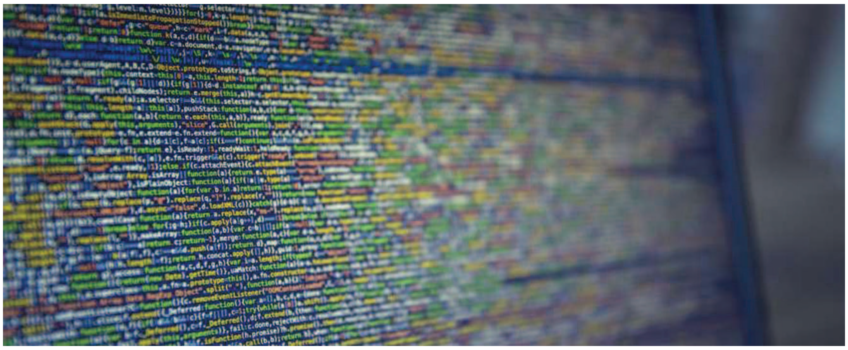
Nasir Memon

# How Biometric Authentication Poses New Challenges to Our Security and Privacy

The use of biometric data—an individual's measurable physical and behavioral characteristics—isn't new. Government and law enforcement agencies have long used it. The Federal Bureau of Investigation (FBI) has been building a biometric recognition database [1]; the U.S. Department of Homeland Security is sharing [2] its iris and facial recognition of foreigners with the FBI. But the use of biometric data by consumer goods manufacturers for authentication purposes has skyrocketed in recent years. For example, Apple's iPhone allows users to scan their fingerprints to unlock the device, secure mobile bill records, and authenticate payments. Lenovo and Dell [3] leverage fingerprints to enable users to sign onto their computers with just a swipe.

Using biometric data to access our personal devices is increasing as a way to get around the limitations of the commonly used password-based mechanism: it's easier, more convenient, and (theoretically) more secure. But biometric data can also be stolen and used in malicious ways. Capturing fingerprints at scale isn't as easy as lifting a credit card or Social Security number, but experience and history tells us that once something is used extensively, criminals will figure out how to misuse and monetize it.


ADOBE STOCK

In addition, with the uptick in data breaches [4] (Yahoo! being the most recent example [5]), we've demonstrated we can't keep secrets or properly protect identities. As more companies use biometric authentication, we must be concerned about how our biometric data is secured: currently there is no restriction on what biometric information companies can share and with whom. This is why we need better solutions—we must develop techniques and protocols based on cryptography and signal processing that would protect biometric data and yet allow authentication. We need mechanisms that provide a user some control on when and how their biometric data are being used.

As more companies use biometric authentication, we must be concerned about how our biometric data is secured.

To ensure we're staying on top and ahead of threats to our personal information, we must better understand the dangers associated with the use of biometric authentication (and the role signal processing can play in alleviating them), and the concerns that come to light with technological advances.

## The dangers of frequent biometric authentication

Why is biometric authentication an important issue now more than ever? Companies are increasingly using different means to identify people and assess their buying decisions and how they live their lives. By simply uploading your picture to Facebook or using your thumb to unlock your smartphone, you may be giving away critical data without realizing where the information is going and what it's being used for. It's feasible to envision a society in which we're all identified, all the time and wherever we go. This is dangerous because it can lead to illegal spying [6] from government and law enforcement agencies. To address these concerns, mechanisms must be put in place to permit people to

(continued on page 194)

Digital Object Identifier 10.1109/MSP.2017.2697179
Date of publication: 11 July 2017

(continued from page 196)

keep some level of anonymity. We need new approaches and tangible solutions to tackle this issue as it will cause significant problems in our future, but the question of how we will accomplish this still remains.

When it comes to secure storage of biometric data, there have been some clever techniques proposed in the past, enabled by signal processing, including fuzzy hash [7] (e.g., the ability to compare two distinctly different items and determine a level of similarity between the two), fuzzy vault [8] (e.g., an encryption scheme that encodes information in a way that is difficult to obtain without a key), and secure sketch [9] techniques. However, these techniques suffer from one of two problems. First, many of the security techniques proposed, from a quantification, storage, and communication point of view, are designed for discrete data and use simple similarity measures. However, true biometric data requires complex similarity functions. Second, the techniques designed for real-world biometric data are either ad hoc and without formal proof of security or don't provide a sufficiently rigorous security formulation.

