Your Digital Pulse

Brenda A. Paredes

IT 104 – 009

February 27, 2017

"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-2/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. 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

In his book, “Going Solo”, NYU sociologist Eric Klinenberg wrote that in 1950, only ten percent of people in the USA lived alone. He put that figure today closer to twenty-seven percent. In the same book, he writes while only twenty-two percent of adults from that time were single, that number now nears fifty percent. As a direct consequence of this phenomenon, technology companies all over the world now strive to find new ways to market their products to an increasingly fragmented and private society. According to BBC profile on Howard Hughes, the inventor, lived in squalid solitude suffering under the yoke of OCD for years. Affording him convenient access to self-care may well have improved his quality of life as well as advanced the understanding of his ailment for others. The tech startup, Scanadu enters the new households of today in a novel way, by enabling a user to control his own healthcare using an app. The Scanadu app and its accompanying investigational device were developed to keep a user informed of his basic health data: pulse oximetry, heart rate, temperature, and blood pressure (Jankowski, 2016). Self-diagnosis based on Scanadu data can prompt a user to seek treatment. It may also prompt a user to believe he knows better than a doctor about his own health (McMahon, 2013). If the stored data is shared to an unethical third party, however, the data could be used to compromise the privacy of user to his detriment. By examining how well the machinery of Scanadu works in conjunction with the potential health benefits of using it; and contrasting it with the potential for privacy abuse, mechanical dysfunction, and antisocial behaviors fueled by a society becoming more reliant on apps than human contact, we will see that this app is an example of a technology to be regulated carefully.

Background/Current Use

Walter de Brouwer conceived of the Scanadu in 2003 after his five-year-old son plummeted forty feet to the ground and into a coma that lasted eleven weeks. De Brouwer learned that none of his son's various health data was being consolidated for collective analysis (Hardy, 2013). Scanadu is a health services app that employs a purchased scanner called Scanadu Scout Investigational device. It is non-invasive. It measures temperature, heart rate, blood pressure, and pulse oximetry. (Jankowski, 2013) It boasts a 32 bit RTOS Micrium platform. According to their crowdfunding page, this is the same technology employed to collect sample data on Mars by the Rover Curiosity. A user holds a light-weight, thirty-six gram, disc-shaped sensor to the forehead for ten seconds, and the data listed above is transmitted to the app (Peppet, 2014). The building material is not currently defined in the material sheet or by any other credible source. The latest edition relies exclusively on optical sensors as opposed to the electroencephalographic technology of the older models. In other words, it uses modified lasers to take its measurements. This feature allows the Scanadu to take measurements from anyone in the room, not just the person holding it. Other systems such as the electrocardiogram, or the electroencephalogram, rely on electrodes placed on the body to record the electrical impulses of the relevant organ (Ginn & Jamieson, 2006). This device measures multiple systems with a comparatively simpler ten second placement of the investigational device's sensor on the user's forehead. The reliance on optical sensors has multiplied its need for a more complex computational brain. A real-time operating system, or RTOS, is an operating system that guarantees a certain functionality within a specified time constraint (Micrium, 2017). The best way to think of it is a factory line. A robot expects to have a certain piece of hardware to continue its work. If that hardware is not present at the right moment, the entire line shuts down. This kind of system is designed so that does not happen. The program

will continue building the item until all components it needs to complete are present, though productivity may decrease. (Micrium, 2017) Once the data is absorbed into the scanner, the communication between scanner and app takes place through Bluetooth technology. Bluetooth is a widespread wireless technology used for exchanging data over short distances using ultra high frequency radio waves (Bluetooth, 2017). Devices can be put into what is called discoverable mode, and then can attach to each other as if on a wired network (Bluetooth, 2017).

Accuracy of hardware is not this tool's primary selling point. Though it boasts a 95% accuracy of pulse oximetry that is not a significant difference than an electrocardiogram (Ginn & Jamieson, 2006). It also makes no claim to be more accurate than an electroencephalogram anywhere on its tech sheet. Also nowhere to be found is a heightened accuracy of blood pressure measurement. It is designed to be a one stop shop for common clinical measurements according to its own authors. Nearly every article discussing this device employ a Star Trek-moniker when describing this machine. That appears to be in response to Scanadu's winning a famous and lucrative Qualcomm competition to invent a medical tricorder (Gorman, 2013). For those unfamiliar with the Star Trek series, a tricorder was a tool that could measure unseen injuries within seconds of being passed over the sufferer. The website steers clear of such claims, preferring to focus on its ability to stockpile useful medical data for a user over time, the stated goal of its inventor way back in 2003. (Hardy, 2013)

On its website, it lists several disclaimers. It keeps a living history of all scans done for the individuals it scans, ostensibly, to help users see if there is an underlying health issue. In addition to the scans, an individual is prompted to input all height, weight, age, info into the app. It goes on to mention that future updates may include requests for more detailed personal information. The website further states that it is not a diagnostic device but rather an investigational device. This

difference appears legal and semantic rather than functional. The nature of the device is explicitly, according to their narrative on the website, intended for diagnostic purposes by the user. That said, they must distinguish themselves legally from approved FDA diagnostic devices during development period.

