McGranahan

THE WALL STREET JOURNAL.

Face-ID Tools Pose New Risk --- Study Shows Power, Privacy Peril, of Software That Recognizes People's Features

Julia Angwin. **Wall Street Journal**. (Eastern edition). New York, N.Y.: Aug 1, 2011. pg. B.1

Abstract (Summary)

Prof. Alessandro Acquisti, the study's author, also found that about 27% of the time, using data gleaned from Facebook profiles of the subjects he identified, he could correctly predict the first five digits of their Social Security numbers. The number of matching photos that were incorrectly rejected by state-of-the-art recognition technology declined to 0.29% in 2010 from 79% in 1993, according to a study by the National Institutes of Standards and Technology.

Full Text (949 words)

As Internet giants Facebook Inc. and Google Inc. race to expand their facial-recognition abilities, new research shows how powerful, and potentially detrimental to privacy, these tools have become.

Armed with nothing but a snapshot, researchers at Carnegie Mellon University in Pittsburgh successfully identified about one-third of the people they tested, using a powerful facial-recognition technology recently acquired by Google.

Prof. Alessandro Acquisti, the study's author, also found that about 27% of the time, using data gleaned from Facebook profiles of the subjects he identified, he could correctly predict the first five digits of their Social Security numbers.

The research demonstrates the potentially intrusive power of a facial-recognition technology, when combined with publicly available personal data. The study was funded largely by a grant from the National Science Foundation, with smaller sums from Carnegie Mellon and the U.S. Army.

Paul Ohm, a law professor at University of Colorado Law School, who has read Prof. Acquisti's paper, said it shows how easy it is becoming to "re-identify" people from bits of supposedly anonymous information. "This paper really establishes that re-identification is much easier than experts think it's going to be," he said.

For his study, Prof. Acquisti used a webcam to take pictures of student volunteers, then used off-the-shelf facial-recognition software to match the students' faces with those in publicly available Facebook photos. "We call it the democratization of surveillance," he said.

The professor said the study also shows how Facebook, with its 750 million users, whose names and profile photos are automatically public, is becoming a de facto identity-verification service.

A Facebook spokesman said that Facebook profiles don't always contain pictures of people's faces. Users can choose whether "to upload a profile picture, what that picture is of, when to delete that picture," he said.

Google Chairman Eric Schmidt discussed his concerns about Facebook at the D: All Things Digital conference in June.

Facebook is "the first generally available way of disambiguating identity," he said. "Historically, on the Internet such a fundamental service wouldn't be owned by a single company. . . . I think the industry would benefit from an alternative that."

Google has been racing to create a rival social-networking service. In June, it launched Google+ to compete with Facebook. In July, Google acquired Pittsburgh Pattern Recognition, or PittPatt, the facial-recognition technology that was used in the Carnegie Mellon study.

Facebook rolled out its facial-recognition service world-wide in June. The service lets people automatically identify photos of their friends. Facebook users who don't want to be automatically identified in photos must change their privacy settings.

A Google spokesman said the company won't introduce facial-recognition technology "to our apps or product features" without putting strong privacy protections in place. At the D conference, Mr. Schmidt said Google had withdrawn a facial-recognition service for mobile phones that it considered too intrusive.

The race to acquire facial-recognition technology reflects the technology's sharp improvement in recent years. The number of matching photos that were incorrectly rejected by state-of-the-art recognition technology declined to 0.29% in 2010 from 79% in 1993, according to a study by the National Institutes of Standards and Technology.

"It's certainly not science fiction anymore," said Peter N. Belhumeur, professor of computer science at Columbia University.

One big reason for the leap forward: the wide availability of photos that people have uploaded to the Internet through social-networking sites. Previously, publicly available pictures of individuals were mostly limited to driver's-license photos, school portraits or criminal mug shots, all of which were difficult to obtain.

In the Carnegie Mellon study, 93 students agreed to be photographed using a web camera attached to a laptop. The shots were immediately uploaded to a cloud computer and compared with a database of 261,262 publicly available photos downloaded from Carnegie Mellon students' Facebook profiles.

In less than three seconds, the system found 10 possible matching photos in the Facebook database. The students confirmed their face was among the top results more than 30% of the time.

Prof. Acquisti said the research "suggests that the identity of about one-third of subjects walking by the campus building may be inferred in a few seconds combining social-network data, cloud computing and an inexpensive webcam."

He then tried to discover whether he could predict sensitive information from the Facebook profile of individuals he had identified. He exploited the fact that, after 1987, the Social Security Administration started assigning Social Security numbers in a way that inadvertently made it easier to predict them based on the person's birthdate.

Drawing from knowledge of the Social Security numbering system used in a previous experiment, Prof. Acquisti was able to predict the first five digits of the subject's nine-digit Social Security numbers 27% of the time, with just four attempts. "The chain of inferences comes from one single piece of anonymous information -- somebody's face."

The last four digits of the number also are predictable: In a 2009 paper, Prof. Acquisti showed that he could predict an entire Social Security number with fewer than 1,000 attempts for close to 10% of people born after 1988.

In June, the Social Security agency launched a new "randomized" numbering system, which will make such predictions more difficult for future generations. An agency spokesman said that even under the old system "there is no foolproof method for predicting a person's Social Security number."

As a demonstration of his latest project, Prof. Acquisti also built a mobile-phone app that takes pictures of people and overlays on the picture a prediction of the subject's name and Social Security number. He said he won't release the app, but that he wanted to showcase the power of the data that can be generated from a single photo.

Credit: By Julia Angwin

Indexing (document details)

Subjects:	State laws, Students, Research, Pattern recognition, Internet, Cloud computing, Computer science
Author(s):	Julia Angwin
Document types:	News

Publication title:	Wall Street Journal. (Eastern edition). New York, N.Y.: Aug 1, 2011. pg. B.1
Source type:	Newspaper
ISSN:	00999660
ProQuest document ID:	2412329341
Text Word Count	949
Document URL:	http://proquest.umi.com/pqdweb?did=2412329341&sid=1&Fmt=3&cl ientId=18999&RQT=309&VName=PQD