While your face isn't a secret, the data about you and your loved ones that it's linked to should be protected unless we truly do want to live in a "Big Brother" society.

## Is technology giving companies unprecedented access to our data?

For most of us, the use of fingerprints today might be limited to our phone or computer, but what does the future hold for biometric authentication? As technology advances, we will encounter privacy and security issues even more frequently. It's within reach for companies to use new technology to replace all passwords, security personal identification numbers, access codes, etc. MasterCard and HSBC are great examples [10] of companies using facial recognition technology to verify a user's identity. Even Ford is partnering [11] with a machine vision company to add facial recognition technology to its vehicles.

But these advances might allow companies to "go too far" with a person's biometric data, giving unprecedented access. While your face isn't a secret, the data about you and your loved ones that it's linked to should be protected unless we truly do want to live in a "Big Brother" society.

All in all, these security concerns will only increase and evolve with time, but signal processing plays a significant role in providing potential solutions to these issues. Although there is a fascination with the science behind our biometric data, we can't head into a future in which we'll be identified at every step of our lives. We must be diligent in ensuring the right policies and laws prevent biometric data from being used indiscriminately. We must ask ourselves how biometric authentication, which is a convenience in our lives, be prevented from becoming an avenue for companies to invade our privacy.

## Author

*Nasir Memon* (memon@nyu.edu) received his B.E. and M.S. degrees from Birla Institute of Technology and Science, Pilani, India, and his Ph.D. degree from the University of Nebraska. He is a member of the IEEE Signal Processing Society and a professor of computer science and engineering at New York University (NYU) Tandon School of Engineering. He also is an affiliate faculty member in the Computer Science Department in the Courant Institute of Mathematical Sciences at NYU.

## References

[1] J. Lynch. (2015). FBI combines civil and criminal fingerprints into one fully searchable database. [Online]. Available: https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again

[2] A. Sternstein. (2015). Department of Homeland Security. [Online]. Available: http://www.nextgov.com/defense/2015/01/dhs-launch-iris-and-facial-recognition-border/103908/

[3] Lenovo and Dell—Laptop with fingerprint scanner. [Online]. Available: http://checklaptop.com/best-laptop-with-fingerprint-reader-44/

[4] P. Ausick. (2016). Data breaches top 600 so far in 2016. [Online]. Available: http://247wallst.com/technology-3/2016/08/19/data-breaches-top-600-so-far-in-2016/

[5] M. Snider and E. Weise. (2016). 500 million Yahoo accounts breached. [Online]. Available: http://www.usatoday.com/story/tech/2016/09/22/report-yahoo-may-confirm-massive-data-breach/90824934/

[6] K. Kimachia. (2013). How to protect yourself from unethical or illegal spying. [Online]. Available: http://www.makeuseof.com/tag/how-to-protect-yourself-from-unethical-or-illegal-spying/

[7] (2007). Using fuzzy hashing techniques to identify malicious code. [Online]. Available: http://www.shadowserver.org/wiki/uploads/Information/FuzzyHashing.pdf

[8] (2011). Fuzzy vault. [Online]. Available: https://wiki.cse.buffalo.edu/cse545/content/fuzzy-vault

[9] L. Qiming, S. Yagiz, and M. Nasir, "Secure sketch for biometric templates," *Adv. Cryptology*, vol. 4284, pp. 99–113, 2006. [Online]. Available: http://dx.doi.org/10.1007/11935230_7

[10] T. Wadlow. (2016). HSBC deploys selfie security: Are passwords finished? [Online]. Available: http://www.businessreviewdeurope.eu/finance/1048/HSBC-deploys-selfie-security:-are-passwords-finished

[11] J. Carroll. (2016). Ford targeting launch of fully autonomous vehicle by 2021. [Online]. Available: http://www.vision-systems.com/articles/2016/09/ford-targeting-launch-of-fully-autonomous-vehicle-by-2021.html