Ethical Concerns of RFID Tag Implants in Humans

Wyatt Croucher
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
wyatt.croucher@wsu.edu

Drayer Sivertsen
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
drayer.sivertsen@wsu.edu

Trevor Naze
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
trevor.naze@wsu.edu

Ethan Burchett
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
ethan.burchett@wsu.edu

Mitchell Kolb
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
mitchell.kolb@wsu.edu

Yingqiang Yuan
School of Electrical Engineering and Computer Science
Washington State University
Pullman, USA
yingqiang.yuan@wsu.edu

***Abstract*— This report discusses the ethical concerns of RFID tag implants in humans. These implants can be used for a variety of uses, including tracking missing persons, use as a payment method, and accessing medical information. Without proper insurance of their safety for users, the use of these tags could lead to massive data security breaches, and users would be at risk for having their personal information stolen. This study will address the ethical concerns surrounding the use of these devices in the context of social contract theory, rule deontology, and utilitarianism and propose conditions to be met in which the risk for individuals who use these devices will be decreased.**

Keywords*— *RFID, implant, security, ethics, SECEPP

I. Introduction

Radio Frequency Identification Device (RFID) Tag Implants are a new twist on the already widely used RFID technology. RFID is commonly used in inventory tracking, employee tracking, and supply chain visibility. An RFID device allows a reader to communicate with the tag and get unique information that it stores along with its location. The most recent implementation of RFID technology occurred in Taiwan, where the government mandated that all pet dogs receive an implanted RFID tag so they can be identified and returned to their owners in case they go missing. The VeriChip Corporation has developed a similar implantable chip but for use in humans. Such a device would contain the user's health information and could be accessed in the case of an emergency. The chip would also have locational capabilities and could be used to find missing persons or even for a more practical use such as an embedded credit card.

Given the invasive nature of such a device, both physically and informatically, it is important that all ethical concerns are addressed. This case study will explore the most predominant ethical concerns and do so by analysis using Social Contract/SECEPP, blank, and Utilitarianism. Specifically, this study will address the following questions: Are RFID tag implants for humans ethically acceptable and what usage policies will ensure that the product's ethics are maintained? Proposing a solution to this ethical challenge will enlighten how RFID Tag implants can be used effectively and with the users best interest in mind.

II. Case Summary

In this case study, we will explore the potential ethical ramifications of emerging RFID technology as it relates to implantable human ID tags. For this study, we will ignore the potential ethical issues that would arise if a state or government apparatus were to mandate the implantation of its citizens as it is beyond the scope of this study. We will assume that the implementation of this RFID project would be in a free and open society where individuals could choose and not be compelled to be implanted by an authority.

Radio-frequency identification technology is not new, it was first developed in the mid-20th century and allows for automatic and passive identification within a certain close range. The RFID chip must physically come into very close proximity with the receiver for authentication to work. The RFID chip consists of a small transponder, a device that when activated by an RFID reader radio pulse, emits an identification number signal that can be interpreted by the RFID reader. This ID number is then sent to a central database to retrieve the personal data of the individual. How this personal data is stored, and the privacy protections allowed to identifiable materials is a larger software engineering and privacy problem and outside the scope of this study. The tag itself can be very small, about the size of a grain of rice, and as it is a passive electronic instrument, it does not require power to function. As we have seen with RFID tags in veterinary use, they are effective for returning lost pets to their owners, cause minimal harm to the patient, and are biologically stable when embedded in tissue for years. The techniques used to implant ID chips are reliable and safe for animals and could be adapted for human use easily. There are several companies today who offer reprogrammable RFID implantable chips for human use, these are popular in "biohacker" communities, but as of 2022, RFID implants have not caught widespread public attention or adoption. [1] Over the last several decades, there have been improvements in human implantable technology, ranging from a powered device with full GPS location services to a simple magnet implanted under the skin.[2] RFID technology has a proven track record of both being very effective in tracking ID tags, both when implanted and when part of an inanimate product.

