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. The use of these implants without proper insurance of their safety for users could lead to massive amounts of data security flaws. This study will address the ethical concerns surrounding the use of these devices and propose scenarios in which the risk for individuals who use these devices will be decreased.**

Keywords*— *RFID, tag, implant, microchip, ethics, SECEPP, utilitarianism

I. Introduction

RFID Tag Implants is a new twist on the already widely used RFID technology. RFID stands for radio frequency identification device and is commonly used in inventory tracking, employee tracking, and supply chain visibility. A 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 the 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 be used to find missing persons or even 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.

Radio-frequency identification technology is not new, it was first developed in the mid-20th century and allows for an automatic and passive identification within a certain close range. 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 get the personal data of the individual. The tag itself can be very small and requires no battery or 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 stable while 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 many use cases for such devices: instant payment at businesses, verification for public transit, concert tickets, parking meter payments, medical history and others. We also 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.

III. Ethical Analysis

To evaluate the ethical concerns of this topic, we will utilize the following ethical theories and models to address concerns they may raise.

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. Companies are also 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 (1.03, 3.12) as well as disclose to users potential dangers to the software towards users (1.04). Under rigorous industry-standard social contracts and laws such as the EU's GDPR and the US HIPAA 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. Under these policies, 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. Rule deontology is a duty-based ethical theory where each individual's morality is based on the obligations that each person has to each 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 on 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. 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 is always in consideration them ethically in the eyes of deontology this works.

C. Analysis Method #3: Utilitarianism

There is another way that we can analyze the same matter above, which is from the perspective of act utilitarianism and rule utilitarianism. When we apply the model of act utilitarianism, there are a lot of things that need to be done to make RFID tag implant ethically acceptable. First of all, companies need to make sure the data they are collecting is safe and sound. To accomplish this goal, I would suggest that companies should collect data from users without a pattern. In that way, those who intend to attack the connection between the users and companies would not know which device is going to upload 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 if they have an STD etc. 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 cause 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 less 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. 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.

IV. Recommendations

In regards to security measures, we would 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. 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.

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 individuals RFID tag without the written consent of said individual. We believe that adhering to this policy is important for upholding an individual's right to privacy.

V. Conclusion

In regards to security measures, we would 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. 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.

References

[1] Werber, Borut, Baggia, Alenka and Žnidaršič, Anja. "Factors Affecting the Intentions to Use RFID Subcutaneous Microchip Implants for Healthcare Purposes" Organizacija, vol.51, no.2, 2018, pp.121-133

[2] 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.

[3] Shafeie, Shekufeh, et al. "Modeling Subcutaneous Microchip Implant Acceptance in the General Population: A Cross-Sectional Survey about Concerns and Expectations." MDPI, Multidisciplinary Digital Publishing Institute, 7 Mar. 2022.

[4] University of Wollongong Research Online - Ro.uow.edu.au.

[5] Teh, Cheryl "A Swedish company has created a microchip that allows users to carry their COVID vaccine passport under their skin." Insider, Dec 23, 2021.

[6] P. Rotter, "A Framework for Assessing RFID System Security and Privacy Risks," in IEEE Pervasive Computing, vol. 7, no. 2, pp. 70-77, April-June 2008, doi: 10.1109/MPRV.2008.22.

[7] P. Rotter, B. Daskala and R. Compano, "RFID implants: Opportunities and and challenges for identifying people," in IEEE Technology and Society Magazine, vol. 27, no. 2, pp. 24-32, Summer 2008, doi: 10.1109/MTS.2008.924862.

[8] Driver, Julia. "The History of Utilitarianism." Stanford Encyclopedia of Philosophy. Stanford University, September 22, 2014.

[9] Alexander, Larry, and Michael Moore. "Deontological Ethics." Stanford Encyclopedia of Philosophy. Stanford University, October 30, 2020.

[10] 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