Biometrics and Consumer Electronics

Patrick M. Lyon

IT103 - 007

Tuesday February 11, 2014

Research Paper

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/the-mason-honor-code/. I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Introduction

The idea of biometrics has been around for some time. From science fiction movies to government applications; but not until recently have consumer electronic companies been putting these instruments into the consumers hand. But according to recent patents submitted from companies, and recent product releases, it suggests that they want to do more then just secure devices. From finger print scanners to heart beat sensors, it seems companies are working to not only secure your device but to give you information about yourself. But what steps are these companies taking to secure this information from people that might be trying to steal your information or your devices?

What is Biometrics?

Biometrics is defined by Merriam-Webster (2014) as, "the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity" (Merriam-Webster.com). Biometrics can be used for security reasons or for informational purposes. There are all different types of biometric scanners out there in fact if you have been to an airport in recent years, you have been through biometric scanners. At airports they use two different types of body scanners, Blackscatter X-ray scanners and Millimeter wave scanners. They both work in different ways but both come out with similar results. These devices are huge and require a lot more technology then what could fit in your pocket.

Fingerprint Scanner.

Every human being on Earth has a different fingerprint. Even identical twins have different fingerprints. So it makes complete sense to use them to secure technology. Fingerprint devices work in different ways. Apple Inc. is using a sensor it calls TouchID. It works by using

an image sensor to take a picture of your fingerprint and saves it. Then when you move your finger over the sensor to unlock your device, it pulls up that image and compares it to what it currently sees. Fingerprint scanners are not new, in fact they are not even new to smart phones. Even more so, fingerprint scanners, can be purchased and connected to your computer via USB.

Facial and Iris and Retina Scanning.

Facial recognition has been used in computers for quite some time. Almost any PC that has a camera, or if you choose to buy a stand alone third party camera, has the ability of doing facial recognition via third party software. It is similar to fingerprint scanning, as it takes and saves an image of your face and then when you log in to your computer it recalls that image and checks if it is a match. Though unlike the fingerprint scanner, it has a much higher rate of error, due to the variability in lighting situations in which the original and log in images were taken.

Iris scanning and retina scanning both work similarly to facial recognition and to fingerprint scanners. The iris scanner works by looking at the colored section of the eye, also known as the iris. John Trader (2012) says, "The **iris** (plural: ***irides*** or ***irises***) is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupils and thus the amount of light reaching the retina." (blog.m2sys.com). Just like fingerprints, both the retina and iris have unique features to each individual. According to John (2012), "The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye." (blog.m2sys.com). Both the iris scan and retina scan use infrared light and a camera to image the eye. One down side to the retina scan is that based on the condition of your health it can change.

Heart Beat Sensors and Pedometers.

Heart beat sensors is a technology, until recently, only used in the health care profession. As companies work to create wearable technology, they are also looking to give them more

functionality. Like many of the other sensors there are different ways of detecting and monitoring a heartbeat. According to Apple Insider (2010), Apple Inc. filed a patent in January of 2009 that, "would be able to track the electrical activity of a heart during a heartbeat." (appleinsider.com).

A pedometer is a device used for tracking how many steps you take. In fact, many devices already have the capability to be pedometers. Pedometers are not anything new. All it takes is an existing motion sensor such as a 3-way gyroscope or a 3-way accelerometer, which most smart phones have both. The only other thing needed is software and algorithms capable of understanding the movement.

Sleep Sensors.

Like the pedometer, sleep sensors use either a 3-way gyroscope or a 3-way accelerometer and some algorithms with software to determine how well you slept at night. Then using the algorithms and software, it will determine whether you were awake or if you were in deep or normal sleep.

Implementation.

