Example Connecting Claims to Evidence Argument Displaying Illustrating, Authorizing, and Countering

Biometrics are all the rage. They are springing up everywhere whether we realize it or not (or want them or not). Are biometrics, though, worth the security risk they pose? Although biometrics offer levels of great convenience and security, biometric technology is not advanced enough yet to make it worth the security risk.

One problem with biometrics is that they often use publicly available information--our bodies. As a *Do Now* article written by the California Academy of Sciences, a museum and scientific institution, states, "Our bodies are on display all the time; body parts used for biometric identification, such as fingers and eyes, can be accessed easily in comparison to protected passwords and security badges." The ease of access to biometric data about us, without our consent, means that they can be stolen and spoofed easily. Once the theft occurs, it is permanent. We can't get a new thumb or eye. Woodrow Hartzog, a Samford University Law professor who is an internationally recognized expert in the area of media and privacy, makes this point: "if a biometric is compromised, you're done. You can't get another ear." Whereas a credit card or a password can be replaced, one of our body parts can't be replaced. The result is that we would be unable to use that part of our body as a biometric identifier ever again, potentially limiting our access to commerce or things that use biometrics.

Also, this biometric data is not totally secure. At some point, it could be hacked, like anything else in our digital world. As April Glaser, a non-profit technology activist and widely published journalist from Wired and Slate magazine, asserts, "Databases get hacked all the time, from the IRS to Target to hospitals and banks, and until some of the very real security concerns surrounding the use of biometric technologies are better ironed our, you wouldn't be wrong to worry about linking data about your body parts to online accounts." Until the time when they can be sure that this sort of breach will not be something as common as breaches seem to be today, giving over your biometric data for using some device is unwise. In this transition time when biometrics are new and less secure, hackers will be tempted to pursue this data even more. April Glaser in her Wired Magazine article makes clear, "Biometric data isn't immune to these attacks." Just as any digital data can be stolen, so could our biometric data. Stealing biometric data is the ultimate permanent identity theft with permanent negative consequences.

Those who support the use of biometrics argue for the convenience that this form of authentication and identification can provide. Dr. Salil Prabhaker, a computer science researcher and CEO of the digital company Delta Inc, states about biometics in cars: "Once a car is connected to a payment system, biometric technologies can execute cashless payments at gas stations, coffee shops, and other drive-through stores, as well as in-car payments for purchases made via ecommerce." Certainly, biometrics if done properly can make our lives easier. However, we currently are rushing into the use of this technology without understanding the security risks. As Hartzog later mentions in his article: "We're probably not ready to hand over the keys to the entire biometric kingdom when we're not sure how this is going to work." Right now this kingdom is not secure and is open to having our biometric data stolen. Until that day when we understand and can be sure that our biometric data is secure and can't be stolen, we should not be so eager to go for the convenience of biometrics because we exchange our privacy for this convenience.

While banks, credit card companies and car manufacturers are rushing to make biometric authentication the key that unlocks the internet of things, we would be wise not to opt into handing over our biometric data until this technology becomes more secure. Perhaps the day will come when this technology is immune to data theft, but that day is definitely not today.

Color Coded Example Connecting Claims to Evidence Argument Displaying Illustrating, Authorizing, and Countering and a Nuanced Claim

Biometrics are all the rage. They are springing up everywhere whether we realize it or not (or want them or not). Are biometrics, though, worth the security risk they pose? Although biometrics offer levels of great convenience and security, biometric technology is not advanced enough yet to make it worth the security risk.

One problem with biometrics is that they often use publicly available information--our bodies. As a *Do Now* article written by the California Academy of Sciences, a museum and scientific institution, states, "Our bodies are on display all the time; body parts used for biometric identification, such as fingers and eyes, can be accessed easily in comparison to protected passwords and security badges." The ease of access to biometric data about us, without our consent, means that they can be stolen and spoofed easily. Once the theft occurs, it is permanent. We can't get a new thumb or eye. Woodrow Hartzog, a Samford University Law professor who is an internationally recognized expert in the area of media and privacy, makes this point: "if a biometric is compromised, you're done. You can't get another ear." Whereas a credit card or a password can be replaced, one of our body parts can't be replaced. The result is that we would be unable to use that part of our body as a biometric identifier ever again, potentially limiting our access to commerce or things that use biometrics.

Also, this biometric data is not totally secure. At some point, it could be hacked, like anything else in our digital world. As April Glaser, a non-profit technology activist and widely published journalist from Wired and Slate magazine, asserts, "Databases get hacked all the time, from the IRS to Target to hospitals and banks, and until some of the very real security concerns surrounding the use of biometric technologies are better ironed our, you wouldn't be wrong to worry about linking data about your body parts to online accounts." Until the time when they can be sure that this sort of breach will not be something as common as breaches seem to be today, giving over your biometric data for using some device is unwise. In this transition time when biometrics are new and less secure, hackers will be tempted to pursue this data even more. April Glaser in her Wired Magazine article makes clear, "Biometric data isn't immune to these attacks." Just as any digital data can be stolen, so could our biometric data. Stealing biometric data is the ultimate permanent identity theft with permanent negative consequences.

Those who support the use of biometrics argue for the convenience that this form of authentication and identification can provide. Dr. Salil Prabhaker, a computer science researcher and CEO of the digital company Delta Inc, states about biometics in cars: "Once a car is connected to a payment system, biometric technologies can execute cashless payments at gas stations, coffee shops, and other drive-through stores, as well as in-car payments for purchases made via ecommerce." Certainly, biometrics if done properly can make our lives easier. However, we currently are rushing into the use of this technology without understanding the security risks. As Hartzog later mentions in his article: "We're probably not ready to hand over the keys to the entire biometric kingdom when we're not sure how this is going to work." Right now this kingdom is not secure and is open to having our biometric data stolen. Until that day when we understand and can be sure that our biometric data is secure and can't be stolen, we should not be so eager to go for the convenience of biometrics because we exchange our privacy for this convenience.

While banks, credit card companies and car manufacturers are rushing to make biometric authentication the key that unlocks the internet of things, we would be wise not to opt into handing over our biometric data until this technology becomes more secure. Perhaps the day will come when this technology is immune to data theft, but that day is definitely not today.