JANUARY 2020

BIOMETRIC DATA PRIVACY in the Digital Age

POTOMAC INSTITUTE FOR POLICY STUDIES

Images by Alex Taliesen, unless otherwise noted.

NOTICE: These assessments are a product of the Potomac Institute for Policy Studies.

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful science and technology policy options and ensure their implementation at the intersection of business and government.

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA, 22203
www.potomacinstitute.org

Telephone: 703.525.0770; Fax: 703.525.0299

Email: webmaster@potomacinstitute.org

CONTENTS

Photo credit: www.depositphotos.com

EXECUTIVE SUMMARY

In recent years, there has been a rapid increase in the generation of biometric data.[1] There are many reasons for this trend, including the expanding capabilities and benefits of biometric technology and authentication, such as improved security and ease of use.[2] The use of biometric data across industries has become so common that it is estimated that over 75% of consumers have used some type of biometric technology, such as fingerprinting or facial recognition scanning, during their lifetime.[3] Despite the growing trend, the U.S. Government has failed to pass proper regulations protecting biometric data, and there are currently no federal laws governing the collection, use, and protection of this category of information.[4] The unrestricted use of biometric technology and data creates a large threat to consumer privacy and national security.

Biometric data is highly sensitive, as identifiers are tied to each unique individual. A malicious entity with sufficient access to this data can endanger an individual's identity; compromise certain accounts, buildings, and files; and perhaps implicate individuals in a crime.[5] Many biometric identifiers contain highly sensitive information beyond the scope of identification, such as health, race, gender, ethnicity, personality, and emotions, which can be used to target and attack individuals in other ways. However, unlike a credit card or password, if biometric information is compromised, it is nearly impossible to change. *Therefore, the damage from a biometric data breach can be lifelong*. As such, the lack of proper regulation of biometric data imposes significant privacy risks to U.S. citizens.

Beyond creating individual privacy risks, the absence of biometric information protection also creates national security risks. Biometric data enables identification and tracking capabilities to a greater extent than previously possible. Adversaries can gain access to this information and create powerful biometric databases of U.S. citizens, thereby posing a threat to our defense and intelligence missions. Despite these threats, biometric technology should not be avoided. Rather, we must implement this technology with caution and with the proper protections in place.

The Potomac Institute seeks to address improvements to biometric data policy that include privacy and security protections, while simultaneously allowing for research and innovation. This report provides findings on current biometric data practices and vulnerabilities, reviews current domestic policy, identifies shortcomings, and provides our recommendation for a policy approach to biometric data privacy. Ultimately, we suggest that to uphold American citizens' right to privacy and promote national security, comprehensive federal legislation must be passed that regulates the collection, use, distribution, and security of biometric data.

Photo credit: www.depositphotos.com

Findings

1. ***The amount of biometric data being generated in the United States is rapidly increasing.***

   There has been a growing trend across multiple industries in the last decade to implement new technologies that utilize and store biometric data for authentication and authorization purposes. Current estimates place the number of consumers who have used biometric technology in some capacity at over 75%. Expanded use of biometrics across multiple sectors has caused the U.S. biometrics technology market to increase by roughly $300 million annually since 2014, and the forecast calls for continued annual market growth of roughly 19% to 2025. Data collection has been a developing trend in this century. Biometric data is no exception, and it opens the door to the collection and use of more comprehensive, sensitive, and largely immutable personal information.

2. ***Biometric identifiers can reveal sensitive information about a person, including gender, race, ethnicity, and physical and mental health.***

   Most biometric features can disclose information about physiological or pathological conditions. For example, genotypes, a form of biometric information, can reveal information about ethnicity and the occurrence of, or predisposition towards, a host of genetic diseases. Certain fingerprint patterns are related to chromosomal diseases, iris patterns can reveal genetic sex and race, and behavior biometrics can reveal neurological diseases and detect emotions.

3. ***The United States lacks federal biometric data privacy laws, leaving consumers vulnerable.***

   Although many bills have been proposed, policymakers have been unable to pass a federal data privacy law. As such, no comprehensive federal policy pertaining to biometric data exists. The Health Insurance Portability and Accountability Act (HIPAA) does not apply to most biometric data, as it is typically collected outside of covered entities (i.e., health plans, healthcare clearing houses, and health care providers). A small number of states have passed laws that apply to biometric data privacy, which results in only a patchy legal framework to protect U.S. citizens.

4. ***The United States lacks federal biometric data cybersecurity laws, which has resulted in national security risk and consumer vulnerability.***

   Due to the lack of federal cybersecurity regulations for biometric data, identifying information is stored within insecure databases. Once biometric information is stolen, adversaries such as China and Russia could create powerful biometric databases that could be used to identify most Americans. These adversaries could then identify U.S. operatives and compromise national security and defense missions. Moreover, adversaries could use stolen biometric data to access sensitive accounts, steal identities of U.S. citizens, and implicate targeted individuals in crimes.

Recommendation

The U.S. Government should pass federal legislation aimed at protecting privacy and security through regulation of biometric information.

A comprehensive policy to protect citizens' privacy and national security should cover consent, transparency, authority, business practices, and stringent cybersecurity best practices requirements for the use of biometric information.

BACKGROUND

Privacy

In order to effectively deal with future challenges in biometric data privacy, the evolving definition and significance of the notion of privacy must be understood. Privacy is an important and fundamental right of U.S. citizens. The right to privacy is alluded to in the fourth amendment of the Constitution, and the case of Griswold v. Connecticut, the Supreme Court established the right to privacy as Constitutional doctrine.[6] Even though privacy has always been important, its definition has changed over time. Before the digital age, privacy meant the "right to be let alone."[7] With this understanding, privacy is something that an individual has so long as entities are denied access to that individual. However, in the information age, the notion of privacy has changed dramatically. People no longer want to be let alone, because they want or need to engage with the offerings of the internet. Internet access provides crucial benefits in areas such as health, education, and employment, and serves as the platform for some of the most significant social spheres of our time.[8] Therefore, privacy has evolved to mean control and protections over the information generated and shared online.[9]

Privacy is of great importance to people for a variety of reasons. Privacy serves as a limit to government and corporate power.[10,11] Privacy affords individuals greater control over their lives and the decisions others make about them based on their personal data.[12] Lastly, privacy protects individuals from negative or harmful data exploitation. Given the significance of privacy, it is imperative that it applies to biometric data.