The developers go on to warn users that they should always consult a physician regarding any medical condition. On the surface, the app is aimed at putting healthcare data in the individual user's control. The obvious logic here: No one would argue that one's health data would be better served in the hands of a distant analyst. Let the users of the app responsibly decide how to employ their own health data when dealing with a health concern (Journal of Engineering, 2017). It allows users to aggregate a multitude of usable data that can used by medical professional to either begin or focus their own diagnosis. Thus far, this device seems to be a boon to people like Howard Hughes who eschew medical care but need it as much if not more than anyone else.

Security

As useful as a device like this can be medically, we have to examine if that utility is outdistanced by any other pressing concerns, such as security or privacy. Tom Kellermen, a chief cybersecurity officer for Dallas software Trend Micro states that a hacker could gain access to one of your appliances, and through it, your entire network—possibly including a baby monitor (Strom, 2015). The case of Scanadu is unsettling. "Any information that is provided to a third party vendor is to be used only for the purpose of performing the analytics and compiling reports of the information (Scanadu Privacy Policy)." In other words, by consenting to the Scanadu privacy agreement, you do consent to third-party disclosure. The upside is that if they get new software that makes it easier to detect an impending heart attacks, user data may be well-served by such a revelation. If, on the

other hand, Scanadu shared your data to an unethical source, it could be used to compromise the user. If insurance companies pay Scanadu to reveal pre-existing conditions in their users, they could use that data to disqualify someone from coverage. Their user agreement makes both eventualities possible. (Bayer & Fairchild, 2000)

But this is not the worst of it. Bluetooth itself is susceptible to hacking. Bluesnarfing is a common method for gaining unauthorized access to the data of any Bluetooth connection. Using a technique called war driving, a person can drive through neighborhoods using a portable computer or a smartphone attempting to discover active Bluetooth networks in order to gain access to them. (Paus, 2017) Once a device is put in discoverable mode, the data it collects is open to outside attacks of this variety. In exceptional circumstances, devices not in discoverable mode can be access by piggybacking nearby discoverable ones (Steinberg, 2015). Most famously, in 2011 in Seattle, police arrested two men who they allege had been driving around for years stealing data worth almost a million dollars from various networks (Liebowitz, 2011). Though Bluetooth has made improvements in its security grid since then, according to their own tech sheets, they are still vulnerable to targeted attacks of this kind, recommending users keep Bluetooth devices out of discoverable mode when they are fearful of malicious attacks (Steinberg, 2015). By extension, Scanadu is vulnerable to this type of attack. Since malicious attacks can come through this fishing expedition-style attack called wardriving, it would seem a user has frequent cause to have that fear. The Department of Health and Human Services Office for Civil Rights estimates that at least 95,000 medical records were compromised in June 2016 (HIPPA, 2016). The HIPAA Journal, or the journal charged with evaluating the safety of the individual's private medical data, in June 2016, estimated that 41% of breaches were the result of hacking, another 41% was insider theft and errors, the remaining 18% made up of both physical loss of paper data or devices containing

data. Until Bluetooth or another company find a more secure way of safeguarding data for Scanadu, they seem ill-prepared for the present security climate.

Legal and ethical issues

There are more personal concerns to consider here in addition to outside security threats. Though under no circumstances will a US citizen be compelled to tender evidence against themselves, there are private situations where users are willing to surrender that right. By signing an interminably long, or vaguely worded consent agreement for Scanadu, one may surrender his own rights. We willfully allow ourselves to be searched at airports in the name of safety, perhaps not realizing that TSA agents did in fact keep body scan data despite many assurances that they were not stored (McCullagh, 2010). Also, in the case of voluntary drug-testing for employment, for example, someone does turn over evidence that can be used against them. But, since it takes place outside of the courtroom, the legal issue does not strongly arise. Even so, being precluded from a job or health coverage because of hacked, leaked, or sold private data is a palpable consequence. Scanadu clearly asks for consent at several stages along the way. Though they may appear to be a health app with the user's best interests in mind, the lack of liability it possesses in relation third parties should give all users a moment a pause when signing up for the service. It appears to take the ownership of the data away from the end user and put in the hands of entities who may not have that user's best interests at heart, or even the best interests of the app's designer.

