What's in a Face: Risks of biometric authentication and data collection

By Anita Lam
Tufts University
December 13, 2019

Abstract

Biometric data collection today has become an increasingly common part of everyday life. From countries using facial recognition software to keep track of their citizens to the daily fingerprint and face ID given to access a user's phone, biometric identification and authentication has seen a surge in recent history. However, current policy and security methods have struggled to keep up with these new developments in terms implementation and protection. When companies who use biometric technology gets hacked, the biometric data, when revealed, is irreversible. Everyone only has one face, one fingerprint—there is no other password to replace it. This paper proposes that the current state of policy enables these attacks and evasive techniques. Thus, this paper will center around two ideas: the current offensive attacks and breaches against biometric authentication and identification, and the defensive methods against biometric identification and data collection. These two topics will be guided through the lens of current policy and laws surrounding biometric identification and authentication.

Introduction

Biometric authentication has rapidly evolved from the first fingerprint collection system used in 1858 due to a growing need for a reliable user authentication method.[1] Today, biometric data can be measured via fingerprints, iris scans, facial recognition, voice identification, and even through a person's gait. The technology is used by the government, businesses, airports, and consumers' everyday lives. As of 2018, 67% of smartphones bought across the world have a fingerprint verification system.[2] Biometric authentication works by comparing two sets of data—one preset by the user and stored away, and another belonging to the user currently trying to access it. If the two are almost identical, then the user is approved. According to ievo Ltd, a company that produce biometric fingerprint recognition products, there are five main ways to securely store biometric data—hardware-based recognition system, portable token, on-device, biometric data base server, and distributed data storage.[3] A hardware-based recognition system is when data is stored on a piece of hardware and used in tandem with the device to authenticate the data. A portable token is a 2-step authentication process where biometric data is used along with a portable fob or smart card. This prevents any biometric data from being transferred over a network, reducing any network-related risks. On-device is used daily on smartphones, storing the data on a chip that is separate from the device's network. With this method, organizations that implemented the process does not have any control over the data stored. A biometric data base server is a network-based method that encrypts data and stores it on an external server. Finally, a

distributed data storage which breaks up the data and stores the some on the server and some on the device. There are a multitude of ways to store biometric data, each one with their own strengths and weaknesses. In this paper, it will discuss the impact of biometric data collection on the community, various strengths of biometric authentication, the landscape of security and privacy risks of biometric data, and an inquiry into US biometric laws.

To the Community

Biometric data collection involves highly sensitive data and as it integrates itself into everyday tasks, it is important to question the security of the databases in which biometric data is stored. Once a person's biometric data is compromised, it is no longer in their control. Moreover, due to its relative novelty, laws in the United States are still unclear on how regulate the collection of biometric data and how privacy should be protected. While companies like ievo Ltd tout that biometric authentication is the "one of the safest methods of authentication," many breaches in both privacy and security over the past couple years have already proven that the security of biometric *data* leaves much to be desired. The general public often times do not have a good understanding of what is being done with their fingerprints or their face scans by companies or their government. With more than 62% of organizations using biometrics for authentication, people rarely give a thought to which companies are now holding valuable data and whether they will protect user privacy and secure it. There is often a gap between technology and policy as the former continuously outgrows the latter. This paper is written in hopes of bridging this chasm a bit and bring to the issue to the forefront of the general populace's minds.

Strengths of Biometric Authentication

Biometric authentication provides an alternative to user passwords and personal identification numbers (PINs). Biometrics provide an accurate and reliable user authentication method that is not easily lost or duplicated by users.[4] It is almost impossible "to replicate a piece of biometric data as the image itself is discarded and a mathematical representation of it is used for the verification process."[3] There is further security in that the person is physically present for the identification and authentication, removing the need to write passwords down and rendering the password sharing phenomena obsolete. Furthermore, biometric readings have a higher information content than normal passwords and would require more effort to mount a brute-force attack that can easily overturn passwords.[4]

Current Threats

Tricking the Hardware

Tricking hardware is relatively easy enough as all someone would have to do for a fingerprint is lift it off something the victim touches.[14] Iris scans can also be mimicked through a

high resolution photo with contact lens to act as the curvature of the eyeball.[15] With each sort of authentication method there is someone who could falsify the data being verified.

