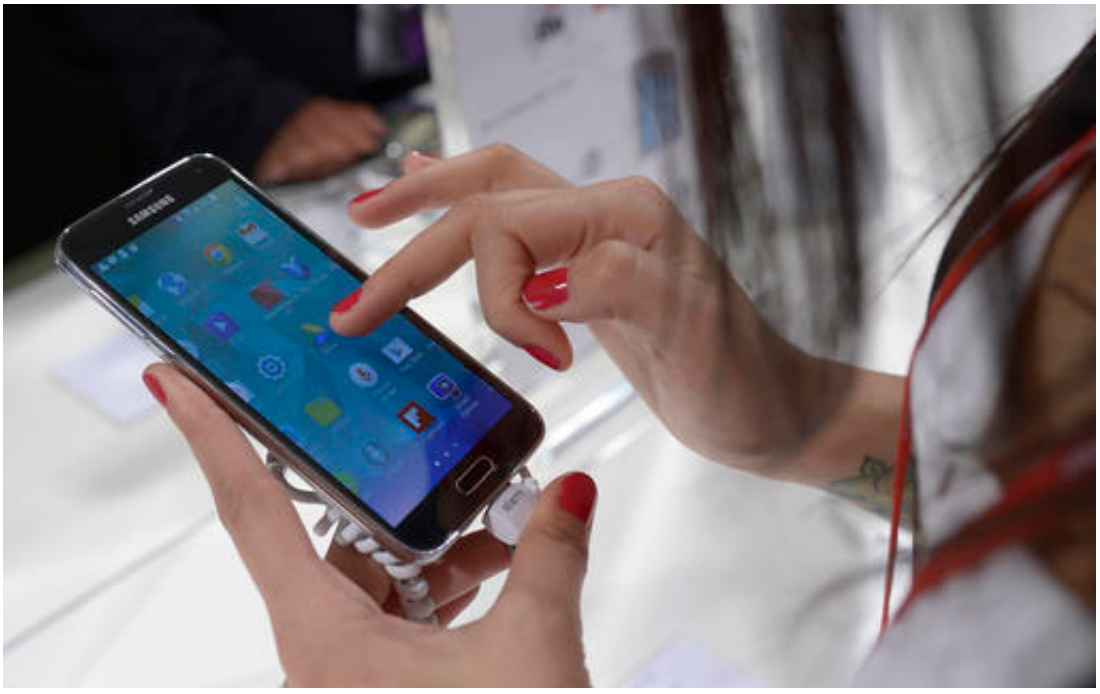
Why fingers make handy, if not foolproof, digital keys

November 21 2016, by Brandon Bailey



In this Feb. 25, 2014 file photo, theSamsung Galaxy S5 is displayed at the Mobile World Congress in Barcelona, Spain, Tuesday, Feb. 25, 2014. Leading tech companies are increasingly nudging consumers to use their own fingers, faces and eyes as digital key to unlock phones and other gadgets. But there are downsides: Hackers could still steal your fingerprint, or its digital representation. And police may have broader legal powers to make you unlock your phone. (AP Photo/Manu Fernandez)

It sounds like a great idea: Forget passwords, and instead lock your

phone or computer with your fingerprint. It's a convenient form of security—though it's also perhaps not as safe as you'd think.

In their rush to do away with problematic passwords, Apple, Microsoft and other tech companies are nudging consumers to use their own fingerprints, faces and eyes as digital keys. Smartphones and other devices increasingly feature scanners that can verify your identity via these "biometric" signatures in order to unlock a gadget, sign into web accounts and authorize electronic payments.

But there are drawbacks: Hackers could still steal your fingerprint—or its digital representation. Police may have broader legal powers to make you unlock your phone. And so-called "biometric" systems are so convenient they could lull users into a false sense of security.

"We may expect too much from biometrics. No security systems are perfect," said Anil Jain, a computer science professor at Michigan State University who helped police unlock a smartphone by using a digitally enhanced ink copy of the owner's fingerprints.

BYPASSING THE PASSWORD

Biometric security seems like a natural solution to well-known problems with passwords. Far too many people choose weak and easily-guessed passwords like "123456" or "password." Many others reuse a single password across online accounts, all of which could be hacked if the password is compromised. And of course some use no password at all when they can get away with it, as many phones allow.

As electronic sensors and microprocessors have grown cheaper and more powerful, gadget makers have started adding biometric sensors to familiar products.

Apple's iPhone 5S, launched in 2013, introduced fingerprint scanners to a mass audience, and rival phone makers quickly followed suit. Microsoft built biometric capabilities into the latest version of its Windows 10 software, so you can unlock your PC by briefly looking at the screen. Samsung is now touting an iris-scanning system in its latest Galaxy Note devices.