Biometric Data

To discuss a policy framework, it is important to first define biometric information. Current state laws each define biometric information differently—some being much broader in scope than others. For example, biometric information under the new California Consumer Privacy Act (CCPA) is defined broadly to include physiological, biological, and behavioral characteristics. This means that under CCPA, traditional markers, such as fingerprints and facial recognition, and non-traditional markers, such as keystroke and gait patterns, are all considered biometric information.[13] Washington notably has an expansive definition, although theirs is limited to biological characteristics.[14] On the other hand, Illinois and Texas define biometric information more narrowly by limiting it to specific types of information, such as retina or iris scans, voiceprints, and face or hand geometry.[15]

For this report, ***biometric information*** **is defined broadly as "physiological and behavioral characteristics that can be used to uniquely identify an individual."** We use this broad definition because increasingly, as technologies collect a widening range of identifying characteristics, regulations will need definitions that allow these technologies to fall under the scope of law to provide adequate protection.

Physiological Biometrics: Physiological biometric data is information collected that offers recognition of an individual through their specific biological measurements, dimensions, and characteristics.[16] The most common examples of physiological biometrics include deoxyribonucleic acid (DNA), facial characteristics, hand characteristics, fingerprints,

and iris and retina scans.[17] Below is a more in-depth description of what type of information is collected for these common physiological biomarkers and how they are used in society.

DNA/Genotype: In DNA or genotype matching, analysis of segments of DNA are used to identify an individual.[18] The use of DNA/genotypes as a biometric marker for identification purposes is more or less limited to forensics, immigration, defense, and healthcare.[19] However, the amount of genetic data has risen dramatically in the last few years due to the increased popularity of direct-to-consumer (DTC) genetic testing. In 2013, the number of consumers who had used consumer genetic testing was roughly 300,000 as compared to over 26 million by 2019.[20] While this data may be collected for purposes other than identification, it nevertheless could be used as a unique biometric identifier. If genetic data from DTC companies is "de-identified," then it is permissible for that data to be shared between researchers, posted to public databases, and bought and sold between firms.[21,22] *However, there is essentially no such thing as de-identified genetic data*. Researchers have shown that, for the vast majority of Americans, genomic data can be reattached to the identity via family maps created by public genealogy databases.[23] In light of this, even genotypes mapped through consumer websites should be considered biometric data.

The type of information that can be revealed about a person through analysis of their genome includes sensitive information about health, physical traits, ancestry, and genealogy.[24,25] Only analysis of a fraction of a percent of the genome is required for such information to be revealed. Moreover, researchers are constantly uncovering new connections between genes and traits, meaning that in the future, much more information can be revealed about someone through their genotype than is currently possible. Lastly, genotypes reveal information not only about the individual being analyzed, but about their family, as well.

Iris/Retina Recognition: Iris recognition involves the scanning of an individual's eye to identify unique biological features of the iris. Similarly, retina recognition utilizes scans to identify individuals based on the unique patterns of veins at the back of the eye.[26] Retinal scans require the individual to be in close proximity, but irises can be covertly scanned at a distance.[27] Iris and retinal scans are largely used by the military and law enforcement agencies, but iris scans are also used in hospital and healthcare settings; consumer electronics, including certain smartphones; and financial institutions.[28] For example, iris recognition scans are used by Google to authorize datacenter access,[29] and by Samsung for authentication purposes in the Galaxy S8 phone.[30] While the use of iris and retina recognition is increasing in the United States, it is used less than other biometric identification methods such as fingerprinting and facial recognition.[31]

Iris and retinal scans can potentially be used for more than just identifications purposes. It is believed that iris patterns are linked to certain personality traits due to the PAX6 gene. This gene helps control the development of the iris during the embryonic stages of life, and mutations in this gene are linked to personality traits like impulsiveness and poor social skills.[32] In one study at Orebro University, researchers found that surveyed individuals who had more crypts in their iris tended to self-report being warmer and more trusting, and individuals who had more furrows in their iris tended to self-report being more neurotic and impulsive.[33] Moreover, researchers from

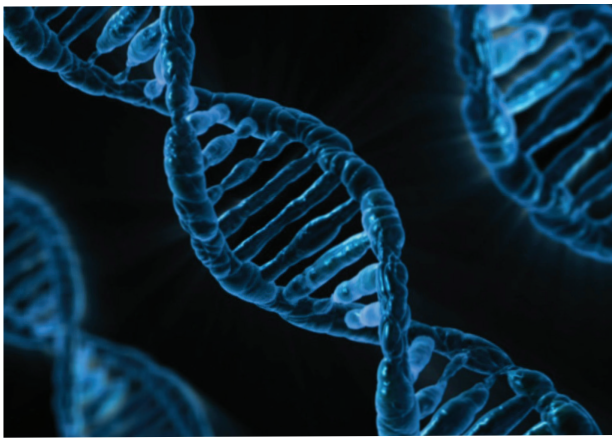


Photo credit: www.shutterstock.com

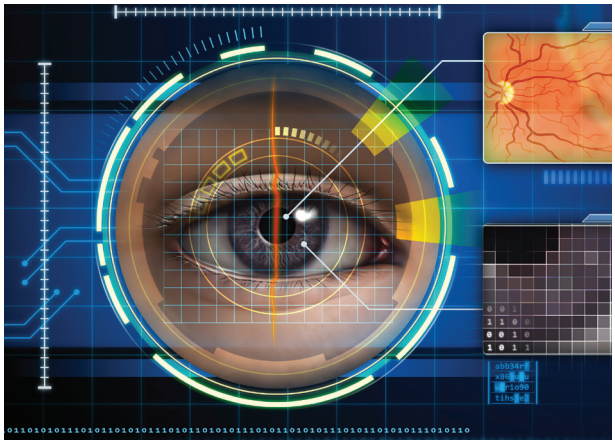


Photo credit: www.depositphotos.com

the University of Notre Dame in Southbend developed a system that shows promise for being able to distinguish between people of different racial backgrounds and sexes from iris scans.[34]

Facial Recognition and Hand/Ear Geometry Recognition: Facial recognition involves the analysis of facial features for authentication/recognition purposes.[35] Hand and ear geometry recognition uses geometric features, such as finger length, hand width, or ear shape to identify an individual.[36]

