Smartphones have you pegged, and for better or worse they'll soon ID you

March 3 2017, by Tim Johnson, Mcclatchy Washington Bureau

Credit: CC0 Public Domain

The things that make human beings unique - fingerprints, irises, facial features - have become the preferred way to sign onto banking accounts online or other sensitive websites, the newest solution to the problem of

hackable and forgettable passwords.

But your fingerprints can be stolen, your photo replicated. Now cyber experts are looking at the next security step: cellphones and computers that actually recognize you from a variety of factors.

Your smartphone now gathers more information about you than you probably realize.

"It's amazing how many sensors there are on a modern-day smartphone. You have motion sensors, like an accelerometer, a gyroscope and magnetometer," said John Whaley, chief executive of UnifyID, a startup that offers what it calls revolutionary authentication.

Then you have other sensors, such as GPS, Bluetooth and Wi-Fi. All told, an average smartphone has 10 or so sensors measuring precise details about location and user habits.

"We can tell what floor of a building you're on. We can tell if you are inside or outside of a building," Whaley said. "Just with a few seconds of your walking data, from your phone sitting in your pocket, we can actually identify you based on that."

All told, smartphones can measure the angle that your cradle your devices, the pressure you put on the screen, how much of your finger touches the pad, the speed at which you type, how you swipe, your physical rhythms, the times you normally stir in the morning, some 100 or more indicators that in combination can give near total accuracy in identifying you.

"Once you combine a large number of these factors together, we can actually get to 99.999 percent accuracy about it being you versus not you," Whaley said. "At that threshold, you can actually use this for

authentication and you don't have to use passwords anymore."

If passwords become a thing of the past, it is likely due to what computer scientists describe as machine learning - which allows computers to find hidden insights without being explicitly programmed where to look - as well as improvements in sensors that measure our lives and actions with precision. What Whaley calls "implicit authentication" may change the way humans interact not only with phones and websites, but maybe the world at large. ATMs may recognize us as we approach. Clerks or cash registers at stores may greet us by name as their computers recognize our smartphones.

Whaley, who has a master's degree in computer science from MIT and a doctorate in the field from Stanford, is catching attention. His company competed with scores of others as the most innovative startup in the field of cybersecurity at the RSA conference in San Francisco last week, which drew 43,000 attendees, and won in a unanimous decision of the judges.

Technology to ensure authentication of users would have repercussions in banking and finance, e-commerce, cybersecurity, transportation security and in fraud detection, sectors with a value that nearly reaches $2 trillion.

"The need for extended authentication technology is going to be great," said Robert Capps, vice president of business development at NuData Security, a Vancouver firm that uses behavioral analytics to help clients identify good users from bad ones.

The downside to using biometrics, such as fingerprints, in computer security is not widely understood.

"There definitely is a gap in the perceived value of biometrics and the

true value," said Daniel Ingevaldson, chief technology officer at Easy Solutions, a Doral, Fla., company that helps banks fight electronic fraud.

Ingevaldson noted that a billion smartphones are now equipped with fingerprint sensors, and consumers clamor for banks to accept biometric proof.

But fingerprints are not secure. In the hack of the federal Office of Personnel Management in 2015, the fingerprints of 5.6 million people were stolen. And prints can be lifted off surfaces such as glass doors. High-resolution photos can also fool facial recognition software.

"Once your biometric credentials are stolen, they are stolen forever. There's no way to easily change your face. There's no easy way you can change your voice. And definitely not an easy way to change your fingerprints," said Ricardo Villadiego, Easy Solutions' chief executive.

Traditionally, the areas of authentication for users are something you know (such as a password), something you have (say, a cellphone or an electronic key) or something you are (a biometric indicator).

As the need for passwords has proliferated, users have grown fatigued. Many users choose ever simpler passwords. They repeat the same password on multiple sites, or make minor modifications.

The advantage of what UnifyID calls implicit authentication is that a user doesn't take conscious action to verify his or her identity. The smartphone, using a data bank of patterns of a given user, is continuously testing against those patterns.

"Security, instead of being up front, like, 'what's your password?' is going to be passive, in the background and happening all the time," Whaley said.

"Your devices will recognize you. Your car will recognize you. Your house will recognize you, and so security will become much more seamless," Whaley said. "It wasn't possible just a few years ago. It's because of a proliferation of sensors, the fact that they are all connected, and machine-learning technology."

Just how such data are stored, and who has access to it, may play out differently in different parts of the world.

"The perception in the U.S. is that consumer data (are) fine in the hands of private industry but not fine in the hands of government," Capps said. In Europe, the opposite is true.

Authentication can occur either on a smartphone itself or in the cloud, and there are tradeoffs. If data is stored on a phone, then the phone itself recognizes a fingerprint and only sends a simple message on to institutions like banks, which cannot conduct further analysis. But if companies collect a large repository of sensitive user data, it becomes a honey pot for hackers.

"Much of the data is actually sensitive," Whaley said, "things about even where you are at a certain time of day. These are examples of data you may not even want your spouse to know."

Kurt Somerville, chief operating office at UnifyID, said companies compiling the vast data that can be extracted from smartphones must be "totally transparent" with users about what they are collecting and what it will be used for, opting in or out for each data point.

"If they are not comfortable with us using their GPS, where they physically move, they can turn that off and all the other factors will essentially re-weigh themselves," he said.

Whaley said the passive biometric data would be kept on the smartphones themselves, not by the company.

"We always want to be in the position that even if somebody hacked into our servers or we got a subpoena from a government or otherwise were compelled to give up data, we can legitimately say there's no way for us to give that data because we don't have it," Whaley said.