



Volume 65
Issue 6 V.65, *Tolle Lege*


Article 3

2-3-2021

As Society Strives for Reduced Contact During the Pandemic, How Can Human Microchipping Help?

Nanci K. Carr

Follow this and additional works at: <https://digitalcommons.law.villanova.edu/vlr>

 Part of the [Labor and Employment Law Commons](#), [Law and Society Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Nanci K. Carr, *As Society Strives for Reduced Contact During the Pandemic, How Can Human Microchipping Help?*, 65 Vill. L. Rev. 46 (2021).

Available at: <https://digitalcommons.law.villanova.edu/vlr/vol65/iss6/3>

This Article is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.

AS SOCIETY STRIVES FOR REDUCED CONTACT DURING THE
PANDEMIC, HOW CAN HUMAN MICROCHIPPING HELP?

NANCI K. CARR, J.D.*

ABSTRACT

As the world continues to fight the spread of the novel coronavirus, we look for new ways to reduce contact. Delivery services leave groceries and packages on the porch without waiting for someone to answer the door. Drive-thru windows at fast food restaurants put scanning machines outside the window or pass credit cards and food to customers on a tray, rather than hand-to-hand. What if we did not need to show a credit card? Or at work, what if we could eliminate germ-covered keys and identity badges? Radio frequency identification chips can be embedded under a human's skin and permit them to unlock doors without keys or key cards, and could eventually replace the need to carry identity, credit and debit cards, or cash. This Article considers the implications of incorporating this cutting-edge technology into the workplace as well as our daily lives, balancing the benefits with the privacy, safety, and legal issues.

* Nanci K. Carr is an Assistant Professor of Business Law and the Carande Family Faculty Fellow at California State University, Northridge (CSUN). J.D., *cum laude*, Southwestern Law School; B.S., Business Administration, Ball State University. Thanks to research assistant Harrison Handel, CSUN class of 2019.

CONTENTS

INTRODUCTION	48
I. BACKGROUND RFID: WHAT IS IT?.....	48
II. RFID IMPLANTS IN HUMANS	49
III. HUMAN IMPLANTS IN THE WORKPLACE.....	50
IV. MICROCHIP IMPLANTS IN EVERYDAY LIFE.....	52
V. IMPLANTS IN THE HEALTH INDUSTRY	52
VI. PRIVACY, HEALTH/SAFETY, AND LEGAL ISSUES.....	53
A. <i>Security and Privacy</i>	53
B. <i>Potential Solutions to Security Issues</i>	55
C. <i>Health and Safety Risks of Implants</i>	55
D. <i>Legal Issues Related to RFID Implants</i>	58
VII. OVERALL BENEFITS V. RISKS.....	58
A. <i>Benefits</i>	58
B. <i>Risks</i>	59
CONCLUSION.....	60

INTRODUCTION

RADIO frequency identification (RFID) was invented, like many modern miracles before it, out of necessity. The British Air Force developed the technology during World War II to identify friendly versus enemy aircraft.¹ Since then, RFID has grown to become a part of our everyday lives, being used in hundreds if not thousands of applications without many even realizing it. It provides patrons access to ski lifts, promotes anti-theft measures for store merchandise, aids in collecting toll fees without requiring vehicles to stop, provides keyless access to vehicles, facilitates entry to secured buildings, aids shelters in identifying lost animals, and forms the backbone of supply chain management.²

RFID, an invisible lock-and-key mechanism responsible for helping our lives run more efficiently, is now being surgically implanted into our bodies to do the same.³ People across the globe, including the United States, England, and Sweden, are getting microchipped—the classic fusion of man and machine—in an effort to simplify their lives.⁴ This Article begins by giving a brief explanation of exactly what RFID is and how it is being used today. It then covers how the chip was incorporated into the body as an implantable device and the benefits it provides to various aspects of life—workplace, healthcare, and personal. Moving forward, this Article examines the security issues, health and safety risks, and legal matters that must be given consideration.