There are many use cases for such devices: instant payment at businesses, verification for public transit, concert tickets, parking meter payments, medical history, and others [3]. We have seen similar applications with services like Google and Apple pay through consumer smartphones. The modern RFID implementation used in smartphones is likely going to be used more than implantable chips, due to the ease of use, widespread adoption of smartphones and the perceived harm or impact of implanting a chip in tissue. There are other ethical issues to consider as well, possible governmental overreach and invasion of privacy is one. We must understand that if this technology is issued by the state, and our government issued ID is also embedded in this personal identifier, then the state will be able to surveil our person to a much greater extent. For those who are concerned about state surveillance, this type of activity should give cause for concern.

Aside from potential misuses of personal data from governments, we will also look at the potential security risks present from malicious actors who can attempt to both harvest your personal identification number as well as spoof your ID. There exist cheap portable devices that can detect nearby RFID chips. There also exist devices that can send the same ID signal to an RFID receiver, "spoofing" the presence of the ID chip. A bad actor could steal your identification, then impersonate you and gain access to your privileges. This could include fraudulently purchasing items or gaining access to restricted areas. Without alternate forms of authentication, there is little an organization can do to prevent bad actors from misusing spoofed RFID access tokens.

III. Ethical Analysis

RFID tag implants could potentially be deemed unethical in certain situations. Since these tags are used by individuals to access sensitive information like financial and personal information, others could try to read one of these implants without the user's consent and collect their information. To evaluate the ethical concerns of this topic, we will utilize the following ethical theories and models to address concerns surrounding these tag implants in hopes of creating a set of guidelines that must be meet to make their widespread use ethically acceptable.

A. *Analysis Method #1: Social Contract / SECEPP*

One of the ways we'll be examining the case is through the lens of social contract theory. Companies are beholden to domestic and international laws regarding the use and disclosure of information of their customers, and since companies that create RFID chips are providing a service both to themselves and other companies, will be held to the standards of these laws. Due to this, an opportunity is presented to analyze the ethics of the issue using Social Contract theory, an ethical system that looks at natural and legal rights to determine if a behavior can be viewed as ethical.

Companies are expected to follow common industry practices such as the SECEPP code of ethics that hold them to only provide software and services when they have a well-founded belief that the software does not diminish privacy and serves the public good (SECEPP 1997, 1.03, 3.12) as well as disclose to users potential dangers to the software towards users (SECEPP 1997, 1.04).[4] In addition to practices and standards established by the industry to regulate itself, companies are also beholden to national and international data privacy laws. The European Union's General Data Protection Regulation requires that companies must take "appropriate technical and organizational measures" to ensure that user data is handled securely.[5] On a national level, laws such as the Health Insurance Portability and Accountability Act (HIPAA) require that healthcare providers go through stringent requirements if they are to conduct transfer of health information from one party to another, as well as take measures to "ensure the confidentiality, integrity, and availability of all electronically protected health information" as well as to "detect and safeguard from anticipated threats to information security" and to "protect against anticipated impermissible uses or disclosures."[6]

Under these rigorous national and international laws, companies intending to use implanted RFID technologies must make all adequate and reasonable measures to ensure that user information is protected and make all reasonable attempts to prevent the unintended disclosure of PII or user identification. Early adopters of RFID technology such as VeriChip use systems that when scanned simply return a user ID. With no protection from any sort of man-in-the-middle or ID replay attacks, these chips provide an attack vector where malicious users could get access to health data without the consent of the patient by reading the ID the chip returns, and using it at a later point in time.[7] Due to these vulnerabilities, systems that simply return user IDs such as those used by early adopters like VeriChip must be redesigned to help prevent duplication or malicious use by bad actors if they are intended to act as an independent system for user identification or authentication.