Social problems

As stated in the introduction, the data suggests we are much more a society of loners than we once were. It raises contradictory questions. Are we making ourselves more isolated because of technology, or is the free exchange of data making it unnecessary to remain social creatures? Or both? Increasingly, convenience of communication is verging on necessity. Scanadu opens a door

to a world where a person's health data could be known before they arrive at a hospital or doctor's appointment. The impersonal nature of data in relation to an in-person diagnosis would further an already spiraling trend where interacting with people is less preferable than interacting with machinery. One study showed that regular use of Facebook led directly to marked bouts of depression (Guernsey, 2014). As every app and smart appliance becomes more and more in tune with the data of the user, not participating in the trend could produce marked antisocial behaviors with dire consequences. While not participating in Scanadu and apps like it do not pose an immediate threat to user safety, it is possible that the trend they are a part of, will do exactly that.

This is raised on their own website. No medical decision should be made without visiting a physician, they say. Thus, in spite of the device potentially making your medical life more apprehensible to a medical professional, there is a risk of it discouraging the user from using the data at all. There are very high profile cases in Japan and the US of young people not willing to leave their homes so they could spend time with their electronic devices (Samakow, 2013). This happens too often to be anecdotal. Encouraging patients to employ devices like this may amplify a tendency to remain at home and not seek the company of others, let alone medical professionals. Internet fasting camps have popped up all over Japan (Somakow, 2015). Internet addiction treatment centers are widespread in the US (Foran, 2015). The data does not yet support the idea that using smartphones or smart devices in excess constitutes a health threat, but it would appear that given the rise of these camps and treatment centers, it is not premature to be wary of things that increase our desire to avoid social interaction.

Conclusion

Scanadu and many other companies are constantly creating products apparently designed to alleviate burdens, ease diagnoses of health conditions, and enlighten the public. Scanadu is a compelling example of a technology that is both useful and dangerous. In spite of promising practicable medical advances, a user chooses between helping themselves improve their quality of life and exposing themselves to crippling vulnerability. By looking at these, it is apparent that we must not only be vigilant about accepting this technology as a part of progress, but find a better way to protect the isolated among us.

References

Bayer, R., & Fairchild, A. L. (2000). Surveillance and privacy. *Science, 290*(5498), 1898-9. Retrieved from https://search-proquest-com.mutex.gmu.edu/docview/213582455?accountid=14541

The article discusses privacy concerns that can arise from the Scout devices by connecting to smart phones and sharing data with doctors. The article states that there are five themes that explain when surveillance is accepted or rejected ethically. The article is a credible sources as it does not take a stance on Scanadu. Rather, it reports on possible shortcoming. Providing an unbiased sources.

Buhr, S. (2016). Scanadu to shut down support for its scout device per FDA regulation and customers are mad.

The article discusses how SCANADU's use of it's Scout technology has been shut down by the FDA. The article states that the FDA did not comment on the reasons for shutting down the use of Scout. The purpose of Scout was to detect vitals such as temperature, blood pressure, and heart rate. SCANADU states that the device must be deactivated due to the investigational nature on which the device was launched. SCANADu states that they will continue providing other similar services.

Foran, C. (November 5, 2015) The rise of the internet-addiction industry. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2015/11/the-rise-of-the-internet-addiction-industry/414031/

Ginn, P. H. , & Jamieson, B. (June 2006). How accurate is the use of ECGs in the diagnosis of myocardial infarct? *Family practice, 55(6).* Retrieved from http://www.mdedge.com/jfponline/article/62227/cardiology/how-accurate-use-ecgs-diagnosis-myocardial-infarct

Gorman, M. (May 22, 2013). Scanadu finalizes tricorder design, wants user feedback to help it get FDA approval. *Engadget.* Retrieved from https://www.engadget.com/2013/05/22/scanadu-scout-tricorder-final-design/

Greenberg, A. (July 26, 2016) Radio hacks steals keystrokes from millions of wireless keyboards. *Battelle.* Retrieved from https://www.wired.com/2016/07/radio-hack-steals-keystrokes-millions-wireless-keyboards/

Guernsey, L. (February 19, 2014) A cautionary tale of pediatricians, parents, and Facebook. *Slate.* Retrieved from http://www.slate.com/blogs/future_tense/2014/02/19/facebook_depression_scare_offers_a_cautionary_tale_of_pediatricians_parents.html

Hardy, Q. (25 December 2013). Personal Tragedy, Tricorders and the Idea of Mapping One's Body. *The New York Times.* Retrieved from https://mobile.nytimes.com/blogs/bits/2013/12/25/tragedy-tricorders-and-aspiring-to-map-ones-body/