I. BACKGROUND RFID: WHAT IS IT?

In order to understand the implications of fusing this technology with the human body, a review of the history of RFID is helpful. “RFID is a term coined for short-range radio technology used to communicate mainly digital information between a stationary location and a movable object or between movable objects.”⁵ It uses a combination of transponders (tags) and interrogators (readers) to digitally communicate information for identification and tracking purposes. The tag has a microchip with stored data along with a radio antenna to transmit information and can be classified as either active or passive.⁶ Active tags are so called because they actively run from their own power source to broadcast signals to the reader—similar to a cell phone communicating with a base station.⁷ Passive tags, on the other hand,

1. See Jeremy Landt, *The History of RFID*, IEEE POTENTIALS, Oct.–Nov. 2005, at 8, 9.

2. *Id.* at 8–10.

3. See Andrew Keshner, *States are Working to Ensure Your Employer Can't Force You to Wear a Microchip*, N.Y. POST (Feb. 4, 2020, 12:58 PM), <https://nypost.com/2020/02/04/states-are-working-to-ensure-your-employer-cant-force-you-to-wear-a-microchip/> [<https://perma.cc/M9U9-2RNF>]; Vivienne Walt, *Is 'Biochipping' a Good Idea?*, FORTUNE (Jan. 8, 2019, 6:30 AM), <http://fortune.com/longform/biochipping-biohax-microchip/> [<https://perma.cc/8JBS-9SHT>]. The Food and Drug Administration approved implantable chips for humans in 2004. See Walt, *supra*.

4. See Walt, *supra* note 3.

5. Landt, *supra* note 1, at 8.

6. See *id.*; see also *Frequently Asked Questions: What's the Difference Between Passive and Active Tags?*, RFID J. [hereinafter *Frequently Asked Questions*], <https://www.rfidjournal.com/faq/whats-the-difference-between-passive-and-active-tags> [<https://perma.cc/6A29-PBFZ>] (last visited July 26, 2020).

7. *Frequently Asked Questions*, *supra* note 6.

are powered by electromagnetic waves sent by the reader that stimulate a current in the tag's antenna to transmit information.⁸ A reader then uses one or more antennas, which emit radio waves to communicate directly with the tag, to retrieve the information and convert it into data on a computer system.⁹

The beauty of using RFID technology is that it has a wide proximity for operation due to the radio waves produced by the antennas from the tag and reader; high frequency devices can function as far as twenty feet away.¹⁰ Unlike barcode systems, which need a line of sight reading in order to work, RFID allows the user the benefit of automation through communication by these waves. The microchips used in the tags also permit a greater array of data to be transmitted than what could be contained in a barcode.¹¹ These benefits are fueling the growth of RFID technology.

II. RFID IMPLANTS IN HUMANS

Employees may wear badges to track their location in the workplace,¹² but RFID technology is now expanding its horizons to functioning as an implantable device to autonomously aid in everyday life. Kevin Warwick, Emeritus Professor at Coventry and Reading Universities in the United Kingdom, became the first person to don an implanted microchip, earning him the moniker "Captain Cyborg."¹³ In 2002, he and a team of medical professionals conducted experiments where he autonomously controlled an electric wheel chair and an intelligent artificial hand using a neural interface.¹⁴

Another early pioneer for RFID implants was VeriMed,¹⁵ which developed the first FDA-approved human implant called the VeriChip.¹⁶ It developed the first and only FDA-approved implant designed to aid emergency personnel in identifying patients as well as accessing personal health information to better facilitate treatment,¹⁷ but the company may have been a bit ahead of its time. Just three short years after

8. *Id.*

9. Bob Violino, *What is RFID*, RFID J. (Jan. 16, 2005), <https://www.rfidjournal.com/what-is-rfid> [<https://perma.cc/T24J-EA32>].

10. *RFID Technology and its Applications*, ELECS. HUB (Aug. 16, 2015), <https://www.electronicshub.org/rfid-technology-and-its-applications> [<https://perma.cc/LYT2-8WZ7>].

11. *Id.*

12. Nicole Lyn Pesce, *5 Ways Your Employer is Tracking You*, MKT. WATCH (July 25, 2017, 11:21 AM), <https://www.marketwatch.com/story/5-ways-your-employer-is-tracking-you-2017-07-25-11882132> [<https://perma.cc/W3QY-ELDU>] (noting nurses at University of California-San Francisco Medical Center and Wyckoff Hospital in Brooklyn wear such tracking badges).

13. Emma Byrne, *Innovation Isn't Safe: The Future According to Kevin Warwick*, FORBES (Sept. 30, 2013, 11:56 AM), <https://www.forbes.com/sites/netapp/2013/09/30/kevin-warwick-captain-cyborg/#58b187835607> [<https://perma.cc/9ZCE-7XSA>].