B. *Analysis Method #2: Rule Deontology*

Another way we'll be analyzing the ethics of RFID implants in humans is through the eyes of rule deontology. [8] Rule deontology is a duty-based ethical theory where each individual's morality is based on the obligations that each person has to the other. The consequences of the situation are never put onto the actions of a person. It as well focuses on the preservation of individual rights and the intentions associated with a particular behavior rather than on the consequences. How this ethical theory relates to RFID tags in humans is because there needs to be a relationship between the company that produces or analyzes the tags and the people who have them attached to them. [9] RFID tags are used mostly in scientific work and this is what is happening. Patients with diseases or medical conditions are allowing these groups to tag them so they can be monitored more easily. As long as this is upheld and the individual rights of the works if the tags and patients who have them are always in consideration ethically in the eyes of deontology this works.

Part of this analysis is to talk about both sides of the situation and regarding this topic, it is important to know how RFID implants can compromise an individual's rights and possibly force the person to go down an immoral path to try and protect themselves. One of the ways that RFID tracking can be used maliciously is if the company decides to sell away the information that they collect about a certain individual. [8] This doesn't follow Rule Deontology because humans have obligations to each other to act in a morally correct way and if the company sells away their data to make a profit that breaks that relationship between each other. [9] Another way that RFID chip tracking can be used is if the company collecting that data begins to do research and draw conclusions based on that data that negatively affects the person who produces that data. For example, what if a person has a medical RFID tracking chip in them and they are monitored by a company that comes to the conclusion that this person will have a high risk of some disease and the patient's insurance decides to no longer serve them. This negatively affects the RFID patient and is something to think about when analyzing this through the lens of Rule Deontology. We should try and lower the chances of these situations occurring to get RFID chips to abide by the ideas that rule deontology discusses.

C. Analysis Method #3: Utilitarianism

Meanwhile, there is another important approach that may yield innovative analysis of the same matter above, which is from the perspective of act utilitarianism and rule utilitarianism.[10] By applying the model of act utilitarianism, we are going to consider what are the actions that need to be done to maximize the interest of each entity involved and thus, ensure the moral acceptability of the given idea. To accomplish such a goal regarding our case, there are a lot of actions that need to be done, or potential flaws that we need to fix for the sake of making RFID tag implant ethically acceptable.

First of all, companies that work on RFID tag implants need to make sure the data they are collecting is safe and sound from the potential attackers who would take advantage of owning that data without permission. To accomplish this goal, I would suggest that companies should collect data from users with a pattern that is difficult to figure out from outside. To be more specific, there needs to be multiple servers that are ready to take in the data and they receive the data randomly. Only in that way, those who intend to attack the connection between the users and companies and steal the data would not know which device is going to upload data, which server is going to receive the data and when is the appropriate time to attack. Second of all, users should have the right to shut down the service to protect their privacy such as information about whether they have an STD etc.[11] Last but not least, the companies also need to make sure they spend enough resources, so criminals do not take advantage of such services and potentially cause unwanted difficulty for users and police to find the lost. More specifically, companies need to develop an alarm system that is easy to use and hard for criminals to disturb.

From the perspective of rule utilitarianism, it is even more difficult to make it ethically acceptable because if the medical industry can do it, the government can do it as well and probably collect the vast amount of data that you could never imagine.[10] If the service that companies in the health industry can develop can track lost children, the government would have the power to track everyone and make sure to keep it discreet. At the same time, it would be difficult to efficiently figure out the balance of collecting data and protecting data for different industries. During that process, the lawful interest of people would be harmed intentionally or unintentionally.[11]

IV. Recommendations

While RFID tag implants do have the potential for being beneficial to people in a wide variety of settings, it's very important that this technology meet several criteria in order to protect its users. In regards to the social contract theory, the use of RFID tag implants have the potential of being ethical as long as the previously stated concerns of privacy and disclosure of potential dangers have been addressed. One could argue that privacy is a natural right for individuals, and we as a society have a social contract to uphold that right for others. If the concerns regarding security and privacy are formally addressed by those who want to produce these microchips, then the distribution of RFID tag implants could be ethical.