Fingerprint, facial, iris, and retina scanning have their uses in security. According to Apple Insider (2010), a patent Apple Inc. filed for in 2009 could, "detect a user's heartbeat when the phone is picked up. That biometric data can be used to identify an individual." (appleinsider.com) So a heartbeat sensor could be used not only for health purposes, but also to identify the particular user. Heartbeat sensors and pedometers have quite a few uses in health and fitness. The sleep sensors have their use in health and fitness as well, and are already being utilized in the Jawbone UP and UP24 bands. There is no knowing what other technologies companies will look at utilizing for further use in electronics. Most smart phones, laptops, and

even desktop computers have a built in camera or have the ability to do third party USB camera. It would not take much to adapt this, currently used technology, and turn it in to an iris scanner. According to Juli Clover at MacRumors (2014), iris scanners have been used in Amsterdam Airport and in the United Arab Emirates at boarder crossings as an alternative to a passport. And Google has been using iris scanners for entry into its data centers (macrumors.com).

Security Concerns

As these technologies have many benefits, they also come with concerns. How is this data being protected from someone that has stolen your phone, or someone trying to hack your computer? As Tom Risen (2013) says, “The risk that a user's fingerprints could be duplicated to access a phone” (usnews.com) is a complete possibility. As detailed on the video in Tom Risen’s article, Apple Inc. has thought about this concern, and has dedicated a place in its phones CPU that stores the fingerprint information. It is not saved on their servers, nor is it even saved in back up files. These concerns stem further then the fingerprint scanner. As companies make these technologies more main stream, it can also make thieves more aware of how to get around the technology. It takes the idea of identity theft to a new level. Only time will tell how companies are truly securing this information from intrusions.

Conclusion

Biometric scanners are becoming more common place rather then science fiction. It is being implemented into wearable technology, smartphones, and computers. Technologies such as fingerprint scanner for security and heartbeat sensors for health. Security might be a purpose for these technologies but it also brings up concerns for these technologies. How are companies keeping this information secure from people that want to steal and or use this information?

Reference List

Apple's future iPhones could recognize a user by their heartbeat. (2010, May 6). *Apple's future iPhones could recognize a user by their heartbeat*. Retrieved February 24, 2014, from http://appleinsider.com/articles/10/05/06/apples_future_iphones_could_recognize_a_user_by_their_heartbeat

Used for potential implementation of heart beat sensors. Useful information on the patent that Apple Inc. had submitted to the U.S. Patent Office. Contained some speculation but other wise a good source.

Biometrics. 2014. In *Merriam-Webster.com.* Retrieved February 11, 2014, from http://www.merriam-webster.com/dictionary/biometrics

Used for the definition of the word Biometrics. This source was very good for defining the word biometrics as well as some light history of the word biometrics.

Clover, J. (2014, January 21). Iris Scanning: The Newest Addition to Apple's Biometric Roadmap?. - *Mac Rumors*. Retrieved February 25, 2014, from http://www.macrumors.com/2014/01/21/apple-iris-scanning/

Used for information pertaining to current use of iris scanners. The information was good but contained more then what was needed.

Risen, T. (2013, 09). Privacy pros and cons of the iPhone 5S fingerprint scanner. *U.S.News & World Report,* , 1. Retrieved from http://search.proquest.com/docview/1448375069?accountid=14541

Used for information on how Apple Inc. is using a fingerprint scanner in a handheld device. As well as used for seeing how the fingerprint scanners can bring up security concerns.

Also contained Apple Inc. video on how TouchID works. Was not as good as it could have been, it provided more comments by others, rather then evaluating why this technology could be bad.

Trader, J. (2011, June 11). Iris Recognition vs. Retina Scanning - What are the Differences? - M2SYS Blog On Biometric Technology. *M2SYS Blog On Biometric Technology*. Retrieved February 23, 2014, from http://blog.m2sys.com/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/

Used to gather information on retina and iris scanning and how they work. This blog post has more information that what was really needed, but provided good detailed information on how both of the technologies work.

Up. (n.d.). *Jawbone*. Retrieved February 24, 2014, from http://jawbone.com/store/buy/up24

Used for information on how they use their sleep tracking systems. Was a useful source but had unneeded information.