14. Kevin Warwick, *Project Cyborg 2.0: The Next Step Toward True Cyborgs?*, KEVINWARWICK.COM, <http://www.kevinwarwick.com/project-cyborg-2-0/> [<https://perma.cc/KS8Z-78WJ>] (last visited July 26, 2020).

15. *See, e.g.*, VeriMed Health Group Homepage, <https://verimedhealthgroup.com> [<https://perma.cc/CXS9-8QSD>] (last visited July 26, 2020).

16. *See* David Prutchi, *Veri-Med's Human-Implantable VeriChip Patient RFID*, IMPLANTABLE-DEVICE.COM (Dec. 30, 2011), <http://www.implantable-device.com/2011/12/30/verimedshuman-implantable-verichip-patient-rfid/> [<https://perma.cc/N4H7-HJPPX>].

17. *Id.*

FDA approval of its VeriChip, the company closed the division due to poor public acceptance of microchip implants as well as “a potential link between RFID transponders and cancer in lab animals.”¹⁸

III. HUMAN IMPLANTS IN THE WORKPLACE

Human microchipping, however, made a comeback in 2017 when a company by the name of Three Square Market offered employees, “the chance to toss their employee ID card and chuck all their passwords.”¹⁹ More than fifty of the company’s eighty employees voluntarily agreed to have the grain of rice sized chip imbedded into their hand between the thumb and forefinger.²⁰ The device allows employees access through the secured entrance to the building, unlocks their computers, and even pays for snacks through the brand’s proprietary self-checkout software—“all with the wave of their hand on a sensor.”²¹ The implant is responsible for eliminating the need for ID badges, secured computer passwords, and credit cards.²² A year after the first fifty employees were implanted, they reported reliance on the chips and another thirty employees volunteered for chip implants.²³ One employee commented that he uses the chip ten to fifteen times a day, from starting his computer to using the vending machine.²⁴

Today, Three Square Market has expanded and launched an entirely new division called Three Square Chip, which is responsible for “developing the next generation of commercial microchip implants.”²⁵ Partnering with cardiologist Michael Mirro, the company aims to develop implants for healthcare, workplace security, law enforcement, and for making everyday life that much more convenient.²⁶ While the first in the United States, Three Square Market is still late to the chipping party; BioHax International, located in Sweden, began placing implants in the workers of local start-up Epicenter back in 2015.²⁷ Today it is estimated there are over 3500

18. Haley Weiss, *Why You’re Probably Getting a Microchip Implant Someday*, ATLANTIC (Sept. 21, 2018), <https://www.theatlantic.com/technology/archive/2018/09/how-i-learned-to-stop-worrying-and-love-the-microchip/570946/> [https://perma.cc/TNP4-ZPSM].

19. See Trent Gillies, *Why Most of Three Square Market’s Employees Jumped at the Chance to Wear a Microchip*, CNBC, <https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html> [https://perma.cc/T4MG-VKGB] (last updated Aug. 13, 2017, 9:00 AM).

20. *Id.* (discussing employee reaction to being “chipped”); Pesce, *supra* note 12 (noting more than fifty employees opted in).

21. Gillies, *supra* note 19.

22. *Id.*

23. Rachel Metz, *This Company Embeds Microchips in Its Employees, and They Love It*, MIT TECH REV. (Aug. 17, 2018), <https://www.technologyreview.com/2018/08/17/140994/this-company-embeds-microchips-in-its-employees-and-they-love-it/> [https://perma.cc/SY3Q-QF5V].

24. *See id.*

25. Weiss, *supra* note 18.

26. *Id.*

27. Associated Press, *Companies Start Implanting Chips Into Workers’ Bodies*, L.A. TIMES (Apr. 3, 2017, 10:15 AM), <https://www.latimes.com/business/technology/la-fi-tn-microchip-employees-20170403-story.html> [permalink unavailable].