The use of facial recognition is increasing across many industries, such as finance, but it is still most prevalent in security, consumer electronics, and social media. Large companies such as Facebook[37] and Snapchat[38] use facial recognition software on their customers' pictures. Smartphones also carry facial recognition technology, and it is estimated that by 2020, 60% of all smartphones will have facial recognition capabilities.[39] Facial recognition technology can be used covertly at a distance, and this practice is currently legal in most areas of the United States.[40] Beyond identification purposes, facial recognition has been used for emotion recognition.[41] In 2016, Facebook acquired FacioMetrics, an emotion detection startup.[42]

Fingerprint Recognition: Fingerprint recognition uses the minute ridges and valleys found on the surface of fingertips to identify an individual.[43] Fingerprint scanning is currently the most common type of biometric authentication, with 57% of organizations currently using this method.[44] Fingerprints are used across many agencies including defense, law enforcement, border and travel security, education, finance, health care, cybersecurity, human resources, and electronics.[45] In 2017, 55% of smartphones shipped globally had fingerprint sensors. Today, over 70% of phones are equipped with such sensors.[46] Many apps utilize the fingerprint sensing technology built into smartphones, including financial apps such as Bank of America and gaming apps such as the Google Play Store.[47]

Beyond authentication, fingerprints can also reveal specific health information, such as identification of individuals with chromosomal abnormalities, for example, Down syndrome,[48] Klinefelter syndrome,[49] and congenital blindness,[50] among others.

Behavioral Biometrics: Behavioral biometric data offers recognition of an individual related to specific measurements of unique human activity patterns.[51] The most common examples of behavioral biometrics include voice identification/verification, typing/handwriting recognition, and gait recognition.[52] Behavioral biometrics are used much less often than physiological biometrics for identification purposes. This is because behavioral biometrics tend to be more difficult to obtain and analyze, and can be less accurate because they are more susceptible to change over time.[53] Nonetheless, the use of behavioral biometrics is increasing, especially for voice verification in the context of electronic personal assistants and customer service call centers.[54] Behavioral biometrics can reveal insights into an individual's gender, age, region of origin, health, and emotional state.

Trends in Biometric Information Usage

There are many reasons that the use of biometric data has increased in recent years. Weak passwords can be easy to guess, which increases the risk of data breaches. Even strong passwords are vulnerable to cyberattacks, especially if they can be reset easily, if they are reused on multiple sites,

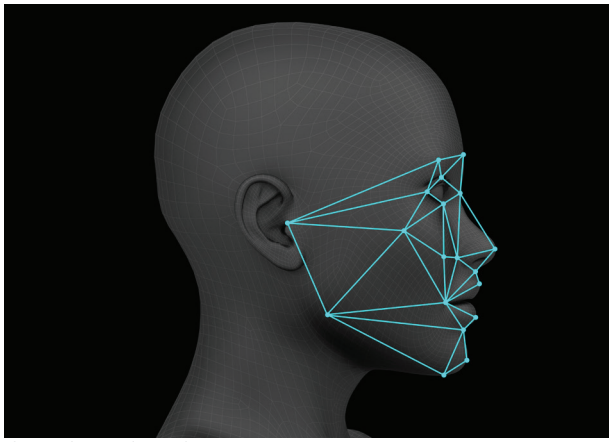


Photo credit: www.depositphotos.com

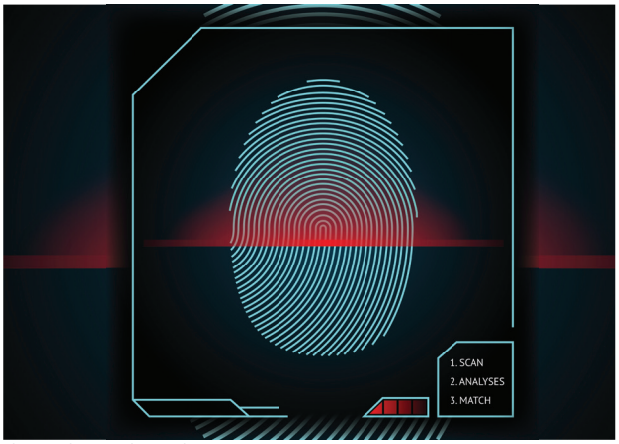


Photo credit: www.depositphotos.com

or if they can be hit with an automated brute-force attack.[55] Passwords can also be difficult to remember, creating obstacles for people trying to access important goods and services. Moreover, using passwords for authentication can be expensive for a company. During an interview with CNN, Alex Simons, Director of Program Management in Microsoft's identity division, said that they spend over $24 million a year in help desk calls regarding people needing to reset their passwords.[56] Overall, biometric identification is viewed as the more secure and more efficient option than passwords.

There are many new technologies that now utilize and store biometric data. This includes personal assistants from companies such as Amazon, Google, and Apple that store and process unique vocal patterns in the cloud.[57] It includes DNA kits that recently emerged on the commercial market and maintain genotypes on file. Mobile devices and Internet of Things have also led to increased usage of biometric data. Cellular phones, tablets, and door cameras capture different forms of biometric data, whether it be fingerprints or facial recognition, and store it on the device or in the cloud.[58] There are also many facets of life where the novel use of biometric recognition may be less obvious. Casinos employ facial recognition to spot banned gamblers such as known card counters.[59] Banks use voice recognition to verify customers over the phone.[60,61] The Nymi wristband uses employees' heartbeats to authenticate them to access a corporate network.[62] And hospitals use Imprivata's PatientSecure to identify patients via the unique vein patterns in the palms of their hands.[63]

With all of these emerging uses of biometric information, it is no surprise that current estimates place the number of consumers who have used biometric technology in some capacity at over 75%.[64] Increased use of biometrics in numerous sectors including government, defense and security, and consumer electronics, has caused the U.S. biometrics technology market size to increase roughly $300 million annually since 2014, and the market is forecasted to continue to grow annually roughly 19%

to 2025.[65] In 2017, the share of smartphone shipments with facial recognition was 5%, as compared to 40% in 2019, with an expected increase to 64% in 2020.[66] This rapid proliferation of biometric data generation has many implications for privacy and security, *given that the information serves as personal, and largely permanent, identifiers*.

CURRENT BIOMETRIC DATA VULNERABILITIES AND POLICIES

Privacy Concerns

Privacy is one of the most important social and political issues of our time. As previously stated, privacy is important because it limits government and corporate power, protects individuals from harm and exploitation, and gives people more control over their lives and the decisions made about them. The rise of biometric data generation in the absence of federal regulation increases concerns of insufficient safeguarding of biometrics information and inadequately upheld privacy rights.

