



PUBLIC FORUM DEBATE

APRIL 2023 TOPIC ANALYSIS



TABLE OF CONTENTS

Definitions:	3
Background:	4
Aff Arguments:	5
Privacy	5
Harms Minorities.....	5
Neg Arguments:	7
Benefits to Business	7
Benefits to Individuals	7

Disclaimer: *This analysis serves as an introduction to the topic and offers guidance for areas students can explore further with independent research. It does not attempt to provide limitations on debater's interpretations of the topic.*

Resolved: The United States Federal Government should ban the collection of personal data through biometric recognition technology.

Definitions:

Ban: [Merriam-Webster](#) defines “ban” as “to prohibit, especially by legal means.” It’s worth noting that this resolution then clearly advocates for a full stop of this data collection.

Collection: Again from [Merriam-Webster](#), “collection” is defined as “the action of collecting.” [Collecting](#), then, is defined as “to gather or exact from a number of persons or sources.”

Personal data: “Personal data” as a phrase is not officially defined by the US government. According to the [European Commission](#), personal data refers to any information that relates to an identified or identifiable living individual. The closest definition the [US government](#) has is its definition of personal identifiable information, which it defines as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Biometric recognition technology: Biometrics are defined by the [US Department of Homeland Security](#) as unique physical characteristics, such as fingerprints, that can be used for automated recognition. Therefore, biometric recognition technology refers to the types of technology that examine biometrics and identify an individual. [The Biometrics Institute](#) details the different types of biometric recognition as well.

Background:

April is an important month for the competitive season, as the Tournament of Champions takes place in late April and, for many, represents a season full of hard work and a chance to receive great feedback before the National Tournament begins in June. This is where the regular season begins winding down and many teams start considering the transition from novice to JV or JV to varsity. This topic presents a great way to delve into something new and practice fine-tuning your debate skills.

At first glance, this topic may seem complex, particularly due to the vocabulary used. However, it examines an area that we are all familiar with on different levels, whether it be through the facial recognition technology on our phones or the use of fingerprinting in criminal cases. There is a great deal of biometric measurements we can refer to in this topic, from fingerprints to facial recognition to behavioral biometrics, such as your pattern of walking.¹ Biometrics as a way of measuring individuals has been common for a while, but particularly gained traction after 9/11.² In recent years, however, the issue of privacy has become a key concern with biometric recognition technologies.

Illinois became the first state to enact a biometric data privacy law in 2008.³ This law requires that any organization that uses and stores biometric identifiers complies with certain requirements, and it provides a private right of action for recovering statutory damages when they fail to comply. Since then, a handful of other states have enacted similar legislation with the aim of protecting their residents. There have been quite a few court cases dealing with this issue, and some recent bills have been proposed to prohibit corporations from collecting biometric data without consumers and employees' consent.⁴

Both affirmative and negative teams will have interesting arguments to explore on this subject. The aff can absolutely discuss privacy and the problems that come up with biometrics, which often result in wrongful application of justice. The neg, however, may want to point out the multitude of benefits that biometrics can offer to businesses and individuals, as well as expediting governmental processes. This should be a really interesting topic for teams to explore, and it will be a great way to close out the regular season!

¹ Tom, Navrup. "What Are Biometrics? The Pros/Cons of Biometric Security." Auth0. 24 May 2021. <https://auth0.com/blog/what-are-biometrics-the-proscons-of-biometric-security/>

² Gibson, Matt. "Biometric Technology Pros and Cons Explained." M2SYS Blog On Biometric Technology. 13 May 2022. <https://www.m2sys.com/blog/biometric-technology/biometric-technology-pros-and-cons/>

³ "Biometric Data Privacy Laws and Lawsuits." Bloomberg Law. 25 Jan. 2023. <https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/>

⁴ Reuters Staff. "Two U.S. senators seek ban on collecting customer biometric data without consent." Reuters. 6 Aug. 2020. <https://www.reuters.com/article/us-usa-congress-facial-recognition-idUSKCN2520CN>

Aff Arguments:

Privacy

Our faces, fingerprints, and other biometric information are things that cannot be easily adjusted or replaced in the event of theft or a security breach in the same way an ID or password could be.⁵ One key area worth considering is DNA testing, particularly as it becomes more prominent; more than 26 million people have taken at-home DNA tests.⁶ Unfortunately, as harmless as these tests may seem, they have a good amount of problems. First, you always run the risk of data breaches. For example, in 2018, popular DNA testing website MyHeritage saw the account details of over 92 million accounts made public.⁷ Additionally, the results of DNA tests are often used in ways the tester may not have known about. DNA test results may be used by health insurance companies to increase the cost of premiums or deny coverage to users.⁸ More severely, in recent years, we have seen DNA test results weaponized against users and their relatives, who often are not given the opportunity to consent to their genetic data being collected and shared. In 2019, Family Tree DNA, one of the largest at-home DNA testing companies in the US, worked with the FBI and allowed agents to search its database.⁹ This was particularly problematic because people whose data was already in the database were unable to further consent to this practice.

