IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Global Implications of Biometrics and Mass Surveillance

Krish Shah

Student, The Bishop's Co-Ed School, Undri, Pune, India

Abstract: In this ever digitizing world, maintaining integrity of data is of utmost importance to ensure that this digital world remains safe for the consumption of the masses. However, as technology advances, the ease of protecting this data decreases as stronger passwords and encryption keys need to be used. In order to keep up with this technological advancement, Biometrics are employed in order to secure these systems and technologies however in the current state of Surveillance, Biometrics is being employed in combination with Mass Surveillance technology. This paper will be talking about the implications of combining the usage of Biometrics and Mass Surveillance technology on the world as a whole.

Index Terms **- Biometrics, Mass Surveillance, Privacy, Artificial Intelligence**

I. INTRODUCTION

As the world digitize, the state of privacy decreases and the state of surveillance increases. In order to counteract this loss in privacy, stronger approaches are being made to secure the data of individuals such as hash cryptography, end-to-end encryption, and more recently – biometrics. The usage of biometrics is extremely advantageous in securing individuals and their data as they are unique but is a cause of concern due to the current state of mass surveillance in the world which is now using biometrics to track people, their intentions and "guess" the next move wanting to be made.

II. BIOMETRICS

Biometrics is defined as "the measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity" [13]. A biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition [20].

Every feature of the human body from the rhythm of the heart to the ridges of the finger can be used for Biometric analysis [although, some features are preferred over others due to their increased sense of uniqueness relative to their method of identification]. Each biometric has an exclusive modus operandi to analyze the unique biological arrangements each (and every) individual has, making them difficult to mimic.

2.1 Biometric Authentication and its Applications

Biometric Authentication compares data for the person's characteristics to that person's biometric "template" to determine resemblance. In order to achieve this, a reference model is first stored and then the data is compared to the stored biometric profile to authenticate. This is the same method used in the process of biometric "Identification" as well [4]. According to Saini (2011) [16], the process by which Biometric Authentication takes place can be summed up in the following three steps:-

1. Enrolment - When you're using a biometric system from scratch, it captures basic information concerning you, such as your name or an identification number. It then records or takes a picture of your unique attribute.
2. Storage - Unlike what you would see in movies, most systems do not save the entire image or video. Instead, they study your characteristics and convert them into code language graphs. Systems can, also, save this information on a portable smart card.
3. Comparison - The program compares your offered characteristics to the recorded biometric information whenever you utilize it. Then, it either accepts or rejects your claim to be who you say you are.

Biger-Levin (2022) [3] states that existent Biometrics can broadly be classified into the following types:

1. Physiological Measurements - These biometrics are based on bodily attributes based on both: the structure and the biological components (of the body). They are further divided into:
    a. Morphological identifiers - Identifiers relating physical components of the body such as fingerprints, Iris, Retina, Shape of hand and fingers, Vein pattern, etc.
    b. Biological Identifiers - Identifiers relating biological components of the body such as DNA, Blood, Saliva, Urine Sample, etc.
2. Behavioral measurements - These are biometric patterns based on behavioral sequences of individuals. These are the primary cause of concern discussed in this paper. Most commonly limited to speech, signature and keystroke analysis: Behavioral Biometrics speak volumes. Behavioral Biometrics is used to differentiate between a "good" user and a

cybercriminal. They are, also, the leading technique (as a second factor) to authenticate identity at higher-posts in major corporations as well as financial institutions.

These biometric indicators are widely used across the world including usage in securing mobile phones, biometric attendance systems in office spaces and schools, forensic profiling in both: civil and criminal cases, to guard secure locations and in cases of mass surveillance – the core point of discussion of this paper.

2.2 Biometric of Intent

Biometric of Intent aims to scan the invisible mental processes of individuals' emotions, intents and beliefs through the usage of external behavioral indicators such as facial expressions. Based on the hypothesis that individuals "who intent to do harm will be concealing this fact, thereby expressing deceitful behaviors – and that deceitful behavior cues are founded in stress, which in turn are displayed in emotions", Biometric of Intent is the leading field of research and development in intelligence and counter-intelligence.