Protection of biometric data privacy is particularly important for numerous reasons.

1. **Biometric identifiers are almost exclusively permanent.** Unlike a credit card number or password, biometric data is incredibly hard to change. If an individual's fingerprint data or facial information is compromised, that individual could use prosthetics or facial alteration surgery to recover after a data breach. However, these solutions are expensive and can take heavy tolls on the individual, potentially threatening their sense of identity.

2. **Biometric data can reveal more than just an identity.** As discussed in the background section, biometric data can reveal sensitive information about a person's gender, race, ethnicity, physical and mental health, and emotional state. This information could be used nefariously to target, assess, discriminate against, and attack individuals and groups.

3. **Biometrics can be used to steal identity.** Once an individual's biometric data is compromised, that person can lose a great deal of control over their lives and incur a significant amount of damage. Once an entity gains access to an individual's biometric data, that entity could access the individual's accounts and even implicate the individual in a crime.

Despite the importance of biometric data privacy, there is little federal regulation of the collection and use of biometric data. For example, facial recognition can be performed inconspicuously from a distance, and this is legal in most parts of the country. Storekeepers could theoretically partner with companies such as Facebook, which has a vast database of identified faces, and use facial recognition to get information about their customers when they enter the store. The customer information they could obtain includes, for example, name, address, income, and credit score.[67] Clearly, this undermines key tenants of privacy including consent to who has access to personal information and how it can be used.

Lack of federal regulation and insufficient security guidelines regarding biometric data also threaten privacy and leave people vulnerable to hackers. Numerous examples of large-scale breaches of biometric data already exist. One such attack took place in 2015, when hackers stole the fingerprints of 5.6 million workers from the federal government Office of Personnel Management.[68,69] With this type of raw biometric data, hackers could access sensitive information, gain entry to buildings, and steal identities. Moreover, damage from this type of attack is long lasting. As long as those 5.6 million individuals live, unless they take drastic measures to alter their fingerprints, their privacy and security will be compromised.

Another example of such a breach involves the British company Biostar 2, a web-based security platform working with organizations from the United States. In this incident, the fingerprints, facial recognition data, usernames, passwords, and other personal information of over one million people were found to be easily accessible to hackers. The biometric information was largely unprotected and unencrypted meaning that hackers could see data from U.S. organizations working with the company. Fortunately, this was discovered by researchers rather than hackers. Wide-ranging damage could have occurred had the hackers discovered it first, especially considering that many of the companies working with Biostar 2 are banks and defense contractors.[70]

The amount of effort required for hackers to hijack systems and cause damage depends on the sophistication of security systems. Breaches involving

raw data take less effort to carry out.[71] While many entities do store raw biometric data, many do not. Some less advanced security systems will accept photos, for example, rather than raw data. However, malicious attacks can still be carried out even when not storing raw biometric data. An example of this occurred in 2016 when investigators were able to break into a criminal's cellular device by printing a fingerprint onto photographic paper.[72] Even with more sophisticated security systems, hackers could use data that isn't raw by creating a 3D printed mold based on a fingerprint picture. In 2017, scientists were able to use this type of 3D printed fingerprint made of silicon to fool capacitive scanners, ultrasound scanners, and optical scanners.[73] Until greater security measures are federally mandated so that biometric data cannot be accessed and used without authorization, people's right to privacy cannot be realized.

Photo credit: www.depositphotos.com

National Security Concerns

Accessibility of biometric information does not only create privacy concerns. It creates national security concerns, as well. *It is possible for an adversary to download millions of genetic data files from public genealogy websites by uploading fake genetic profiles*.[74,75,76] A foreign counterintelligence agency could download and access over a million U.S. DNA profiles. Using family mapping, that foreign intelligence agency would then be able to identify nearly every American. They could identify spies and diplomats, find compromising information about American targets, discover genetic kompromat, or uncover health-related predispositions. Moreover, DTC genetic companies are allowed to exchange genetic information with third parties as long as the genetic information has been de-identified. However, as stated earlier, researchers have shown that *most genetic samples can be re-identified*. Therefore, adversaries could be paying for genetic information, including that of servicemembers, and then re-identifying them. The Pentagon recently warned employees of threats posed by using take-home DNA tests.[77] Even if Pentagon employees refrained from using the tests, if their relatives use the tests, their identity is still compromised. This problem applies to more than just genetic biometric information. As all types of biometric data are being generated across multiple industries with minimal protection, U.S. operatives become more limited in their ability to work covertly. The exposure of biometric information creates increased risk to the Joint Force and to U.S. missions.[78]

Current U.S. Federal Laws and Regulations

There is no single principal data privacy legislation in the United States. Instead, there are sector-specific and type-specific federal data protections. There exists a health information privacy law, the Health Insurance Portability and Accountability Act (HIPAA), but it only applies to data collected by covered entities. Covered entities are defined in the HIPAA rules as health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards.[79] Because most biometric data is not collected by covered entities, most biometric data in existence does not fall within the scope of HIPAA, so its privacy laws do not apply. There are no comprehensive federal laws regulating the collection or use of biometric data.

Current U.S. State Laws and Regulations

Currently, only four U.S. states, California, Illinois, Washington, and Texas, have statutes specifically dedicated to the protection of biometric information. The California Consumer Privacy Act (CCPA) provides individuals with certain rights regarding their personal information, which by definition includes biometric data. Under this law, individuals can request to see data collected and stored about them, request data about them be deleted, and prohibit the use or disclosure of data collected about them. Moreover, companies that store personal information, and therefore biometric data, must implement stringent security and protection protocols.[80] This law applies to for-profit entities doing business in California that have annual gross revenues exceeding $25 million, that have the personal information of 50,000 or more consumers, or that earn more than half of their annual revenue from selling consumers' personal information.[81] The Illinois Biometric Information Privacy Act (BIPA), was the first state biometric privacy law and has served as

the foundation upon which Washington and Texas would later draw upon. BIPA is comprehensive and sweeping, and its main requirements are:

- businesses must have informed consent before collecting biometric data;
- businesses have limited rights for disclosure;
- businesses cannot profit from biometric data;
- businesses must protect and retain biometric data according to the statues; and
- individuals have a private right of action under circumstances in which businesses do not comply with the statute.[82]

Washington and Texas' biometric laws are very similar to Illinois' but they do not give their citizens a private right of action clause.[83] While these are the only states with statutes specifically dedicated to the protection of biometric information, Arizona, Florida, and Massachusetts have recently proposed legislation addressing the issue of biometric privacy.[84]

While these state laws are a good first step in the right direction, they do not adequately address the need for greater cybersecurity of biometric information, and they create at best a patchy legal framework, which is an issue when dealing with data that can easily cross state lines. The necessary solution to sufficiently addressing biometric data privacy rests in the passing of comprehensive federal legislation.