HIPAA Journal. (July 11, 2016) Major 2016 healthcare data breaches: mid year summary. *Hippa Journal.* Retrieved from http://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/

Howard Hughes. *BBC.* Retrieved from http://www.bbc.co.uk/science/humanbody/mind/articles/disorders/gallery/gallery_case6.shtml

Lazarus, D. (January 15, 2016). Our privacy is losing out to Internet-connected household devices. *Los Angeles Times.* Retrieved from http://www.latimes.com/business/la-fi-lazarus-20160115-column.html

Liebowitz, M. (April 25, 2011) 'Wardriving' hackers cracked Wi-Fi networks from black Mercedes. *NBC News.* Retrieved from http://www.nbcnews.com/id/42754967/ns/technology_and_science-security/t/wardriving-hackers-cracked-wi-fi-networks-black-mercedes/#.WLT3PoWcH6U

Jankowski, T. (February 22, 2016). Quantified Self: How does the Scanadu Scout measure blood pressure? *Quora*, https://www.quora.com/Quantified-Self-How-does-the-Scanadu-Scout-measure-blood-pressure\

The article explains the way in which the SCANADU scout is able to accomplish its many task. The article states the devices that make up the Scout that allow it to measure body temperature, blood pressure, and heart rate. The EEG and blood pulse are two sensors that allow the Scout to measure Pulse Transit Time. The article also states what a certain diagnoses may indicate about the users body.

McMahon, T. (2013, Feb 27). The smartphone will see you now. *Maclean's, 126*, 46. Retrieved from https://search-proquest-com.mutex.gmu.edu/docview/1313218253?accountid=14541

The article discusses another device developed by SCANADU that can be used at home. The test strips can be scanned by the users phone to analyze saliva for strains of flu or strep throat. The strips can also analyze the users urine sample for infections or renal failure. This source is very reliable as it is a scholarly article. It reports on SCANADU's most recent development with smart phones and their apps.

McCullagh, D. (August 4, 2010) Feds admit storing checkpoint body scan images. *CNET.* Retrieved from https://www.cnet.com/news/feds-admit-storing-checkpoint-body-scan-images/

Paus, L. (February 2, 2017). Wardriving: A digital census of Wi-Fi networks? *ESET.* Retrieved from http://www.welivesecurity.com/2017/02/02/wardriving-digital-census-wi-fi-networks/

Peppet, S. R. (2014). Regulating the internet of things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review, 93*(1), 85-176. Retrieved from https://search-proquest-com.mutex.gmu.edu/docview/1636877419?accountid=14541

The article discusses the privacy and security concerns that arise form devices such as the SCANADU Scout or more generally health devices that connect to smart phones. The article discusses the collection of information and how it would be secured. The possibility of discrimination that can occur due to the collected data is also discussed. The source is reliable as it is a scholarly journal. Additionally, it does not solely focus on the SCANADU Scout.

SCANADU INCORPORATED; patent issued for method and apparatus for determining analyte concentration by quantifying and interpreting color information captured in a continuous or periodic manner (USPTO 9528941). (2017). *Journal of Engineering,* , 6402. Retrieved from https://search-proquest-com.mutex.gmu.edu/docview/1855887324?accountid=14541

The journal discusses a patent by SCANADU incorporated which involves the quantitative analysis of urine. Currently, such test result in a color change from the dipstick used. SCANADU proposes a more technological method in which a machine can more precisely quantify any color change. This eliminates the human error that can arise thus leading to inaccurate diagnosis. The source is reliable and provided an objective reporting of SCANADU's most recent development. The technology here is similar to that in SCANADU Scout.

Steinberg, J. (October 20, 2015). Why your Bluetooth Devices Aren't as Secure as You Think. *Inc.*. Retrieved from http://www.inc.com/joseph-steinberg/are-your-bluetooth-devices-secure-maybe-not.html

Strom, D. (April 22, 2015) 2 more wireless baby monitors hacked: Hackers remotely spied on babies and parents. *ComputerWorld.* Retrieved from http://www.computerworld.com/article/2913356/cybercrime-hacking/2-more-wireless-baby-monitors-hacked-hackers-remotely-spied-on-babies-and-parents.html

Samakow, J. (August 28, 2013) Japan internet 'Fasting Camps' aim to treat screen addicted kids. *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/2013/08/28/japan-internet-fasting-camp_n_3824697.html

(2017) How it Works. *Bluetooth.* Retrieved from https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works

(2017) The number one RTOS on Earth. *Micrium.* Retrieved from https://www.micrium.com/rtos/