The Economist

Face recognition

Anonymous no more

You can’t hide –from anybody

Jul 30th 2011

Not quite lost in the madding crowd

IF YOUR face and name are anywhere on the web, you may be recognised whenever you walk the streets –not just by cops but by any geek with a computer. That seems to be the conclusion from some new research on the limits of privacy.

For suspected miscreants, and people chasing them, face-recognition technology is old hat. Brazil, preparing for the soccer World Cup in 2014, is already trying out pairs of glasses with mini-cameras attached; policemen wearing them could snap images of faces, easy to compare with databases of criminals. More authoritarian states love such methods: photos are taken at checkpoints, and images checked against recent participants in protests.

But could such technology soon be used by anyone at all, to identify random passers-by and unearth personal details about them? A study which is to be unveiled on August 4th at Black Hat, a security conference in Las Vegas, suggests that day is close. Its authors, Alessandro Acquisti, Ralph Gross and Fred Stutzman, all at America’s Carnegie Mellon University, ran several experiments that show how three converging technologies are undermining privacy. One is face-recognition software itself, which has improved a lot. The researchers also used “cloud computing” services, which provide lots of cheap processing power. And they went to social networks like Facebook and LinkedIn, where most users post real names and photos of themselves.

In their first experiment, the researchers collected images from 5,000 profiles of people on a popular American dating site in a particular city—most of whom used pseudonyms. They fed the pictures into an off-the-shelf face-recognition programme that compared them with 280,000 images they had found by using a search engine to identify Facebook profiles from the same city. They discovered the identity of just over a tenth of the folk from the dating site.

That might not seem a big percentage, but the hit rate will get better as face-recognition software improves and more snaps are uploaded. The researchers did a second experiment: they took webcam photos of 93 students on Carnegie Mellon’s campus, with their assent. These were fed into the face-recognition software along with 250,000 photos gleaned from publicly available profiles on Facebook. About a third of students in the test were identified.

But the most striking result was from a third experiment. By mining public sources, including Facebook profiles and government databases, the researchers could identify at least one personal interest of each student and, in a few cases, the first five digits of a social security number. All this helps to explain concerns over the use of face-recognition software by the likes of Google and Facebook, which have been acquiring firms that specialise in that technology, or licensing software from them. (Google recently snapped up Pittsburgh Pattern Recognition, the firm which owns the programme the researchers used for their tests.) Privacy officials in Europe have said they will scrutinise Facebook’s use of face-recognition software to help people “tag”, or identify, friends in photos they upload. And privacy campaigners in America have made a formal complaint to regulators. (Facebook notes that people can opt out of the photo-tagging service by altering their privacy settings.)

Given the sensitivity, Google decided not to release a face-recognition search engine it had made. Eric Schmidt, the executive chairman, has said it took the decision because “people could use this stuff in a very, very bad way, as well as a good way.” But face-recognition methods may still spread. As Mr Acquisti says, sharing named photos online has “opened the floodgates” to a new, privacy-sapping world. Shutting them will be hard.