RECOMMENDATION

Privacy and Security Prioritization

The U.S. Government should pass federal legislation aimed at protecting privacy and security through regulation of biometric information.

Consent: Consent is an integral component of privacy because it serves as a way for individuals to exercise control over their personal information. It is important to give individual consumers control over their own sensitive biometric data, as this data is more or less permanently tied to the individual and can reveal fundamental insights about them. We recommend that federal legislation require entities to obtain an individual's consent for both the collection and analysis of biometric identifiers (exceptions may be made for legal guardians and law enforcement). Federal legislation should also require that entities obtain consent for the retention of samples once their intended purpose has been satisfied. Lastly, we recommend that federal legislation require entities to obtain consent for the distribution of biometric information to any third-party entities, and individuals should be given the right to withdraw consent at any time.

Transparency: Transparency is necessary for digital privacy because it enables consumers to make informed decisions about who they trust with their data. We recommend that federal legislation require entities to provide each individual access to their own collected biometric information. We further recommend that federal legislation require entities to disclose biometric information usage via annual reports to individuals.

Authority: Authority, and therefore control, over data is necessary for privacy. Data is essential to many decisions made about individuals. Thus, giving people authority over their information gives them more control over their lives and better enables people to protect themselves. As such, we recommend that federal legislation give individuals the right to request deletion of their collected biometric data. Legislation should also give consumers a private right of action for recourse if entities fail to act in response to a troublesome practice regarding biometric data. If biometric data is compromised, the amount of harm that could result is far reaching and long lasting. Individuals exposed to the potential harm should have recourse. Furthermore, legislation should define biometric data as the property of the individual from which it came. Lastly, legislation should require that entities provide to consumers a brief summary of all of the rights provided in this legislation, including displaying the summary on products and on the front page of entities' websites.

Business Practices: We recommend that entities be prohibited from profiting from the distribution of biometric data. Biometric information is replacing passwords and other methods of authentication and verification. Entities are not allowed to sell, trade, lease, or otherwise profit off of passwords, and similarly, they should not be allowed to profit from the distribution of biometric data.

Security of Data: Insufficient security over biometric information poses a threat to the privacy and safety of individuals, and this nation as a whole. We recommend that biometric information be defined as physiological and behavioral characteristics that can be used to uniquely identify an individual. We believe that this broad definition ensures that new technologies, which assess a growing range of characteristics that can identify individuals, will fall under the scope of federal law to more aptly provide privacy and protection. We recommend that entities constructing and maintaining files of biometric information be required to both employ cybersecurity best practices and develop stringent standards for protection of biometric information.

The following are examples of cybersecurity best practices that could be required for biometric information. In the PricewaterhouseCoopers Legal, LLP report "Biometrics and Privacy," it is advised that companies should not retain biometric information on their centralized servers, but rather, companies should rely on a system where the biometric information is stored on the user's device.[85] Then, when a consumer does business with a third-party, the device and the website can exchange confirmation signals to verify identity. This is how the iPhone's Apple Pay works, and it is becoming standardized through protocols such as Fast Identity Online (FIDO).[86] This method would allow people to have greater control over their biometric data and would drastically reduce the volume of biometric data at risk in a given hack. However, it should be noted that a drawback of storing biometric information on a device is that if the device is hacked, the malicious user will have access to a more detailed profile of the owner due to the personal data already stored there. This issue could be addressed by requiring additional security for device biometric information.

Another way that consumers' biometric information should be protected is through encryption. A digital key can be securely bound to each biometric in order to minimize hackers' access to raw data. Entities with databases that store biometric information, regardless of the type of encryption used should be expected to use secure algorithms. They should also be expected to update the systems they use in accordance with the most recent publications from the National Institute for Standards and Technology (NIST).

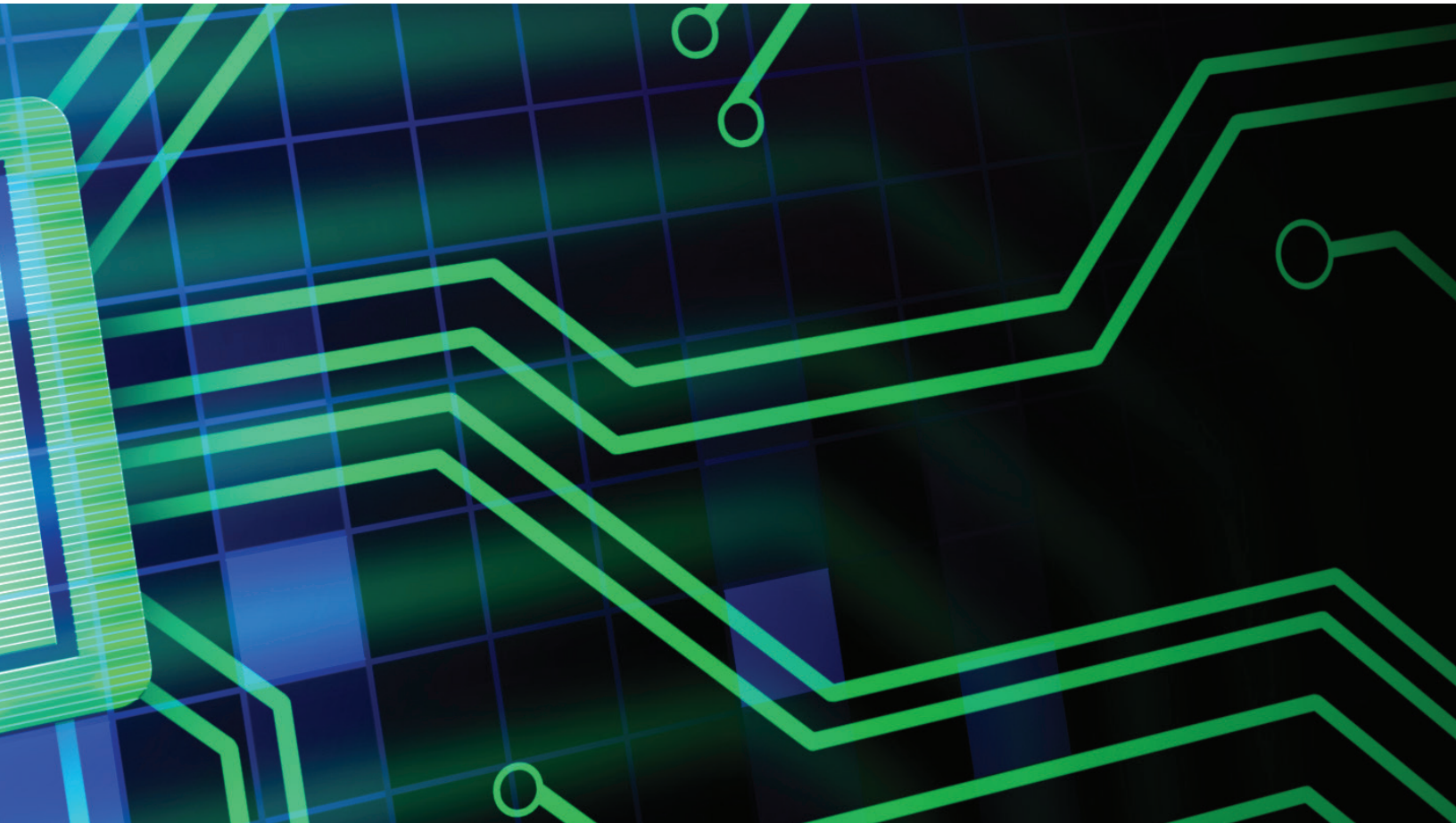
Looking towards the future, instead of using encrypted biometric data, entities could consider using hash functions as a secure method of verifica-

