Purpose Section:

The purpose of this paper is to describe the growing concern of unwarranted use and storage of biometric technology. Biometric technology is technology that is used to identify someone based on an aspect of their biology. This includes technology like fingerprint scanning, facial recognition, and retina scanning (Dastbaz & Wright). This type of technology is being used more abundantly in a lot of different industries, and there is not much protection for consumers against it at the moment. Some issues regarding this technology are that there are not many set parameters as far as what consent is required to obtain and store biometric data, how long it can be stored for, and what kind of security measures are required to protect people's data.

This research is significant to me because the use of biometric data has become an issue for many brands in the fashion industry. This is a concern for both consumers and businesses themselves. Companies need to know how to mitigate risk if they want to utilize these types of technologies, as they are growing in popularity. There are many things that need to be considered before using this technology since there are some state laws in place that regulate this technology. I hope to work in the legal environment of a fashion company one day, so this research is very important to my own future career. Almost all major fashion brands are using technology, such as virtual try-ons, and they need to understand the risks that come with collecting and storing that data without following the right procedures (Menaldo & Potesta).

Background Section

Concerns revolving around biometric technology are a relatively new issue. Biometric data itself has been utilized for over a hundred years. However, it was not always readily available for companies to use for that long. In the early 1960s, an automated fingerprint identification system was created (Babich). From there, it developed into automated technology to record signatures and kept developing until 1980 when the idea of facial recognition was first developed by Goldstein, Harmon, and Lesk, and then later came retina recognition (Babich). However, even with all these developments happening very quickly, the first biometric standards were not adopted until 2002 (Babich).

The idea of what qualifies as biometrics is quite broad. According to Aleksandra Babich's *Biometric Authentication* biometrics is anything that each person has, is unique from one person to another, is constant in people over time, is easy to measure, can be quickly

measured, and anything that is difficult to fraudulently produce (Babich). There are a lot of advantages to using this type of technology, which is why it is so widely used. It can sometimes increase security, it cannot be copied, it is convenient, accurate, and usually not very expensive (Babich). Biometric data is used for security purposes in almost all industries. From the medical industry to the FBI and even to small businesses, the use of biometric technology is rapidly spreading (Zarkowsky). It is used in airports to increase security, in prisons to keep track of inmates, and even in retailers to help survey potential shoplifters. More recently, it has even been used to track the spread of Covid-19 (Zarkowsky).

Although biometrics do have a lot of advantages, they also come with some drawbacks. For example, they can sometimes be duplicated, biometric databases can be hacked, companies can share and sell data to other organizations against people's consent, people can be tracked without their knowledge, and even though biometrics are highly accurate, there are still incidents where technology can be wrong (Zarkowsky). Because of these drawbacks, legislation is required to help protect consumers. However, as of right now, not many states have any proposed legislation, Pennsylvania included (*Biometric data privacy laws and lawsuits*).

Primary Legislation

Many states do not have any proposed legislation regarding biometric technology. Some states have introduced laws surrounding biometrics including California, Kentucky, Maine, Maryland, Massachusetts, Missouri, and New York. However, the only states that have enacted these laws are Illinois, Texas, and Washington. Of these, Illinois is also the only state that allows individuals to have a private right to action (DiRago et al.).

The most well-known legislature regarding this issue is the Illinois Biometric Information Act of 2008, commonly known as BIPA. This law gives people more control over their own data by setting strict guidelines of what companies must do and what consent they must obtain before collecting any data. Companies must inform people in writing what data is being collected. For example, if someone is going to use touch ID to sign into an app, they must be notified if their fingerprint is going to be stored anywhere. If the data is being stored, they must also be informed of how long it is going to be stored and the purpose of storing it. Finally, the person must give their written consent before the data is stored and used (DiRago et al.). This law includes protection over fingerprints, retina scans, voice recordings, hand scans, facial scans, DNA, and any other information that is biologically unique to a person. It also makes it illegal for any

company to sell biometric data once it is obtained (DiRago et al.). BIPA is currently the most protective law against the unwarranted use and storage of biometric data because it is the only law that allows individuals to take a company to court if they violate the standards of this law (DiRago et al.).