A recent example of using Biometric of Intent to enhance security measures within the country is 'SPOT.' Already operational in the United States, an example of this is the deployment of "Behavioral Detection Officers" by the Transport Security Administration (TSA)in the context of the SPOT (Screening Passengers by Observational Techniques) [6].

Shachtman & Beckhusen (2013) states how the Pentagon's blue-sky researchers at DARPA (Defense Advanced Research Projects Agency, USA) started work on the "Unique Signature Detection Program" in the early and mid-2000s to explore the use of odor as a biometric. Their work was succeeded by the Department of Homeland Security of the United States of America fielding solicitation for research in ways Human scent can be used to detect whether someone is engaging in deception to be deployed at sites of entry into the country such as Airports, border patrols and ports [17].

Shachtman & Beckhusen (2013) also shows how California security firm, Irvine Sensors Corporation received a similar contract from the United States Army to develop software to recognize "abnormal perspiration and changes in body temperature" to understand if a person has malicious intent at border-patrol stations [17]. University of Albany's Jan Halamek's research has already outlined how sweat and its Amino Acid contents can be used for Biometric Authentication to increase cyber security [1]. Furthermore, sweat is being used to secure fingerprint biometric as well. Stephanie Schuckers, associate professor of electrical and computer engineering at Clarkson, developed an algorithm that detects and accounts for perspiration (sweat) when reading a fingerprint image to further ensure the biometric identity of an individual [10].

Even walking patterns are used as unique biometric markers. Once thought to be difficult to survey due to the presence of obstructive components such as briefcases and bags: Researchers at Carnegie Mellon University have used accelerometer sensors in the cell phone to capture a person's walking pattern which serves as a unique biometric. In collaboration with the CyLab Biometrics Centre, researchers were able to get a 99.4% success rate in identifying subjects based on walking patterns [17].

Even one's heartbeat is a uniquely identifiable biometric, that can't be hidden in any form. Various systems such as LifeReader, and DARPA's Radar Scope already exist. Further research is on-going under the name of "Biometrics at a distance" to build sensors that can remotely identify humans and tell them apart in a crowd. All this goes to show how biometrics have diversified from just the simplistic fingerprint and facial recognition to complex and sophisticated ways to identify individuals and intentions [15].

III. MASS SURVEILLANCE

The United States of America's Patriot Act of 2001, drafted and enacted mere weeks after the 9/11 tragedy gave various agencies of the United States of America the "right" to conduct mass surveillance on its citizens in the name of preventing terrorism [2]. Agencies track laptops, cell phones, online activity and phone calls among others. Major internet companies such as Yahoo, Microsoft and Google have all been linked with sharing private data with governmental agencies such as the NSA [11]. These companies however control a bigger portion of the internet than one can imagine, with Microsoft and Google acting as two of the biggest cloud & hosting service providers in the world! This means that these companies not only have access to private data of users on their platform, but also the private data of users on other platforms using services of these companies.

Furthermore, the United States isn't the only country conducting mass surveillance. The Republic of Ireland is also known for conducting mass surveillance on its citizens despite various directives from the European Union asking them not to do so [12]. The Xinjiang region of China is another such example where mass surveillance actively takes place [21]. The Australian Strategic Policy Institute shows how one app used by the police officers of Xinjiang in China can provide all the information on a particular individual with the click of a few buttons. The Chinese Communist Party (CCP) takes mass surveillance very seriously with cameras not being the only element of control. They use an array of data including banking information, mobile payment apps, WeChat, Social Credit Score, biometric data, Great Firewall, third-generation national ID Card, mobile phones, televisions among other surveillance hardware and software showing the extent of control possessed by China over its people [19].

To ease the process of mass surveillance between countries, the formation of alliances to share such information has taken place such as: Five Eyes, Nine Eyes and Fourteen Eyes including prominent countries such as The United States of America, The United Kingdom, New Zealand, Canada, Australia, France, The Netherlands, Denmark, Norway, Germany, Belgium, Italy, Sweden, Spain and Japan [18].

The above examples show the extent of control and mass surveillance exhibited by the various governments across the world, and how much information is controlled by the governments across the globe.