Biometric database security

While there are certainly strengths in biometric authentication and identification, they still have their own vulnerabilities. Each aspect of biometric authentication from hardware to databases have their own set of problems. In August 2019, Suprema—a company that specializes in biometrics, security and identity solutions—was breached. Suprema launched Biostar 2 which uses fingerprints and facial recognition to identify people entering certain buildings. According to *The Guardian*, two researchers Noam Rotem and Ran Locar discovered a major flaw in Suprema's system. Through a simple manipulation of the URL search criteria, they were able to search the Biostar 2 database and accessed "27.8m records, and 23 gigabytes-worth of data including admin panels, dashboards, fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, and personal details of staff."[5] There were further problems with storing passwords in plain-text and un-hashed fingerprints that can be copied and used maliciously. According to Rotem, these problems are "very common."[5] This vulnerability also allowed the researchers to manipulate the database including, but not limited to, adding and removing in users and their biometric data.

Government Surveillance Privacy

On perhaps an even bigger scale, Dutch security researcher Victor Gevers exposed the surveillance tracking of a Chinese software database, SenseNets, this year. SenseNets is employed by the Chinese government to support their notorious surveillance state by providing facial recognition and crowd analysis technology. The surveillance database was open to the public for months, compromising millions of people's personal data.[7] But beyond a database breach, the data revealed that China was tracking more than 2.5 million Xinjiang Muslims, keeping real-time information on their GPS locations, a concern that is augmented by current news on China's Muslim internment camps.[8] Thought the world has grown used to China's surveillance state, according to Gevers, this is a clear invasion into the populace's privacy.[9]

Another China data breach revealed a database that registered 1.8 million women, determining if they were of "BreedReady" status. The youngest girl in the database was 15 years old.[7] This data, like most data in China, is provided through their elaborate facial recognition system.

Corporate Surveillance Privacy

It is not simply China or governments that misuse data collected from biometric software. In American headlines, the conclusion of a data breach with Perceptics came to a close on October 2019.[6] Perceptics was contracted to work with the US Customs and Border Protection (CBP); however, it was discovered on June 2019 that Perceptics have been using CBP's data to

train their own facial biometric algorithm—tying car license plates to people's faces (without the CBP's or the people's explicit permission). House Homeland Security Committee chairman Rep. Bennie Thompson stated after this incident that "The federal government does not have a great track record securing America's personal data."[10] However, the CBP has deemed this event as "unacceptable" but not unethical or illegal and is looking to continue their contract with Perceptics after some company changes are implemented.[10] There is a disappointed response to this contract renewal as people hope that agencies who find vulnerable technology or severe breaches in privacy not only revisit their contract, but also revisit how they are using the technology in the first place as there can only be bigger breaches in the future.

Overview of US Biometric Laws

As of now, there is no encompassing federal law regulating the collection and use of biometric data in the US. Illinois is currently the state with the strictest biometric laws due to the Biometric Information Privacy Act (BIPA). Under BIPA, it "prohibits private entities from collecting, capturing, or otherwise obtaining an individual's biometric data without first informing him or her in writing, and disclosing the specific purpose and length of time for which the data is being collected and stored."[11] As of now, only two other states have biometric privacy laws in place—Texas and Washington. California's California Consumer Privacy Act (CCPA) will be effective as of January 1, 2020. Arizona, Florida, and Massachusetts have begun proposing legislation addressing biometric privacy.