Other states also have laws based on BIPA. Texas, for example, has the Texas Biometric Privacy Act that also requires businesses to inform individuals and obtain consent before collecting any personal data and protects against data being sold (2020). Unlike BIPA, companies that violate this law are subject to receiving a civil penalty of no more than $25,000 (2020). Washington was the third state to enact a biometric privacy law. Unlike BIPA, Washington's law does not require written notification about why the data is being collected and why it is being stored. Contrary, the need for consent is dependent on the context of the situation. It also differs from Texas' and Illinois' laws because it has a "security exemption" that exempts individuals from the regulations if they are collecting and storing the data for security purposes. Other than a few differences, it closely resembles BIPA (Andrews Kurth, 2018). A few other states have proposed bills regarding this matter, but these are the only states with legislation at this time.

Regulatory Agency and Regulation

Currently there are no federal laws that regulate the use and storage of biometric data; however the Federal Trade Commission (FTC) does intend to focus on this area. The main goal of the FTC is to protect consumers in America (*Federal Trade Commission* 2022). The FTC has done what they can to help protect consumers against their data being used in a way they did not consent to. They have recognized the risks when collecting this data and have provided information for companies to help them properly collect this data. They make sure that companies are receiving consent before collecting any data, making sure that they are not selling the data, and making sure that companies take the proper steps to protect the data once it is collected (2021). They also urge consumers to report any companies that are not following these guidelines so that they could enforce any laws that could possibly apply depending on the state (2021).

There are also state and local agencies that can protect consumers. Each state has its own Consumer Protection Agencies that can provide services to protect consumers in the area. In Pennsylvania, there is not a state law regulating biometric data, but the Consumer Protection

Office “conduct[s] investigations and prosecute[s] offenders of consumer laws” (*State and local consumer agencies in Pennsylvania: Usagov*). However, since Pennsylvania and a lot of other states do not have specific laws regarding this matter, they may not handle complaints about biometric technology.

Case Law

There have been some recent cases regarding unfair use of biometric technology. This October, a federal district court in Illinois heard their first case regarding a business violating the Biometric Information Privacy Act in the case *Rogers v. BNSF Railway Co.* In this case, BNSF was allegedly collecting fingerprints from truck drivers without receiving proper consent. BNSF would have truck drivers scan their fingerprints when they arrived at their facility in order to confirm their identity when they came to pick up or drop off loads. Richard Rogers sued on behalf of all the truck drivers who were affected (Hirschorn). The jury ended up concluding that BNSF violated BIPA 46,500 times and that they were doing so intentionally. Under BIPA, companies can be fined up to $5,000 per violation if they recklessly or intentionally violate the law. They ended up suffering $228 million dollars in damages, however they are intending to appeal (Noonan).

The outcome of this case could have an impact on other companies as well. This case opened a lot of company’s eyes to how strong BIPA’s power is over companies when it comes to using biometric technology. There is expected to be a litigation spike following the outcome of this case. In this case, the state justices ruled that a plaintiff does not have to prove any actual injury occurred in order to sue, they just need to be able to prove the violation. Because of this, it is predicted that more claims are going to be filed in the future (Witley et al., 2022). Also, companies are being encouraged to review their practices when using biometric technology in order to prevent future violations. Some companies that use this kind of technology are violating BIPA without even realizing it. This case helped companies realize the impact and importance of BIPA.