tion. Under this system, the entity would be federally required to delete the biometric data. The only thing that would be stored on a database, then, are hash codes and names of the people they correspond to. To authenticate a user, the live biometric presented by the user would be hashed and compared with the entity's stored information. If a breach occurs, hackers will only have access to hash digests, which are extraordinarily difficult to reverse engineer.[87] This is just one possible method among many that could be employed in the future to make biometric authentication more secure.

The bottom line is that stringent cybersecurity best practices should be required for biometric information in order to promote individual and national security to the fullest extent feasible.

CONCLUSIONS

The last decade of the information age has seen an explosion in personal data generation and use, and biometric data is no exception. Undoubtedly, the use of biometrics for authentication and verification provides certain benefits. Biometric identifiers arguably protect privacy because they are more difficult to copy than other authentication and verification methods. They are unique to individuals, which helps to restrict access to personal information. Also, biometrics do not need to be remembered by consumers, which provides convenience to consumers and financial savings to companies. Given these benefits, the prevalence of biometric information data use will continue to grow. However, it is of paramount importance to also acknowledge and address the new privacy and security threats posed by the use of biometric identification. Unlike other forms of personally identifying information, **biometric data is almost exclusively permanently linked to individuals, can reveal significantly more sensitive information, and can be used for indiscriminate targeting, tracking, and attacking**. If biometric information is breached, the damage to an individual can be substantial and long lasting. U.S. citizens cannot realize their right to privacy as long as this very sensitive and important category of information has little to no regulatory protections. Moreover, the United States is vulnerable to adversaries using our citizens' biometric information against us. This will not change until the federal government requires stronger and more comprehensive cybersecurity practices. We should not resist new biometric technology, but we must use caution in how we govern its collection, use, and distribution.



ENDNOTES

1. September 2018. Biometrics Technology Market Analysis Report By End-Use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), and Segment Forecasts, 2018-2025. Grand View Research. Retrievable from: https://www.grandviewresearch.com/industry-analysis/biometrics-industry.
2. Larson, S. March 18, 2018. Beyond passwords: Companies use fingerprints and digital behavior to ID employees. CNN Business. Retrievable from: https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html.
3. Lui, S. May 22, 2019. Biometric Technologies- Statistics & Facts. Statista. Retrievable from: https://www.statista.com/topics/4989/biometric-technologies/.
4. Wernick, A. July 2, 2019. Biometric Information- Permanent Personally Identifiable Information Risk. American Bar Association. Retrievable from: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_8/.
5. Tynan, D. February 21, 2017. What are the risks of biometric identification? The Parallax. Retrievable from: https://the-parallax.com/2017/02/21/risks-biometric-identification/.
6. McKay, R. December 1965. The Right of Privacy: Emanations and Intimations. Michigan Law Review. Retrievable from: https://www.jstor.org/stable/1287069?seq=1.
7. Westin, A. April 29, 2003. Social and Political Dimensions of Privacy. Journal of Social Issues. Retrievable from: https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/1540-4560.00072.
8. Coward, C; Sey, A. August 14, 2013. Global Impact Study of Public Access to Information & Communication Technologies. University of Washington. Retrievable from: https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/51519/IDL-51519.pdf?sequence=1&isAllowed=y.
9. March 25, 2015. The evolution of the concept of privacy. EDRi. Retrievable from: https://edri.org/evolution-concept-privacy/.
10. Gavison, R. 1980. Privacy and the limits of Law. Yale Law Journal. Retrievable from: https://www.jstor.org/stable/795891?seq=1.
11. Aquisti, A; Taylor, C; Wagman, L. June 2, 2016. The Economics of Privacy. Journal of Economic Literature. Retrievable from: https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442.
12. West, S. July 5, 2017. Data Capitalism: Redefining the Logistics of Surveillance and Privacy. Business & Society. Retrievable from: https://journals.sagepub.com/doi/10.1177/0007650317718185.
13. McGinley, M; Brotman, K; Rigney, E. March 25, 2019. The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States. The National Law Review. Retrievable from: https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.
14. Ibid.
15. Ibid.
16. Koong, C; Yang, T; Tseng, C. July 24, 2014. A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. The Scientific World Journal. Retrievable from: https://doi.org/10.1155/2014/781234.
17. Slobodan, R; Pavešić, N. 2017. De-identification for privacy protection in biometrics. Institution of Engineering and Technology. Retrievable from: https://bib.irb.hr/datoteka/923532.PBSE0040_Vielhauer_Chapter13_Proof-1.pdf.
18. Types of Biometrics. Biometrics institute. Retrievable from: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.
19. November 26, 2019. What are single nucleotide polymorphisms (SNPs)? Genetics Home Reference. U.S. National Library of Medicine. Retrievable from: https://ghr.nlm.nih.gov/primer/genomicresearch/snp.
20. Daniel, R; Sanchez, J; Nassif, N; Hernandez, A; Walsh, S. August 2008. SNPs associated with physical traits: A valuable tool for the inference of biogeographical ancestry. Forensic Science International: Genetics Supplement Series. Retrievable from: https://www.sciencedirect.com/science/article/pii/S1875176808001959.
21. DNA Biometrics. International Biometrics Identity Association. Retrievable from: https://www.ibia.org/biometrics-and-identity/biometric-technologies/dna.
22. Regalado, A. 2019. More than 26 million people have taken an at-home ancestry test. Retrievable from: https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.
23. Molteni, M. May 1, 2019. The U.S. Urgently Needs New Genetic Privacy Laws. Retrievable at: https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/.
24. Clayton, E; Evans, B; Hazel, J; Rothstein, M. 2019. The law of genetic privacy: application, implications, and limitations. Retrievable at: https://academic.oup.com/jlb/advance-article/doi/10.1093/jlb/lsz007/5489401.
25. Erlich, Y; Shor, T; Pe'er, I; Carmi, S. November 9, 2018. Identity inference of genomic data using long range familial searches. Nature. Retrievable at: https://www.ncbi.nlm.nih.gov/pubmed/30309907.
26. Types of Biometrics. Biometrics institute. Retrievable from: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.
27. October 25, 2019. Street-Level Surveillance: Iris Recognition. Electronic Frontier Foundation. Retrievable from: https://www.eff.org/pages/iris-recognition.
28. September 2019. Iris Recognition Market- Growth, Trends, and Forecast (2020-2025). Kenneth Research. Retrievable from: https://www.mordorintelligence.com/industry-reports/iris-recognition-market.
29. September 18, 2013. Security and Data Protection in a Google Data Center. Google. Retrievable from: https://www.youtube.com/watch?v=cLory3qLoY8.
30. Security. Samsung. Retrievable from: https://www.samsung.com/global/galaxy/galaxy-s8/security/.
31. Thakkar, D. 2015. Global Biometric Market Analysis: Trends and Future Prospects. Bayometric. Retrievable from: https://www.bayometric.com/global-biometric-market-analysis/.