As states begin to follow in Illinois' footsteps on protecting the biometric data of individuals, companies that employ biometric authentication or collect biometric data are beginning to see the consequences of biometric data leaks. Following the events of SenseNets' breach, lines of Microsoft code was found and SenseNets also lists Microsoft as one of their partners.[12] However, Microsoft has refuted those claims and in January 2019 Microsoft Chief Executive Satya Nadella advocated for the regulation of facial recognition technology, stating that "self-regulation among tech companies might not be enough."[13]

It should however be noted that on the other side of this, there are still many tech companies out there that are not as devoted in regulation, whether that is self-regulated or government regulated. Facebook has expressed support to amend BIPA so that it is not as strict. As of 2011, Facebook has been a quiet lobbyist on issues of data security and consumer privacy, spending $1.4 million.[16] By 2016, this amount grew to $8.7 million.

Amazon too brought up concerns with their facial recognition tool, Rekognition, which is being sold to U.S. police departments. The public, often prone to sensationalizing technologies that can be seen as threats civil liberties, jumped on the problematic ease in which this tool can be implemented—fearing that this is a large step towards a China-esque surveillance state. The public's fears may hold a grain of truth, however. Rekognition is open to all and a small experiment within Forbes showed that the tool was setup in a matter of hours.[17] Amazon has pointed out that they will not allow anyone to break laws with Rekognition or to threaten privacy rights, but Forbes writer Thomas Brewster brings up the question of how Amazon might monitor the multitude of customers they have.[17] Furthermore, there are high security concerns as there

have been a history of open and public databases used through Amazon Web Services. If law enforcements do not take care in securing their databases, another breach can lead to fatal consequences.

Currently the United States is a patchwork of biometric laws, each state forming its own regulations, some states having none. It might be vital to consider a single federal law for biometric data regulation, like the EU and their General Data Protection Regulation (GDPR). The most influential essays in American Law is one concerned with privacy. "The Right to Privacy" published in 1890 is at once outdated and prevalent. Addressed at that time towards the press, it states, "The press is overstepping…the obvious bounds of propriety and decency" and goes further to assert that there must established restrictions between public and private life and that it goes beyond the right to be let alone.[18] Now the lines between public and private life has long since been blurred so how might the law interpret biometric authentication and identification today? Data that was once private is now public data, most companies that consumers interact with have it, and as history has shown, the insecurity and sometimes the collection of that data obviously oversteps the "bounds of propriety and decency." Establishing a uniform federal law regarding biometric data will bring a much-needed update to the 1890 privacy laws. Furthermore, with individual state laws, there is often jurisdiction issues, so a federal law might just save companies the trouble of litigation.

Conclusion

The widespread usage of biometric technology has already threatened many civilian's personal data. These instances serve as a reminder that there is rarely a "better authentication method." Biometric authentication is subjected to many of the same vulnerabilities that passwords are too. Biometric *data* is subjected to the same network or database attacks passwords are too. It is necessary to further protect databases from revealing such personal and unique information. Moreover, it there remains the question of what data is being collected by governments or by companies through biometrics. In the end everything sums up to be that there needs to be implementations in place, standards across people who use biometric data, to protect the information of the general populationf whether that is from breaches or from oversurveillance. As identity theft expert, John Sileo said, "If we implement biometrics without doing our due diligence on protecting the identity, we are doomed to repeat history—and our thumbprint will become just another Social Security Number."[18]

References

[1] Mayhew, Stephen. “History of Biometrics.” *Biometric Update*, 20 July 2018, www.biometricupdate.com/201802/history-of-biometrics-2.

[2] “Global Smartphone Fingerprint Penetration 2014-2018.” *Statista*, www.statista.com/statistics/522058/global-smartphone-fingerprint-penetration/.

[3] ievo Ltd. “How Biometric Data Is Stored.” *Ievo Ltd*, 4 Jan. 2019, ievoreader.com/how-biometric-data-is-stored/.

[4] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Enhancing security and privacy in biometrics-based authentication systems." *IBM systems Journal* 40.3 (2001): 614-634.