Another case of a company disregarding BIPA was *ACLU v. Clearview. ai*. Clearview uses facial recognition technology to attempt to reduce crime, fraud, and make communities safer (*Overview*). A lawsuit was filed in January of 2020 in an Illinois state court after it was revealed that Clearview was storing people’s biometric data without their consent and then selling the data to private companies and law enforcement agencies. Using the database that

Clearview put together, people can be identified with surprising accuracy and can be surveilled without even knowing it. A focus of this case was the impact that this technology has on people such as domestic violence survivors, undocumented immigrants, and people of any other vulnerable communities. With this information being collected without consent and sold, a lot of people were put at risk (*ACLU v. Clearview Ai*). This was the first case to focus on that aspect of Illinois' privacy laws. Clearview was brought to court because people felt that the data that clearview attained without consent should be deleted since they did not comply with BIPA. Clearview argued that it should be shielded from regulation of BIPA due to their First Amendment rights, but this was denied by the court (2022).

Both cases showed how important it is for states to regulate how biometric technology is being used. In both cases, people were able to protect their personal information from companies, but only for the people who were governed by the laws. For example, in any case where a company violates BIPA, affected individuals are usually entitled to compensation, but only in Illinois. For example, when Snapchat was sued for violating BIPA by using facial recognition without consent, the only people who were entitled to compensation were people who lived in Illinois, even though data was being collected from all over the world (ABC7 Chicago Digital Team, 2022). Cases like these show the need for federal regulation of biometric technology. In a lot of states, people do not have any defense against companies if they are collecting biometric data without receiving consent first.

Proposed Legislation

A lot of states have recently proposed legislation regarding this issue. California recently proposed a Senate bill that mimics BIPA. It provides the same protections as BIPA does, it just fines companies between $100 and $1,000 as opposed to BIPA that fines companies between $1,000 and $5,000 (Wieckowski et al.). Kentucky also passed House Bill 626 that also models BIPA, but it does not give consumers a right to sue companies (Commission). Other states including Maryland, Massachusetts, Maine, Missouri, and New York have also proposed legislation that is very similar to BIPA (DiRago et al.). As of right now, no federal legislation has been proposed in relation to the use and storage of biometric technology.

Discussion or Findings

As biotechnology grows in popularity, more and more states are beginning to propose legislation. Biotechnology is used in a variety of fields for a variety of different purposes. As

companies are utilizing this technology more, they do not always know what kind of protections they owe to consumers. Because of this, more states are likely to propose legislation in the future. This is also a big issue for anyone who owns and operates a business. Facial recognition or fingerprint scanning is used on almost all apps to sign in and a lot of companies use biometric technology to track employees or people entering their place of business, but they have to make sure they are following the standards put in place in their state.

Laws regarding biometric technology have not been around for very long. The law that has the strongest protection for consumers when it comes to biometric technology was passed in 2008. Before that, there was very little protecting consumers' information. However, since 2008, biometric technology has grown in popularity and is used almost everywhere, but legislation has not kept up. There are some states that still have no legislation in this area. Biometric features are unique to each individual and cannot be replaced if that information is stolen. As technology increases, so should the laws that protect consumers.

There are not too many cases that have arisen recently that regard the issue of the protection of biometric data. Most companies who are sued for unlawfully using biometric data that they collect usually just end up settling before it could be brought before the court, but as states pass more legislation, it is expected that there will be more companies being held accountable for using biometric data without consent.

References

ABC7 Chicago Digital Team. (2022, August 24). *Snapchat agrees to $35m settlement in Illinois Privacy Class Action Suit*. ABC7 Chicago. Retrieved November 28, 2022, from https://abc7chicago.com/snapchat-lawsuit-class-action-settlement-illinois/12158193/

ACLU v. Clearview Ai. American Civil Liberties Union. (n.d.). Retrieved November 28, 2022, from https://www.aclu.org/cases/aclu-v-clearview-ai

Andrews Kurth, H. (2018, April 5). *Washington becomes Third State to enact biometric privacy law*. Privacy & Information Security Law Blog. Retrieved November 28, 2022, from https://www.huntonprivacyblog.com/2017/06/01/washington-becomes-third-state-enact-biometric-privacy-law/

Babich, A. (n.d.). *Biometric authentication. types of biometric identifiers - theseus*. Retrieved November 29, 2022, from https://www.theseus.fi/bitstream/handle/10024/44684/Babich_Aleksandra.pdf?sequence

