NII Special

2

Get Control of Personal Data Back in Our Hands

PrivacyVisor raises discussion on arbitrary facial recognition

The risk that personal data is used for unexpected purposes due to collection of big data and development of analytical technologies has started to be pointed out. The situation in which personal information, such as the name and address of a person in a picture, is entirely exposed independently of the person's intent from the content registered or posted on an SNS has become a reality. Is it possible to control personal data in cyberspace by one's hands? The PrivacyVisor, a tool for preventing facial detection, developed by Professor Isao Echizen, is causing a new stir in discussions on the use of big data and the protection of privacy.

Problems in Facial Recognition

Associated with the popularization of cell phones with cameras and smartphones and the expanding use of SNS, snapshots on the street and of commercial facilities are increasingly disclosed on the Internet. Even if permission is obtained from a person photographed, those who happen to appear in the picture behind the person may not have thought their pictures would be made public. Using current facial recognition technology, however, the same people can easily be identified from facial features of those in the picture. And even the date and location information can be disclosed through the information incidental to the picture. If a person can be identified, it will not be difficult to search and collect related information from information sources on the Internet. In other words, someone unknown to you will come to know what you do, when and where from a single picture in which you happened to be photographed, and even other information such as your job and friends will be revealed if various links are followed.

In addition, since practical application of wearable devices with cameras, as represented by Google Glass, has been imminent, times when the personal data of a person viewed through these devices can be revealed in real time and onsite are just around the corner.

Professor Isao Echizen at NII says, "I want people to think about what they can do to protect their privacy against the fact that their own information will spread in the cyberspace and could be used for a commercial purpose. For example, when Carnegie Mellon University experimented on whether those who agreed to have their picture taken anonymously could be identified based on their headshot by checking with Facebook, one-third of the test subjects were identified, and even the personal interests and social security number of some test subjects were revealed. Times when privacy is exposed only by a headshot have already arrived."*

Isao Echizen
Professor, Digital Content and Media Sciences Research Division, NII
Professor, Department of Informatics, School of Multidisciplinary Sciences, The Graduate University for Advanced Studies

PrivacyVisor tricks facial detection

Given the concern that infringement on privacy could become a reality precisely because we are living in the era when big data are available, Echizen continues rapid development of the PrivacyVisor. "The PrivacyVisor," he says, "is an attempt to protect ourselves by preventing our facial image, which is personal information, from being used arbitrarily. With the device, we will be able to prevent infringement on our privacy when photographed by nullifying facial detection, which is a preprocessing of facial recognition, whatever the mechanism of those who collect information may be."

Currently, even standard digital cameras carry a technology for detecting only human faces from images. The Viola-Jones method, adopted as a typical facial detection method, detects a face by checking with the accumulated and learned image data of a face by extracting differences in luminance (light and dark) mainly around the eyes, bridge of the nose and the nose itself.

The method is fairly accurate and it is said that not only faces photographed from 22 meters away, but also in an experiment by Echizen even those disguised with five types of sunglasses of different design could be detected accurately. Although measures to force this facial detection to fail have been proposed, such as coloring the face with special pigments, using a special hairstyle, or wearing a mask covering the face, there was a weak point in the measures: that is, they pose an obstacle to face-to-face communication in the real world. As a tool to prevent facial detection that can be used more naturally, the goggle-type PrivacyVisor was developed.

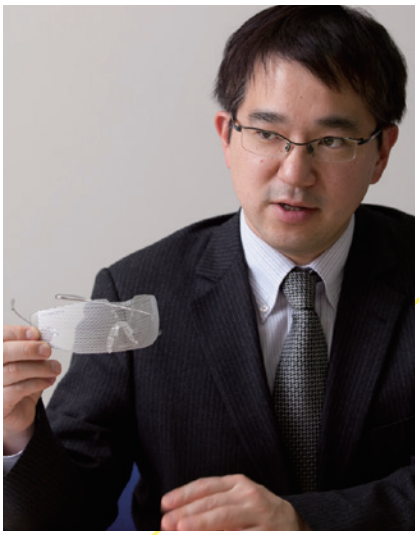
Echizen installs 11 near-infrared LED lights in goggles that cover areas around the eyes so that users can put the lights on when they do not want to have their face detected. Since near-infrared lights have a wavelength beyond the human visible range, they are invisible for a person facing the user. However, because consumer-use cameras detect the infrared range, LED lights are reflected as noise. As a result, luminance differences around the eyes cannot be detected, so facial recognition will fail. This is how the PrivacyVisor works.

In an experiment shooting 10 test subjects standing in front of a camera, the facial detection of seven to eight of them who stood 20 meters away succeeded when they did not wear the PrivacyVisor. While the facial detection rate remained almost unchanged when they wore the PrivacyVisor but did not turn the LED lights on, facial detection was not successful for any subjects standing within 22 meters if the lights were on.

New and fashionable PrivacyVisor needs no power source

The trial product had trouble in that a battery was needed to light the LEDs. And it failed to work since professional cameras did not sense the infrared range. Therefore, since the end of last year and jointly with eyeglass manufacturers in Sabae City, Fukui, which is recognized worldwide for its eyeglasses, Echizen has been moving forward with development of a new PrivacyVisor that needs no LED lights.

Prototype of the PrivacyVisor



The new visor uses a material that reflects visible light for concave areas around eyes, etc. that a face detector deems dark, and conversely a material that absorbs visible light for convex areas deemed bright, such as the upper part of the nose. With white as the basic tone, a trial product sprinkles fine dots and patterns in its transparent parts. This is likely to relatively reduce the sense of discomfort and burden when carrying the device and wearing it like sunglasses. Echizen and the eyeglass manufacturers are said to be seeking launch of a prototype by year's end after adding some design improvements.

Balance between use and application of information and protection of privacy is important

Meanwhile, one concern is the possibility of the PrivacyVisor being used for criminal purposes.

"For example, facial recognition is used in security cameras at airports for identifying terrorists," Echizen says. "In such places, institutional measures such as not allowing the visor to be worn will be necessary. It is important to achieve a good balance between public interest and protection of privacy." The PrivacyVisor also presents this challenge.

Echizen also points out the possibility that wearing the PrivacyVisor could become a sign of refusing use of personal images. He proposes a mechanism to promote the use and application of data by indicating the permissible scope via what we wear (such as accessories and badges) and based on the conditions thereof.

In the age of big data, it seems necessary to think carefully about what to protect and disclose in our personal data to minimize risk and maximize our interest, as well as how to protect data.

(Written by Masahiro Doi)

*Following a request from the European Union (EU), Facebook decided in 2012 not to provide the facial recognition function in Europe. Google Glass has also expressed that it will not be equipped with the function. However, as long as such technology remains practicable, new service providers or application developers could develop and provide facial recognition functionality, even if Facebook and Google do not.