[5] “Major breach found in biometrics system used by banks.” *The Guardian*, https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[6] Burt, Chris. “Breached License Plate Recognition Provider Back to Work for CBP.” *Biometric Update*, 11 Oct. 2019, www.biometricupdate.com/201910/breached-license-plate-recognition-provider-back-to-work-for-cbp.

[7] Doffman, Zak. “Interview – Meet Victor Gevers , The Ethical Hacker Who Exposed ‘BreedReady’ and ‘SenseNets’”, 13 Mar. 2019, https://www.forbes.com/sites/zakdoffman/2019/03/13/why-victor-gevers-was-so-reluctant-to-expose-the-sensenets-and-breed-ready-data-breaches/#5937f84750c0.

[8] Buckley, Chris, and Austin Ramzy. “Facing Criticism Over Muslim Camps, China Says: What's the Problem?” *The New York Times*, The New York Times, 9 Dec. 2019, www.nytimes.com/2019/12/09/world/asia/china-camps-muslims.html.

[9] Goud, Naveen, et al. “Chinese Database Hack Reveals the Grievances in Government Surveillance.” *Cybersecurity Insiders*, 20 Feb. 2019, www.cybersecurity-insiders.com/chinese-database-hack-reveals-the-grievances-in-government-surveillance/.

[10] Harwell, Drew. “Surveillance Contractor That Violated Rules by Copying Traveler Images, License Plates Can Continue to Work with CBP.” *The Washington Post*, WP Company, 10 Oct. 2019, www.washingtonpost.com/technology/2019/10/10/surveillance-contractor-that-violated-rules-by-copying-traveler-images-license-plates-can-continue-work-with-cbp/.

[11] Marotti, Ally. "Shutterfly lawsuit tags Illinois as battleground in facial recognition fight." Chicagotribune.com. 21 Sept. 2017, http://www.chicagotribune.com/business/ct-biz-biometricsshutterfly-lawsuit-20170920-story.html.

[12] Arjun, Kharpal. “Microsoft Says Facial Recognition Firm That Beijing Allegedly Uses to Track Muslims Is Lying about a 'Partnership'.” *CNBC*, CNBC, 17 Mar. 2019, www.cnbc.com/2019/03/15/microsoft-facial-recognition-firm-sensenets-lying-about-partnership.html.

[13] Browne, Ryan. “Microsoft CEO Says Facial Recognition Technology Needs to Be Regulated.” *CNBC*, CNBC, 25 Jan. 2019, www.cnbc.com/2019/01/24/davos-microsofts-nadella-says-facial-recognition-needs-regulation.html.

[14] Porter, Kim. “Biometrics and Biometric Data: What Is It and Is It Secure?” *Official Site*, us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.

[15] Sulleyman, Aatif. “Samsung Galaxy S8 Iris Scanner Hacked Using Contact Lens.” *The Independent*, Independent Digital News and Media, 24 May 2017, www.independent.co.uk/life-style/gadgets-and-tech/news/samsung-galaxy-s8-iris-scanner-hack-contact-lens-security-smartphone-chaos-computer-club-a7752616.html.

[15] “Facebook Inc: Lobbying.” *OpenSecrets.org*, www.opensecrets.org/orgs/lobby.php?id=D000033563.

[16] Fox-Brewster, Thomas. “We Built A Powerful Amazon Facial Recognition Tool For Under $10.” *Forbes*, Forbes Magazine, 6 June 2018, www.forbes.com/sites/thomasbrewster/2018/06/06/amazon-facial-recognition-cost-just-10-and-was-worryingly-good/#7590637351db.

[17] Stroup, Jake. “Why Biometric Identification May Not Be All It's Cracked Up to Be.” *The Balance*, The Balance, 11 Dec. 2019, www.thebalance.com/biometric-identification-and-identity-theft-1947595.

[18] Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4, no. 5 (1890): 193. Accessed February 22, 2018. doi:10.2307/1321160.