Rule deontology is a duty-based ethical theory, where morals are founded on obligations humans have to one another, and never on the consequences of human actions. Again, our main concerns with the use of this technology is the preservation of any individuals privacy, whether that be from the companies that manufacture and process the data from these microchips, or from individuals who attempt to read someone's microchip without them knowing. One could reason that in this context, humans should uphold the level of privacy for others that they'd expect for themselves. With this in mind, we can create a general rule along the lines of "always ensure the safety of user's information before product deployment" which should be upheld by the companies that manufacture these microchips, as well as any other third-parties that may be involved with the processing of data/transactions from these microchips.

In the context of utilitarianism, RFID tag implants could be ethical given that we are creating the greatest amount of good for the greatest number of people. Act utilitarianism emphasizes that an act is ethical if it does the greatest amount of good for the greatest number of people. While the use of these chips could do a lot of good for a lot of people, if the concerns to user privacy are not addressed and user privacy isn't assured, then one could reason that the standards of act utilitarianism are no longer being upheld. Rule utilitarianism is the application of a general rule that also emphasizes the greatest good for the greatest number of people. If we look at our previously stated rule for rule deontology: "always ensure the safety of user's information before product deployment", since we can reason that (ideally) there would be more users compared to individuals that make these chips and process their transactions, this rule also would be beneficial for consumers in the context of rule utilitarianism.

We need to ensure that someone's information couldn't be stolen if someone found a way to read these tags without the user's knowledge. A secure channel is even more important with implants because of the fact that implanting removes a critical physical security method. NFC and RFID typically benefit from the physical security requirement of a very short distance, typically less than a few inches. If someone wanted to eavesdrop on a communication or steal your identification information, it'd have to be very obvious since they'd need to have a reader within inches of your card or NFC device. You don't get that benefit from RFID implants. Typically the implants go in your hand, and so now if you have an implant, you have to consider how close your hand is to things. If an attacker wanted to hijack the ID of an implant, it is much easier for them to do because they could simply offer a handshake, or hand you their phone. It's much easier for a stranger to get in close proximity to your hand, then it is to a security badge or wallet. Because of this, the most reliable security measure for RFID is thwarted, and additional measures must be put in place in order to ensure that the information that identifies a user is protected. One method for doing this would be to implement an encryption method. Encryption is a method used for translating information into an undecipherable format in which only the intended recipient can decode using an encryption key. However, there are a few issues with encryption in this scenario. Most encryption is done by a sender and a receiver, where the sender encrypts the message using an encryption key, and the receiver decodes the message with the same or complimentary encryption key. The problem is that a RFID tag implant doesn't have the capability to create an encrypted message for each transaction. It could be possible for the RFID information to be encrypted before being stored in the tag, however since the code never changes this could be easily hacked. We need a method in which once a transaction is triggered, some kind of authentication is performed in order to complete the transaction. This process should be performed by the company that produces the microchips, or by an authorized third party to help accommodate for the volume (however, the number of third-parties should be limited as much as possible to reduce the amount of user data distribution, which would help with the protection of said data). Without the assurance of proper data encryption, RFID tags shouldn't be used due to the level of sensitive information someone steal get from someone else's tag.

Additional security measures should be put in place to ensure that these devices won't be used for purposes outside of the user's intent. Since some of these devices could be used to track someone who is lost or missing, restrictions need to be in place to prevent companies or government organizations from collecting data of user's whereabouts without their knowledge. We recommend that privacy laws should be passed that state that it would be illegal for any government or organization to use the data from any individual's RFID tag without the written consent of said individual. In the United States, California is the only state that adheres to a consumer privacy act, and no such privacy laws are adhered to on a federal level.[12] In order to support the individuals who want to utilize the RFID tag implant technology, the act itself should read that "The protection of an individual's information and privacy should always be considered first and foremost before distribution of a product to the general public for consumption." We would have this implemented by going to congress and having the privacy act voted on during the next federal election. Since this act would protect a large number of Americans (even outside the context of RFID tag implants), this act would be ethical under the principles of utilitarianism. Privacy can be considered to be an inheritance right, and it's one's duty to ensure that right is upheld for others, making this proposed act also ethical in the light of the social contract theory and rule deontology. We believe that adhering to this proposed act is critical for upholding an individual's right to privacy.

