



Scanning, Privacy, and 802.11 Facing up to Wireless Internet Monitoring

Automated face scanners have removed another layer of privacy, but the potential for more intrusive systems is growing, as inexpensive sensors and wireless Internet connectivity make scanning cheap, mobile, and potentially widespread.

Wireless technologies offer the potential to connect camera-like sensors with Internet computing resources. Most components for a wireless scanning system are available now and wireless scanning could easily follow the growth trajectory of cell phones and personal digital assistants (PDAs). Mobile sensors have been available for some time to the military and intelligence community. Commercially available sensors are increasingly smaller and cheaper—digital camera and webcams are the most familiar of the new, cheap sensors. These turn images into bytes that can be manipulated and analyzed by computers. In the next few years, the types of sensors available on the commercial market will increase in number, but their size and price will shrink. Among them will be disposable sensors, or tiny, coin-sized sensors capable of detecting movement or changes in lighting, and multispectral sensors, such as the infrared sensors now found in some cars for nighttime driving. New sensors will be palm-sized or smaller, battery powered, and use wireless Internet connections, making them unobtrusive.

These sensors could be wirelessly connected to impressive computing power. 802.11 is not a zip code but the name given to a popular standard for connecting wireless devices to the Internet. 802.11 lets devices link into a computer network without wires (Bluetooth, another wireless standard, also links devices, but at shorter ranges). The use of standards like 802.11 and the spread of wireless networks will provide wireless connectivity to the Internet and let many devices, including sensors, access the Internet.

This computing power will come from the Internet, as it makes computers interconnected and ubiquitous. Processing power and memory will no longer be scarce resources. New software applications will take advantage of these ubiquitous computing resources and automate many tasks (allowing machine to talk to machine without human interaction). Among these tasks will be monitoring and scanning. Cheap sensors will be able automatically to collect digital data, pass it through wireless connections to high speed computing networks and large databanks for storage or processing, and then have the results returned or forwarded to a new application.

The public has some experience of the monitoring of public places with mounted cameras, such as at the 2000 Super Bowl, where spectators' faces were scanned and processed against a database of potential terrorists or criminals. Public reaction to such a monitoring system has been negative. Protestors in Tampa's nightclub district donned masks and jeered police cameras connected to a computer database of 30,000 persons. Those who dislike red-light cameras to catch speeders are also unhappy with the new systems. But the relatively large and expensive systems used in Tampa are just the forerunners of the cheaper and more advanced systems that will use wireless connections to the Internet to link sensor data to powerful computing resources.

Prior to now, a human being had to sit in front of a screen and recognize a face to connect a remotely transmitted image and an identity. Computers have automated this process. The software necessary for image recognition is commercially available. Unlike bulky video tapes, cheap computer memory means that the images collected by these sensors can be stored digitally, allowing them to be processed for less money and longer times, and allowing Internet users to access them remotely. A sensor could be mounted on a car or a telephone pole or even a person and relay its data wirelessly through the Internet to powerful computing and data services for rapid and automatic sorting and identification. Newspapers could place dozens of cheap sensors around a city to track celebrities or (with the right software) watch for newsworthy events. Publicly available information will be collected, sorted, and augmented in ways that were impossible before.

Private use of wireless sensors for identification would require commercial databases linking images and identities. These are not yet available (although most states have pictures from drivers licenses and related data on computers). Companies could begin to collect images and link them to identities, at checkout counters, for example, but the law is unclear whether this data could be sold or transferred without an individual's consent. Individuals might also willingly allow companies to collect image recognition and other biometric data to provide a means of authenticating identity for credit card use or other transactions.

Unregulated, this combination of technologies could lead to a considerable extension of knowledge about one's fellow citizens. If commercial databases link digital images of faces to identities and personal data, standing in a public place, scanning it with a wireless sensor, and receiving the biographies of very person for whom there was a 'hit' in the data base on a PDA could be possible. Ready access to information has been one of the principal attractions of the Internet and identification services that expand access to personal information will be attractive-politicians could greet every of their constituents by name if their cellphone whispers it in their ear.

There are also potential benefits to public safety. Computer monitoring of airports and other public places for the faces of parole violators or convicted criminals could increase safety. Stores and malls may want to monitor their public spaces for pickpockets and shoplifters. Credit card companies might automatically scan faces when a bill is paid, to match the purchaser and the face stored in its computers. However, computer monitoring of public spaces is chillingly reminiscent of 1984 and Big Brother.

Commercial applications of sensor data pose another set of problems. A coffee chain captures an individual's image and links that image to that person's name when he or she uses a credit card to pay for coffee. If the coffee shop obtains the individual's cellphone number or e-mail address from a public source, it could then send that person a message when a sensor records him or her walking down the street, alerting the individual to the next coffee shop.

Our legal system has not sorted out the line between private and public for these technologies. The central issue is the status of images taken in public spaces. Actions taken in the public view, where there is no reasonable expectation of privacy, are not private; they are in the public domain and unprotected. If an individual takes a picture of a crowded street, he or she needs no one's permission and owns that picture.

Current laws do impose some limits on monitoring. One cannot trespass or intrude (the legal term is "objectionable intrusion") in collecting sensor data. The data collected cannot be used for commercial or trade purposes (such as an advertisement) without an individual's consent. And if the collector is from the police or another government agency, the individual cannot be subjected to an "unreasonable search," which the Fourth Amendment prohibits.

The courts have not yet tried the test cases needed to determine what is unreasonable. Is it an unreasonable search, for example, if the cameras now mounted on many police cars are connected through the Internet to police computers so that they can identify a person with an outstanding warrant walking down the street? The person has no reasonable expectation of privacy, but instead relies on the likelihood that the police officers he encounters will not know him or her. Now, the knowledge of the police can be extended through sensor/wireless internet/computing systems. The courts have recently limited the ability of police to use sensors to look into a person's house, but appear to tolerate the monitoring of public spaces.

The courts could interpret the coffee store's collection of an individual's image and using it to send spam (a quick advertisement to one's cellphone, for example) as commercial use, which would require the individual's permission, but this would require an extension of existing law. It is unclear if the law would consider it commercial use if a company collected images of its public spaces, linked the images to identities, but kept them for internal company use and did not sell or transfer them.

This is particularly true if the person using the sensor has done something to limit expectations of privacy. Those signs on the highway saying that radar, lidar, or aircraft will monitor your speed limit your expectation of privacy. The posting of similar signs by stores, malls, and the police in other public spaces would reduce legal objection to the new monitoring.

The California legislature recently rejected a bill that would significantly curtail the use of scanning in public places, but other bills are sure to follow. The Biometric industry and facial-recognition software manufacturers have proposed regulations or principles that would require public notification of the use of scanning equipment and limitations on image databases.

The pre-wireless treatment of public action will need adjustment for the wireless Internet era. The European Union's Privacy Directive, as implemented in some countries, forbids webcams from collecting images from public spaces. It is unclear, however, that draconian restrictions are in the public interest. So far, the privacy debate in the United States has not had to confront the question of how to treat data collected in public spaces. The challenge will be to balance new

services and protections derived from this data with the "reasonable expectation" of public anonymity the public now enjoys.