32. Larsson, M; Pedersen, NL; Stattin, H. May 2007. Associations between iris characteristics and personality in adulthood. Biological Psychology. Retrievable from: https://doi.org/10.1016/j.biopsycho.2007.01.007.

33. Larsson, M. 2007. Human Iris Characteristics as Biomarker for Personality. Orebro University. Retrievable from: https://pdfs.semanticscholar.org/81c0/6c35e2ae8ddd46b8423331d0bf44da919ff6.pdf.

34. Sandhana, L. October 12, 2011. Iris scanner could tell your race and gender. NewScientist. Retrievable from: https://www.newscientist.com/article/mg21228346-000-iris-scanner-could-tell-your-race-and-gender/.

35. Types of Biometrics. Biometrics institute. Retrievable from: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

36. Ibid.

37. Simonite, T. March 17, 2014. Facebook Creates Software That Matches Faces Almost as Well as You Do. MIT Technology Review. Retrievable from: https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

38. Ghosh, S. August 29, 2018. Snapchat figured out how to analyze people's selfies to score their emotions. Business Insider. Retrievable from: https://www.businessinsider.com/snapchat-patent-uses-facial-recognition-detect-mood-2018-8.

39. Naiya, P. February 7, 2018. More than one billion smartphones to feature facial recognition in 2020. Counterpoint. Retrievable at: https://www.counterpointresearch.com/one-billion-smartphones-feature-face-recognition-2020/.

40. Houser, K. November 15, 2019. Protestors Wearing Head-Mounted Cameras Scan 13,000 Faces In DC. Futurism. Retrievable from: https://futurism.com/the-byte/protestors-cameras-scan-faces-dc.

41. Inderscience Publishers. April 27, 2016. Emotion detector: Facial expression recognition to improve learning, gaming. Science Daily. Retrievable from: https://www.sciencedaily.com/releases/2016/04/160427103627.htm.

42. Constine, J. November 16, 2016. Like by smiling? Facebook acquires emotion detection startup FacioMetrics. TechCrunch. Retrievable from: https://techcrunch.com/2016/11/16/facial-gesture-controls/.

43. Types of Biometrics. Biometrics institute. Retrievable from: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

44. Larson, S. March 18, 2018. Beyond passwords: Companies use fingerprints and digital behavior to ID employees. CNN Business. Retrievable from: https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html.

45. Fingerprint Biometrics. International Biometrics Identity Association. Retrievable from: https://www.ibia.org/biometrics-and-identity/biometric-technologies/fingerprints.

46. Holst, A. July 12, 2019. Global smartphone fingerprint sensor penetration rate 2014-2018. Statista. Retrievable from: https://www.statista.com/statistics/804269/global-smartphone-fingerprint-sensor-penetration-rate/.

47. Raphael, JR. May 3, 2016. 16 standout Android apps with fingerprint support. Computerworld. Retrievable from: https://www.computerworld.com/article/3063544/android-apps-fingerprint-support.html.

48. Rajangam, S; Janakiram, S; Thomas, IM. December 31, 1994. Journal of the Indian Medical Association. 93(1):10-13.

49. Komatz, Y; Yoshida, O. 1976. Finger Patterns and Ridge Counts of Patients with Klinefelter's Syndrome (47, XXY) among the Japanese. Human Heredity. 26:290-297. Doi: 10.1159/000152816.

50. Viswanathan, G; Singh, H; Ramanujam, P. 2002. Dermatoglyphic analysis of palmar print of blind children from Bangalore. Journal of Ecotoxicology and Environmental Monitoring. 12:73-75.

51. Koong, C; Yang, T; Tseng, C. July 24, 2014. A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. The Scientific World Journal. Retrievable from: https://doi.org/10.1155/2014/781234.

52. Slobodan, R; Pavešić, N. 2017. De-identification for privacy protection in biometrics. Institution of Engineering and Technology. Retrievable from: https://bib.irb.hr/datoteka/923532.PBSE0040_Vielhauer_Chapter13_Proof-1.pdf.

53. German, R; Barber, KS. November 2016. Current Biometric Adoption and Trends. The University of Texas at Austin Center for Identity. Retrievable from: https://identity.utexas.edu/assets/uploads/publications/Current-Biometric-Adoption-and-Trends.pdf.