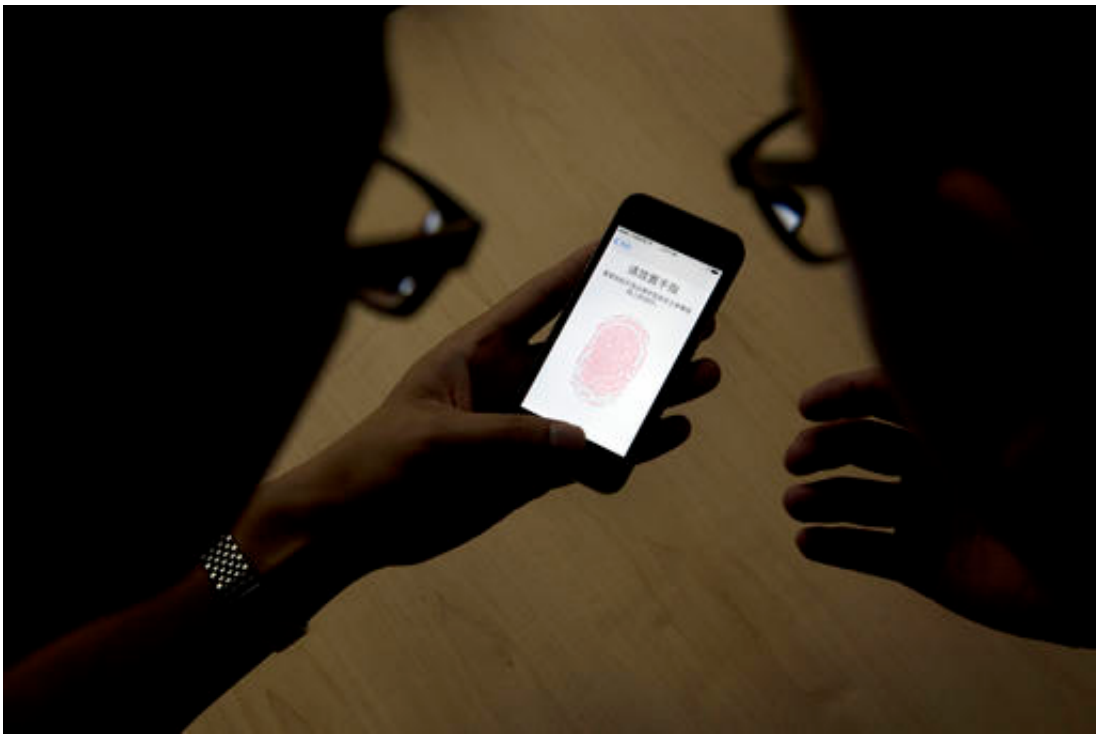
All those systems are based on the notion that each user's fingerprint—or face, or iris—is unique. But that doesn't mean they can't be reproduced.

LIFTING PRINTS, FAKING FACES

Jain, the Michigan State researcher, proved that earlier this year when a local police department asked for help unlocking a fingerprint-protected Samsung phone. The phone's owner was dead, but police had the owner's fingerprints on file. Jain and two associates made a digital copy of the prints, enhanced them and then printed them out with special ink that mimics the conductive properties of human skin.

"We tried the right thumb and it worked right away," Jain said.

Researchers at the University of North Carolina, meanwhile, fooled some commercial face-detection systems by using photos they found on the social media accounts of test subjects. They used the photos to create a three-dimensional image, enhanced with virtual reality algorithms. The spoof didn't work every time, and the researchers found it could be foiled by cameras with infrared sensors. (The Microsoft face-recognition system uses infrared-capable cameras for extra precision.)



In this Sept. 11, 2013, file photo, an Apple employee, right, instructs a journalist on the use of the fingerprint scanner technology built into the company's iPhone 5S during a media event in Beijing. Leading tech companies are increasingly nudging consumers to use their own fingers, faces and eyes as digital key to unlock phones and other gadgets. But there are downsides: Hackers could still steal your fingerprint, or its digital representation. And police may have broader legal powers to make you unlock your phone. (AP Photo/Ng Han Guan, File)

But some experts believe any biometric system can be cracked with sufficient determination. All it takes are simulated images of a person's fingerprint, face or even iris pattern. And if someone manages that, you can't exactly change your fingerprint or facial features as you would a stolen password.

To make such theft more difficult, biometric-equipped phones and computers typically encrypt fingerprints and similar data and store them locally, not in the "cloud" where hackers might lift them from company

servers. But many biometrics can be found elsewhere. You might easily leave your fingerprint on a drinking glass, for instance. Or it might be stored in a different database; Jain pointed to the 2015 computer breach at federal Office of Personnel Management, which compromised the files—including fingerprints—of millions of federal employees.

COMPELLED TO UNLOCK

Most crooks won't go to that much trouble. But some experts have voiced a different concern—that biometrics could undermine important legal rights.

U.S. courts have ruled that authorities can't legally require individuals to give up their passwords, since the Fifth Amendment says you can't be forced to testify or provide incriminating information against yourself. In the last two years, however, judges in Virginia and Texas have ordered individuals to unlock their phones with their fingerprints.

There's a legal distinction between something you know, like a password, and something you possess, like a physical key or a fingerprint, said Marcia Hofmann, a San Francisco attorney who specializes in privacy and computer security. While you can't be forced to reveal the combination of a safe, she noted, the Supreme Court has said you can be required to turn over a physical key to unlock a door.

"Getting your thumb print or iris scan is not the same as making you speak," agreed Orin Kerr, a law professor at George Washington University. "In practice it's another way of getting access to the computer, but through a very different means."

The issue hasn't been tested yet in higher courts, though it's likely just a matter of time.

Even with vulnerabilities, some analysts say the convenience of biometric locks is a plus—not least because it may give the password-averse another easy option to secure their devices. "It's bringing secure authentication to the masses," said Joseph Lorenzo Hall, a tech policy expert at the nonprofit Center for Democracy and Technology.

Others say the best approach would combine biometric systems with other protections, such as a strong password or PIN.

"It's good to see biometrics being used more, because it adds another factor for security," said Jain. "But using multiple security measures is the best defense."