IV. COMBINATION OF BIOMETRICS AND MASS SURVEILLANCE

As mentioned in the previous section, various companies use Google, Microsoft and big data companies' servers to host their services and store their data. This data is being shared with the government and other private agencies opening the public to a slew of problems.

When systems or technologies are used to process anyone's biometric data in public spaces such as parks, squares or online public spaces (or in publicly-accessible spaces such as arenas and train stations) can be considered biometric mass surveillance." Biometric mass surveillance works by analyzing the data of each and every person entering a certain place thereby giving the perception that you are always being watched even if the data is later discarded [9].

An example of such technology being used is in the Italian city of Como. Using Huwaei's technology, the city was using Biometric Mass Surveillance to check whether packages were being left unattended in public areas, whether people were entering forbidden areas and to, also, facially scan each and every person to enter the area. This practice was, however, later deemed to be illegal by the Italian Government [5].

Countries in the European Union have continued using such techniques with police forces using Biometric Mass Surveillance technology against protestors such as the usage in Slovenia in 2020 where facial recognition was combined with scouring of social media and other online platforms to survey and target individuals attending legitimate protests [9].

Similar to the Como case, Belgian police also unlawfully deployed facial recognition systems at their airports which checked for biometric facial signatures on individuals and compared them to the self-composed "black list" generated by the Belgian government [14].

The "Living Labs" experiment in the Netherlands is transforming normal communities into biometric surveillance nerve centers. Biometric surveillance models such as GAIT and facial recognition are combined with social media surveillance in order to "infer if young people are hanging out on a street and predicting their future life outcomes on this basis" [8].

The access of biometric data to major corporations and governments allows for more accurate identification of individuals during mass surveillance. Facial recognition is commonly integrated with mass surveillance cameras as it is easy to identify individuals using such technology using high resolution cameras installed at every nook and corner of this world [7]. Trained Artificial Intelligence Models are able to distinguish between the various moods of an individual. This is further being integrated with mass surveillance systems in order to better predict the moods of individuals. Pictures taken digitally and/or uploaded to digital mediums serve as raw data for these models to train off of. The above examples simply show how far biometric surveillance has already gone.

V. IMPACT

In a world where all our movements are tracked, all our words are monitored using some technological entity, combining biometrics and mass surveillance only adds up to complete loss of all our privacy. The inherent right of an individual is being stripped away in the name of security and research.

As mentioned in previous sections, biometric technologies are advancing every single second (Alongside the technology used to conduct mass surveillance). Cameras, now, produce sharper images and are able to track movements with greater ease, computer systems are now able to take larger loads and audio recording systems are able to distinguish between sources of different sounds in a single surrounding!

We are moving towards a world where every movement of an individual is tracked, every word spoken is monitored and every action made is analyzed. Under observation, the behavior of individuals changes. People stop being themselves and start acting in a way they feel is more pleasing to the observer. The "Instagram effect" takes place where reality starts getting masked by filters for acceptance and "likes". Underlined under the Observer effect, the Behavior of a person greatly changes when the person is under observation by others. The system of Biometric surveillance will be taking this observer effect to an entirely new and unprecedented level.

This system of surveillance can be a boon. If Biometric of Intent can be properly applied and combined with mass surveillance, it would help greatly in preventing events of mass tragedy as these systems are well equipped in determining the intentions of individuals. This would however be coming at a great cost: PRIVACY!

All our private and sensitive information is present with the government. Nothing remains personal anymore as every tap of the screen, every movement of the finger is being closely monitored for any ulterior motive. It takes away from the general public their autonomy, their right to do things their way due to the constant fear of being monitored.

However, the greatest and the most negative impact would be the breaches caused in data being protected using such biometric locks as these biometric identifiers are no longer privy to just the individual but are stored and used in tracking, artificial intelligence and various other services.

Technical giants and governments are no strangers to hacks, and breaches. Having so much personal data being stored in such servers puts all involved individuals at a massive risk of losing - not just private information- but parts or even the entirety of their identity.

VI. CONCLUSION

Mass surveillance combined with biometrics would significantly increase the security of a place but will be at the cost of the privacy of the users. This increase in security will be at the cost of the autonomy and freedoms that the individuals enjoy today. So the choice the people have to make is whether such security is worth the trade!