54. Ibid.

55. Maurer, R. April 6, 2018. More Employers Are Using Biometric Authentication. Society for Human Resource Management. Retrievable from: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-using-biometric-authentication.aspx.

56. Larson, S. March 18, 2018. Beyond passwords: Companies use fingerprints and digital behavior to ID employees. CNN Business. Retrievable from: https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html.

57. Phillips, J. February 6, 2019. BeyondTrust expert on why biometric data poses unique security risk. Intelligent CIO. Retrievable from: https://www.intelligentcio.com/eu/2019/02/06/beyondtrust-expert-on-why-biometric-data-poses-unique-security-risk/.

58. Ibid.

59. Houser, K. April 24, 2019. Casinos Are Using Facial Recognition To Keep Banned Gamblers Away. Futurism. Retrievable from: https://futurism.com/the-byte/casinos-facial-recognition-problem-gamblers.

60. Groenfeldt, T. June 27, 2016. Citi Uses Voice Prints To Authenticate Customers Quickly And Effortlessly. Forbes. Retrievable from: https://www.forbes.com/sites/tomgroenfeldt/2016/06/27/citi-uses-voice-prints-to-authenticate-customers-quickly-and-effortlessly/#7c8a3485109c.

61. Hickey, S. March 27, 2016. Banks will recognize your voice when you call them with a query. The Guardian. Retrievable from: https://www.theguardian.com/money/2016/mar/27/banks-voice-recognition-video-mortgage-advice.

62. Yury, C. 2014. Your Heartbeat May Soon Be Your Only Password. Wired. Retrievable from: https://www.wired.com/insights/2014/06/heartbeat-may-soon-password/.

63. Gormley, B. February 6, 2019. Hospitals Turn to Biometrics to Identify Patients. The Wall Street Journal. Retrievable from: https://www.wsj.com/articles/hospitals-turn-to-biometrics-to-identify-patients-11549508640.

64. Lui, S. May 22, 2019. Biometric Technologies- Statistics & Facts. Statista. Retrievable from: https://www.statista.com/topics/4989/biometric-technologies/.

65. September 2018. Biometrics Technology Market Analysis Report By End-Use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), and Segment Forecasts, 2018-2025. Grand View Research. Retrievable from: https://www.grandviewresearch.com/industry-analysis/biometrics-industry.

66. Petrock, V. October 3, 2019. Biometric Marketing 2019. eMarketer. Retrievable from: https://www.emarketer.com/content/biometric-marketing-2019.

67. September 4, 2019. Biometric data and data protection regulations (GDPR and CCPA). Gemalto. Retrievable from: https://www.gemalto.com/govt/biometrics/biometric-data.

68. Roberts, J. May 12, 2016. How Biometrics are Worse than Passwords. Fortune. Retrievable from: https://fortune.com/2016/05/12/biometrics-passwords/.

69. Peterson, A. September 23, 2015. OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought. The Washington Post. Retrievable from: https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

70. Taylor, J. August 14, 2019. Major breach found in biometrics system used by banks, UK police and defense firms. The Guardian. Retrievable from: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms?CMP=share_btn_link.

71. Pandya, J. March 9, 2019. Hacking Our Identity: The Emerging Threats From Biometric Technology. Forbes. Retrievable from: https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology/#591909cc5682.

72. Ibid.

73. Chen, A. September 21, 2019. This fake finger could help make our fingerprint scanners more secure. The Verge. Retrievable from: https://www.theverge.com/2017/9/21/16345500/biometrics-fingerprint-identification-technology.

74. Edge, M; Coop, G. October 22, 2019. Attacks on genetic privacy via uploads to genealogical databases. Retrievable from: https://www.biorxiv.org/content/10.1101/798272v1.

75. Ney, P. 2019. Securing the Future of Biotechnology: A Study of Emerging Cio-Cyber Security Threats to DNA-Information Systems. University of Washington. Retrievable from: https://digital.lib.washington.edu/researchworks/handle/1773/44143.

76. Regalado, A. October 30, 2019. The DNA database used to find the Golden State Killer is a national security leak waiting to happen. MIT Technology Review. Retrievable from: https://www.technologyreview.com/s/614642/dna-database-gedmatch-golden-state-killer-security-risk-hack/.

77. Yilek, C. December 23, 2019. 'Personal and operational risks': Pentagon warns military members against using DNA kits. Washington Examiner. Retrievable from: https://www.washingtonexaminer.com/news/pentagon-warns-military-members-against-using-dna-kits.

78. Neale, S. December 30, 2019. CIA troubled as biometric tracking and digital footprints pull spies from the shadows. Washington Examiner. Retrievable from: https://www.washingtonexaminer.com/news/cia-troubled-as-biometric-tracking-and-digital-footprints-pull-spies-from-the-shadows.

79. October 18, 2017. What Are Covered Entities Under HIPAA? HIPAA Journal. Retrievable from: https://www.hipaajournal.com/covered-entities-under-hipaa/.

80. Miles & Stockingbridge P.C.; Jackson, V; Wells, R. June 5, 2019. Biometric Data: Companies Should Act to Mitigate Risks in the Face of Growing Regulations and Increased Risk for Liability. JDSUPRA. Retrievable from: https://www.jdsupra.com/legalnews/biometric-data-companies-should-act-to-37485/.

81. Myrow, R. December 30, 2019. California Rings In The New Year With A New Data Privacy Law. NPR. Retrievable from: https://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law.

82. McGinley, M; Brotman, K; Rigney, E. March 25, 2019. The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States. The National Law Review. Retrievable from,: https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

83. Ibid.

84. Ibid.

85. Room, S. May 2016. Biometrics and Privacy- On Device vs On Server matching. Pricewaterhouse-Coopers Legal, LLP. Retrievable from: https://digitalidentityguide.com/wp-content/uploads/2018/02/pwc-device-server-biometrics-2018.pdf.

86. Roberts, J. May 12, 2016. How Biometrics are Worse than Passwords. Fortune. Retrievable from: https://fortune.com/2016/05/12/biometrics-passwords/.

87. Magana, G. August 16, 2019. Researchers found fingerprints of more than 1 million people stored by a biometrics company to be vulnerable to breach. Business Insider. Retrievable from: https://www.businessinsider.com/vulnerability-found-in-major-biometrics-system-2019-8.


POTOMAC INSTITUTE FOR POLICY STUDIES
Falicia Elenberg