Biometric data privacy laws and lawsuits. Bloomberg Law. (n.d.). Retrieved November 28, 2022, from https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/

Commission, K. L. R. (n.d.). *Kentucky General Assembly*. 22RS HB 626. Retrieved November 28, 2022, from https://apps.legislature.ky.gov/record/22rs/hb626.html

Dastbaz, M., & Wright, S. (n.d.). *Biometric technology*. Biometric Technology - an overview | ScienceDirect Topics. Retrieved November 28, 2022, from https://www.sciencedirect.com/topics/computer-science/biometric-technology

DiRago, M. S., Phan, K., Raether, R. I., & Lin, R. W. (n.d.). *A fresh "face" of privacy: 2022 biometric laws*. Troutman Pepper - A Fresh "Face" of Privacy: 2022 Biometric

Laws. Retrieved November 28, 2022, from https://www.troutman.com/insights/a-fresh-face-of-privacy-2022-biometric-laws.html

Hirschorn, D. (n.d.). *Rogers v. BNSF verdict signals companies about the cost of violating Illinois' biometric law*. Lockton. Retrieved November 28, 2022, from https://global.lockton.com/news-insights/rogers-v-bnsf-verdict-signals-companies-about-the-cost-of-violating-illinois

Illinois Court rejects Clearview's attempt to halt lawsuit against privacy-destroying surveillance. American Civil Liberties Union. (2022, May 11). Retrieved November 28, 2022, from https://www.aclu.org/press-releases/illinois-court-rejects-clearviews-attempt-halt-lawsuit-against-privacy-destroying

Menaldo, N., & Potesta, J. (n.d.). *Getting the right fit: Biometric privacy and the apparel industry*. Perkins Coie. Retrieved November 28, 2022, from https://www.perkinscoie.com/en/news-insights/getting-the-right-fit-biometric-privacy-and-the-apparel-industry.html

Noonan, A. (n.d.). *First biometric privacy jury trial results in massive $228 million dollar verdict*. JD Supra. Retrieved November 28, 2022, from https://www.jdsupra.com/legalnews/first-biometric-privacy-jury-trial-7528243/

Overview. Clearview AI. (n.d.). Retrieved November 28, 2022, from https://www.clearview.ai/overview

Richard Rogers, individually an on behalf of similarly situated individuals v. BNSF Railway Company (United States District Court, N.D. Illinois, Eastern Division June 21, 2022).

Staff, the P. N. O., & Staff, D. P. I. P. and C. T. O. (2021, December 22). *News and events*. Federal Trade Commission. Retrieved November 28, 2022, from https://www.ftc.gov/news-events

Staff, the P. N. O., & Staff, D. P. I. P. and C. T. O. (2022, February 11). Federal Trade Commission. Retrieved November 28, 2022, from https://www.ftc.gov/

State and local consumer agencies in Pennsylvania: Usagov. State and Local Consumer Agencies in Pennsylvania | USAGov. (n.d.). Retrieved November 28, 2022, from https://www.usa.gov/state-consumer/pennsylvania#es-1-off-hop

Texas biometric privacy law: Key requirements for businesses. Hyperproof. (2020, July 2). Retrieved November 28, 2022, from https://hyperproof.io/texas-biometric-privacy-law/

Wieckowski, S., Newman, S., & Rivas, L. (n.d.). *Bill text*. Bill Text - SB-1189 Biometric information. Retrieved November 28, 2022, from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB1189

Witley, S., Brown, C., & Smith, P. (2022, October 14). *Biometric privacy perils grow after BNSF loses landmark verdict*. Bloomberg Law. Retrieved November 28, 2022, from https://news.bloomberglaw.com/privacy-and-data-security/biometric-privacy-perils-grow-after-bnsf-loses-landmark-verdict

Zarkowsky, A. (n.d.). *Biometrics: An evolving industry with unique risks - the Hartford*. Retrieved November 29, 2022, from https://www.thehartford.com/insights/technology/biometrics