REFERENCES

[1]. Agudelo, J., Privman, V., & Halámek, J. (2017). Promises and challenges in continuous tracking utilizing amino acids in skin secretions for active multi-factor biometric authentication for Cybersecurity. ChemPhysChem, 18(13), 1714–1720. https://doi.org/10.1002/cphc.201700044

[2]. Beens, R. E. G. (2020, September 25). Council post: The State of Mass Surveillance. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=1e0ed13bb62d
[3]. Biger-Levin, A. (2022, March 8). What is behavioral biometrics?. What Is Behavioral Biometrics? https://www.biocatch.com/blog/what-is-behavioral-biometrics
[4]. Biometrics: Definition, use cases, latest news. Thales Group. (n.d.). https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics
[5]. Carrer , L., Coluccini , R., & Di Salvo, P. (2020, September 17). How facial recognition is spreading in Italy: The case of como. Privacy International. https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como
[6]. Chamieh, J., Al Hamar, J., Al-Mohannadi, H., Al Hamar, M., Al-Mutlaq, A., & Musa, A. (2018). Biometric of intent: A new approach identifying potential threat in highly secured facilities. 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). https://doi.org/10.1109/w-ficloud.2018.00037
[7]. Clark, M. (2019, April 9). Facial recognition for biometric mass surveillance. Bayometric. https://www.bayometric.com/facial-recognition-biometric-mass-surveillance/
[8]. Hersey, F. (2021, July 9). Europe heading for "open-ended biometric mass surveillance": Report: Biometric update. Biometric Update |. https://www.biometricupdate.com/202107/europe-heading-for-open-ended-biometric-mass-surveillance-report
[9]. Jakubowska, E., & Naranjo, D. (2020, May 13). Biometric mass surveillance: What is it, and why does it need to be banned?. Biometric Mass Surveillance: What is it, and why does it need to be banned? https://edri.org/wp-content/uploads/2020/12/Biometric-mass-surveillance-explainer.pdf
[10]. Kanellos, M. (2005, December 21). New biometrics software looks for sweat. ZDNET. https://www.zdnet.com/article/new-biometrics-software-looks-for-sweat/
[11]. MacAskill , E., & Rushe , D. (2013, November 1). Snowden document reveals key role of companies in NSA Data collection. The Guardian. https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms
[12]. Manancourt, V. (2022, July 31). Europe's state of mass surveillance. POLITICO. https://www.politico.eu/article/data-retention-europe-mass-surveillance/
[13]. Merriam-Webster. (n.d.). Biometrics. In Merriam-Webster.com dictionary. Retrieved May 9, 2023, from https://www.merriam-webster.com/dictionary/biometrics
[14]. Peeters, B. (2020, June 17). Facial recognition at Brussels Airport: Face down in the mud. CITIP blog. https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/
[15]. Rawnsley, A. (2011, November 18). Follow your heart: DARPA's quest to find you by your heartbeat. Wired. https://www.wired.com/2011/11/follow-your-heart-darpas-quest-to-find-you-by-your-heartbeat/
[16]. Saini, H. (2021, December 5). What is biometrics and how does it work?. Analytics Steps. https://www.analyticssteps.com/blogs/what-biometrics-and-how-does-it-work
[17]. Shachtman, N., & Beckhusen, R. (2013, January 25). 11 body parts researchers will use to track you. Brookings. https://www.brookings.edu/opinions/11-body-parts-researchers-will-use-to-track-you/
[18]. Taylor, S. (2023, January 3). Five eyes, nine eyes, 14 eyes (what to avoid in 2023). RestorePrivacy. https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/
[19]. Thayer , B. A., & Han, L. (2019, May 29). China's weapon of mass surveillance is a human rights abuse. The Hill. https://thehill.com/opinion/technology/445726-chinas-weapon-of-mass-surveillance-is-a-human-rights-abuse/
[20]. The National Biometrics Challenge (2011). What is a Biometric. Department of Homeland Security. https://www.dhs.gov/biometrics
[21]. Wang, M. (2019, May 1). China: How mass surveillance works in Xinjiang. Human Rights Watch. https://www.hrw.org/news/2019/05/01/china-how-mass-surveillance-works-xinjiang