CELEBRATING 25 YEARS OF SERVICE
1994-2019

SWCP Portal

November 2019

Do you feel like you're being watched?

Big Data Is Looking For You

The digital age has turned information into power – particularly private information. Thus, many people are highly – and rightfully – jealously concerned about the safety of their personal financial data. But that is just a very small drop in a very large bucket.

Each human being constantly generates a huge cloud of data about themselves, most of which is ignored. But the truly important facts are out there all the time, freely accessible, and upon them depends most of our interaction with fellow human beings.

This is the physical data about ourselves, starting with our image and voice, that others rely on to identify us and judge our current state. Computers are being trained to read this data. They are learning to recognize people and emotions with a wide range of intimate telling details, called **biometric** data.

Facial recognition technology is a key method in this pursuit, but only one. Success will be very useful for both good and ill purposes, for while it promises a closer interaction with machines, it will also enable them to keep us under close surveillance all the time.

While there are still **bugs**, it's already being deployed. Already, *half* of the adult population of the US – over *117 million* – are already **captured in police databases** that can be read by facial recognition software.

Race for the face

The utility of having computers recognize humans is obvious. Not only could it enhance security and services, personal connections make relationships easier. So researchers around the globe are competing to develop facial recognition, while others contend with the many **legal issues** raised by it. Already a few cities in California have **banned government use** of such tech and the state has imposed a **3-year moratorium** on its use by law enforcement agencies.

Such bans are not just due to its surveillance potential but also **inaccuracy**. Facial recognition works by building templates of an individual's face that measure the landmarks – the size of the nose, shape of the eyebrows, distance between the eyes, etc. While templates can distinguish individuals, **London police** had a *98%* mismatch rate, while an MIT study found that systems were particularly **biased** against dark-skinned women, generating errors of over *30%*.

Employing the technology to identify **emotional states** of observed people is already generating a *$20 billion* market but is even more problematic at this stage. While computer vision systems can detect scowls, for instance, they have trouble properly interpreting them, as human emotions and their subtle changes in social interactions are very complex.

Do lowered eyebrows always mean anger or could they show intense concentration? Researchers found that angry people do *not* scowl *70%* of the time. Yet the judgments computers make can have critical real world implications if they are relied upon in legal or medical situations, or even in line **at the airport**.

A two-year university review found that the correlation of emotional states and expressions is flawed. For one thing, actors are often hired to train machines, and they naturally tend to greatly exaggerate their expressions, warping the results.

Age detection is another potential use for facial recognition. Australia wants it for **age verification** for porn viewing, but haven't managed to get it working yet. Britain also tried, but **gave up** earlier this year. Why anyone imagines that people would voluntarily submit to such a system is the real question.

Beyond the image

Developers are therefore turning to other biometrics -- fingerprints, **irises**, identification by voice or even **walking gaits**. *Anything* physically unique about an individual is fair game to determine identities, eventually even **brain scans**. Yet all have their problems.

Many people have fingerprints that are **not machine-readable**, for example, yet ironically, it has been **demonstrated** that some phone cameras can capture photos of distant celebrities waving hands, for instance, good enough to be used for spoofing.

Speech recognition efforts have an even longer history than that of identifying faces, but much of that work has been devoted to making computers understand the quirks and complexities of natural speech.

Continued on back

Continued from front

Identifying individual speakers first requires sampling that person's speech patterns. If done for identity verification, it can be based on set passwords; for other purposes, the process may be longer, unknown to the subject, and involve speech recognition.

DNA profiling, the ultimate in identity verification, is also coming along. The remains of recently slain ISIS leader Abu Bakr al-Bagdadi, for instance, were confirmed **on the spot**. Not only that, but every day brings more stories of **cold cases solved** or people who have found **unsuspected half-siblings** through genetic screening sites. Yet the **DNA database** could be hacked with the submission of rigged DNA data.

People can also be tracked through things they own or use, like vehicles. Uber is fighting against cities tracking the use of **rental scooters**, citing privacy concerns. Plus a **private network for repo men**, investigators, and the police uses cars like Google's to scan millions of plates as they cruise around.

Ever notice that vehicle plates in pictures posted online are often blurred? That may be because tech giants including Google and Facebook reportedly **routinely read pictures** of license plates that are uploaded to their services and store that information.

Not only that but *all* phone photos by default carry information including exactly **where and when** they were taken, unless that data is deliberately removed. Facebook also **tags individuals** in photos using facial recognition, unless that feature is purposely turned off by users – or at least public display of it.

Just about *any* activity online can be a source of information about users. **Surveys, quizzes, and games** seem innocent fun, but they collect personal data and may even try to hijack people's accounts.

An infinite hell of mirrors

The dangers of all this is apparent in the way Hong Kong protesters must hide their features from the **Chinese surveillance state**. Meanwhile in the West, designers are coming up with all kinds of **anti-surveillance fashion** accessories intended to foil video cameras and AI by blinding or confusing them.

While constant surveillance is an ideal tool for oppression, it can have a benign aspect. Studies have proven that people who think they are **being watched** – like **religious individuals** – generally behave better than their unconcerned peers.

In the 18th century, English philosopher **Jeremy Bentham** proposed jailing prisoners in a **panopticon** – a circular, multi-level prison where the cells of incarcerated criminals could be observed invisibly by a lone guard in a central tower, who was also watched. America's "**supermax**" prisons and many others are based on the concept. Bentham wrote up his proposal while crossing the ocean on a slave ship, which to many critics through the centuries has seemed a perfect metaphor for its potential for enslavement

Social media has been called an **electronic panopticon**, where people are always on display and being judged by the platform itself. If all our data was integrated, the internet could become an inescapable Orwellian prison overnight, but it doesn't have to be as overt as **China's**. Perhaps the cell doors have quietly **clicked shut** and we just haven't noticed it yet.

Going to LightSpeed

SWCP LightSpeed, our premium fiber-DSL access service, has expanded with many more speed options for both downloading and uploading than before. Prices have dropped in some categories, and the old activation charge has been eliminated.

However, CenturyLink, the ultimate successor to Ma Bell here in New Mexico and the provider of our high-speed DSL services, has also decided to eliminate their legacy DSL circuits. Those users still on the old Qwest Megabit circuits will also have to get the new CenturyLink modems to use the new LightSpeed connections just like brand-new customers.

This is an excellent opportunity to upgrade speeds. Once CenturyLink's fiber reaches a neighborhood, old-style DSL really slows down anyway. Plus, the previous set of bandwidths may not be enough for using net-connected appliances, such as IP doorbells, and most are quite insufficient for video streaming.

SWCP will soon be contacting all our members who still rely on those or other obsolete services to urge an upgrade. Available home speeds may be found at **LightSpeed at Home** at **https://www.swcp.com/lightspeed-home/** while **LightSpeed for Business** is at **https://www.swcp.com/lightspeed-business/**.

More about this change, including speeds needed for streaming, can be found on the SWCP blog at **https://www.swcp.com/big-changes-to-dsl/**.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⦿ **SWCP.com** ⦿ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**
Click on blue terms in PDF file to open links.