Harms Minorities

Surveillance strategies in the US have a long history of being applied disproportionately against minority populations, and biometric recognition technologies are no better. In 2015, the Baltimore Police Department used aerial surveillance, location tracking, and facial recognition to identify people who protested the death of Freddie Gray.¹⁰ Asian and African-American

⁵ Sheard, Nathan and Schwartz, Adam. "The Movement to Ban Government Use of Face Recognition." Electronic Frontier Foundation. 5 May 2022. <https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition>

⁶ Molla, Rani. "Genetic testing is an inexact science with real consequences." Vox. 13 Dec. 2019.

<https://www.vox.com/recode/2019/12/13/20978024/genetic-testing-dna-consequences-23andme-ancestry>

⁷ Kelly, Makenna. "MyHeritage breach leaks millions of account details." The Verge. 5 Jun. 2018.

<https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach>

⁸ Cuddigan, Timothy J. "The Good, the Bad, and the Ugly of DNA Testing." Cuddigan Law. Last accessed 14 Mar 2023. <https://www.cuddiganlaw.com/blog/the-good-the-bad-and-the-ugly-of-dna-testing.cfm>

⁹ Hernandez, Salvador. "One Of The Biggest At-Home DNA Testing Companies Is Working With The FBI." BuzzFeed News. 1 Feb. 2019. <https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy>

¹⁰ Turner Lee, Nicol and Chin, Caitlin. "Police surveillance and facial recognition: Why data privacy is imperative for communities of color." Brookings. 7 Apr. 2022. <https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>

people are up to 100 times more likely to be misidentified by facial-recognition systems than white men.¹¹ Native Americans had the highest false-positive rate of all ethnicities, and the faces of African-American women were falsely identified more often in the searches used by police investigators in identifying a suspect. In fact, the use of facial recognition software has led to wrongful arrests of Black men.¹² As the lawmakers who endorsed the most recent bill aiming to ban the use of facial recognition technology argue, these kinds of technologies perpetuate injustice and stand in the way of any real change.¹³

¹¹ Harwell, Drew. "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use." Washington Post. 19 Dec. 2019.

<https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

¹² Tsukayama, Haley. "Trends in biometric information regulation in the USA." Ada Lovelace Institute. 5 Jul. 2022.
<https://www.adalovelaceinstitute.org/blog/biometrics-regulation-usa/>

¹³ Konkel, Frank. "Lawmakers Intro Bill to Ban Government Use of Facial Recognition." NextGov. 7 Mar. 2023.
<https://www.nextgov.com/technology-news/2023/03/lawmakers-intro-bill-ban-government-use-facial-recognition/383691/>

Neg Arguments:

Benefits to Business

Fingerprint biometrics can provide both physical access to company buildings and logical access to internal resources such as enterprise computers and systems. Unlike magnetic strip cards or passwords, individuals always carry their fingerprints with them, and they cannot be lost or forgotten.¹⁴ There's a reason you see biometric scanning in all the spy movies! Businesses also recognize that biometric technologies can and will increase productivity due to delays or backups.¹⁵ Biometrics are also popular with workers due to how quick the procedure is. Workers can scan their fingerprint, iris, or another part of their body to speed up the process of getting to work each morning.¹⁶

Benefits to Individuals

Technology is now able to shorten the amount of time it takes to accurately identify suspects through fingerprinting. Mobile fingerprinting devices enable officers in the field to obtain fingerprints of persons in the field and check them against State and Federal fingerprint databases in under a minute. Through the use of this device, officers can determine whether a person has provided a false identity, has a criminal history, or is wanted for a crime.¹⁷ Additionally, although fingerprinting has been criticized as inaccurate in the past, newer technologies are combating these inaccuracies and better positioning offers to obtain fast and accurate results.¹⁸ Importantly, this will help families and individuals obtain justice in a shorter amount of time. The layer of security provided is also critical; PINs and passwords are often quickly forgotten and thus need to be written down, which creates a further insecurity that cannot exist with biometrics.¹⁹

¹⁴ Thakkar, Danny. "Importance of Biometric Fingerprinting Technology." Bayometric. 12 Nov. 2016.

<https://www.bayometric.com/importance-of-biometric-fingerprinting-technology/>

¹⁵ Fire Monitoring Canada. "5 Security Benefits of Biometrics | Fire Monitoring Of Canada." Fire Monitoring Canada. 21 Jun. 2022. <https://www.fire-monitoring.com/blog/5-security-benefits-of-biometrics/>

¹⁶ Mitek "What Are Biometrics in the Digital World." Miteksystems.com. 10 Nov. 2022. <https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics>

¹⁷ Aware, Inc. "Biometrics Software Solutions." Aware. 24 Mar. 2022. <https://www.aware.com/blog-benefits-rapid-fingerprinting-law-enforcement/>

¹⁸ Police1. "New algorithm may make fingerprint analysis more reliable and efficient." Police1. 28 Nov. 2017. <https://www.police1.com/police-products/crime-scene-investigation/articles/new-algorithm-may-make-fingerprint-analysis-more-reliable-and-efficient-GVTbPvCLFUx29CuY/>

¹⁹ Jones, Billy. "Top ten mind blowing advantages of biometric technology." M2SYS Blog On Biometric Technology. 6 Dec. 2015. <https://www.m2sys.com/blog/guest-blog-posts/top-ten-mind-blowing-advantages-of-biometric-technology/>