progress on a computerized tool called the Biometric Optical Surveillance System. The system, if completed, will use video cameras to scan people in public (or will be fed images of people from other sources) and then identify individuals by their faces, presumably by cross-referencing databases of driver's license photos, mug shots or other facial images cataloged by name.

While this sort of technology may have benefits for law enforcement (recall that the suspects in the Boston Marathon bombings were identified with help from camera footage), it also invites abuse. Imagine how easy it would be, in a society increasingly videotaped and monitored on closed-circuit television, for the authorities to identify antiwar protesters or Tea Party marchers and open dossiers on them, or for officials to track the public movements of ex-lovers or rivals. "Mission creep" often turns crime-fighting programs into instruments of abuse.

At the moment, there is little to no regulation or legal oversight of technologies like the Biometric Optical Surveillance System. We need to implement safeguards to protect our civil liberties — in particular, our expectation of some degree of anonymity in public.

The Department of Homeland Security is not the only agency developing facial-surveillance capacities. The Federal Bureau of Investigation has spent more than $1 billion on its Next Generation Identification program, which includes facial-recognition technology. This technology is expected to be deployed as early as next year and to contain at least 12 million searchable photos. The bureau has partnerships with at least seven states that give the agency access to facial-recognition-enabled databases of driver's license photos.

State agencies are also participating in this technological revolution, though not
video cameras. On Monday, Ohio's attorney general, Mike DeWine, confirmed r
enforcement officers in his state, without public notice, had deployed facial-recc

software on its driver's license photo database, ostensibly to identify criminal suspects.

A total of 37 states have enabled facial-recognition software to search driver's license photos, and only 11 have protections in place to limit access to such technologies by the authorities.

Defenders of this technology will say that no one has a legitimate expectation of privacy in public. But as surveillance technology improves, the distinction between public spaces and private spaces becomes less meaningful. There is a vast difference between a law enforcement officer's sifting through thousands of hours of video footage in search of a person of interest, and his using software to instantly locate that person anywhere, at any time.

A person in public may have no reasonable expectation of privacy at any given moment, but he certainly has a reasonable expectation that the totality of his movements will not be effortlessly tracked and analyzed by law enforcement without probable cause. Such tracking, as the federal appellate judge Douglas H. Ginsburg once ruled, impermissibly "reveals an intimate picture of the subject's life that he expects no one to have — short perhaps of his wife."

Before the advent of these new technologies, time and effort created effective barriers to surveillance abuse. But those barriers are now being removed. They must be rebuilt in the law.

Two policies are necessary. First, facial-recognition databases should be populated only with images of known terrorists and convicted felons. Driver's license photos and other images of "ordinary" people should never be included in a facial-recognition database without the knowledge and consent of the public.

Second, access to databases should be limited and monitored. Officers should be given access only after a court grants a warrant. The access should be tracked and audited. The authorities should have to publicly report what databases are being mined and provide aggregate numbers on how often they are used.

We cannot leave it to law enforcement agencies to determine, behind closed doors, how these databases are used. With the right safeguards, facial-recognition technology can be employed effectively without sacrificing essential liberties.

Ginger McCall, a lawyer and privacy advocate, is the founder of Advocates for Accountable Democracy.