V. Conclusion

Radio Frequency Identification Device (RFID) Tag Implants are a new twist on the already widely used RFID technology. RFID is commonly used in inventory tracking, employee tracking, and supply chain visibility. An RFID device allows a reader to communicate with the tag and get unique information that it stores along with its location. RFID Tag Implants for use on humans presents a good deal of ethical problems. The majority of time spent in the product's development focuses on the usability aspect of the technology and less of the privacy risks that a more personalized technology may bring. Much of the information that is planned to be stored on the implant is personal information about the user (medical history, location). Without proper encryption and security measures in place, ethical concerns related to privacy are not manageable. By analyzing the lack of security through a Utilitarianism lens and with the SECEPP it is clear that the RFID Implant is littered with ethical red flags. After determining the product's shortcomings, a resolution was presented that addresses the ethical problems that the technology has. We believe that the addition of a secure encryption method for data transactions to and from an RFID device would be the optimal solution. With safer data, the privacy threat to a user would be alleviated and the positive benefits of the technology would be felt seamlessly.

References

[1] S. R. Bradley Munn, K. Michael and M. Michael, "The social phenomenon of body-modifying in a world of technological change: past, present, future," 2016 IEEE Conference on Norbert Wiener in the 21st Century (21CW), 2016, pp. 1-6, doi: 10.1109/NORBERT.2016.7547463

[2] K. Michael, "Go ?Get Chipped?: A Brief Overview of Non-Medical Implants between 1997-2013 (Part 1)," in IEEE Technology and Society Magazine, vol. 36, no. 3, pp. 6-9, Sept. 2017, doi: 10.1109/MTS.2017.2742238.

[3] K. Michael and M. G. Michael, "The diffusion of RFID implants for access control and epayments: A case study on Baja Beach Club in Barcelona," 2010 IEEE International Symposium on Technology and Society, 2010, pp. 242-252, doi: 10.1109/ISTAS.2010.5514631.

[4] Gotterbarn, Don, et al. Software Engineering Code of Ethics. Association for Computing Machinery Committee on Professional Ethics, Nov. 1997, ethics.acm.org/code-of-ethics/software-engineering-code/. Accessed 29 Apr. 2022.

[5] Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" General Data Protection Regulation (GDPR) Compliance Guidelines, GDPR.EU, 7 Nov. 2018, gdpr.eu/what-is-gdpr/. Accessed 29 Apr. 2022.

[6] Centers for Disease Control and Prevention. "Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Centers for Disease Control and Prevention, 14 Sept. 2018, www.cdc.gov/phlp/publications/topic/hipaa.html. Accessed 29 Apr. 2022.

[7] Halamka, John et al. "The security implications of VeriChip cloning." Journal of the American Medical Informatics Association : JAMIA vol. 13,6 (2006): 601-7. doi:10.1197/jamia.M2143 Zhanel Tucker and Chutima Boonthum-Denecke. "Security, privacy, and ethical concerns on human radio-frequency identification (RFID) implants: poster." In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19). Association for Computing Machinery, New York, NY, USA, 2019. 322–323.

[8] UKEssays. (November 2018). Differences Between Deontology And Act Utilitarianism Philosophy Essay. Retrieved from https://www.ukessays.com/essays/philosophy/differences-between-deontology-and-act-utilitarianism-philosophy-essay.php?vref=1

[9] Tech Spirited (September 2019). RFID Chips in Humans. Informational Website. Retrieved from https://techspirited.com/rfid-chip-in-humans

[10] Driver, Julia. "The History of Utilitarianism." *Stanford Encyclopedia of Philosophy*, Stanford University, 22 Sept. 2014, https://plato.stanford.edu/entries/utilitarianism-history/.

[11] The Privacy Act of 1974 5 U.S.C. § 552a, the United States Department of Justice https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

[12] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021) (February 11, 2021). (2021) 169 Privacy Laws & Business International Report. 6-19, Available at SSRN: https://ssrn.com/abstract=3836261 or http://dx.doi.org/10.2139/ssrn.3836261