Swedes using their implants to improve their everyday life.²⁸ From keyless entry into their homes or workplaces, access to the local gym, and even their train pass for daily transportation, the implants have been praised for making their wearers lives more convenient.²⁹

The chips benefit not only the employees but also the employers. Employers have the right to monitor productivity and performance, often by the use of video surveillance or other technology.³⁰ Some office equipment has built in sensors to monitor mouse clicks and keystrokes.³¹ Companies can track the use and location of company-issued cell phones with GPS, ensuring, for example, that delivery workers are where they are supposed to be. However, that monitoring may extend beyond work hours, often without the employee realizing it.³² There are few laws that regulate employers' electronic tracking of employees.³³ The RFID chips present another opportunity for such monitoring, but employers need to be aware that continuously tracking an employee, even after hours, may violate that employee's privacy. To protect both employers from liability and employees' privacy, the employee needs to have some control over the chip so that it can be disabled after hours, and the employer should provide training to the employee regarding such control.

In a unionized workplace, requiring RFID chips, and using them to gather data about employees, could violate a collective bargaining agreement (CBA) if issues of employee privacy have been negotiated in that agreement. Violating the agreement, or mishandling the data collected, could give rise to a charge of unfair labor practices.³⁴

Under the Fair Labor Standards Act (FLSA), employees must be compensated for "donning and doffing"—time spent changing into and out of clothes such as a uniform or safety gear required for the job—unless such compensation is prohibited by a CBA.³⁵ If employees can successfully argue that required RFID chips are "clothes," employers may need to pay employees for the time spent during the implantation procedure.³⁶ Another consideration is whether the Occupational Safety

28. *All Things Considered, Thousands of Swedes Are Inserting Microchips Under Their Skin*, NPR (Oct. 22, 2018, 10:48 AM), <https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin> [<https://perma.cc/8JGX-V3XW>].

29. *Id.*

30. See Pesce, *supra* note 12 ("The average American is caught on surveillance camera more than 75 times a day.")

31. *Id.*

32. See *id.* (noting that "62% of companies with employees working out in the field were using GPS to track the staff.")

33. See Jitendra M. Mishra & Suzanne M. Crampton, *Employee Monitoring: Privacy in the Workplace?*, S.A.M. ADVANCED MGMT. J., Summer 1998, at 4, 4–5.

34. GARRY G. MATHIASON ET AL., LITLER ON LEGAL COMPLIANCE SOLUTIONS FOR THE TRANSFORMATION OF THE WORKPLACE THROUGH ROBOTICS, ARTIFICIAL INTELLIGENCE, AND AUTOMATION 37–40 (2017).

35. See *Perez v. Mountaire Farms, Inc.*, 650 F.3d 350, 367 (4th Cir. 2011) (concluding "donning and doffing" was "integral and indispensable" to chicken processing and therefore compensable); *Mitchell v. JCG Indus.*, 929 F. Supp. 2d 827, 839 (N.D. Ill. 2013) (employer need not compensate employees for time spent "donning and doffing" if that activity is excluded from compensable time by bona fide CBA); Hilary M. Goldberg & Nanci K. Carr, *When Does Compensation for 'Time Spent Under the Employer's Control' Include Pre And Post Shift Waiting and Other Activities?*, 6 S. J. BUS. & ETHICS 33, 40 (2014).

36. MATHIASON ET AL., *supra* note 34, at 27.

and Health Administration (OSHA) safety standards will apply to such chips. While OSHA prescribes safety measures for operating machinery, an embedded chip would not fall under such measures.

IV. MICROCHIP IMPLANTS IN EVERYDAY LIFE

So what can these chips really do? For the everyday person, the RFID implant can be used to make one's life easier. How often are lost keys the culprit to one being late to work or locked out of a home? What about being denied admittance to a train because the wallet or purse containing cash or a train pass was misplaced? RFID chips can act as a digital wallet; they can act as an encryption for personal computer or home office; they can store contact information for business contacts; they can unlock or start a vehicle; and they can even replace the need for house keys by acting as a security device when entering a home.³⁷ RFID implants solve these issues and more.³⁸ Particularly during the pandemic when businesses and individuals are trying to reduce physical contact, an embedded chip could be just the answer.

V. IMPLANTS IN THE HEALTH INDUSTRY

The applications of RFID grow further, however, for the health industry. Incorporating technology into the human body is not new and, if anything, is commonplace today. Whereas in years past getting a pacemaker was a big ordeal, today it is a routine operation someone can undergo when the need arises. Cochlear implants are now being used to give the hearing impaired the chance to hear for the first time.³⁹ Adding an RFID implant may be just as common as these procedures in the near future. "RFID has the potential to save organizations time and money by providing real-time traceability, identification, communication, temperature, and location data for people and resources."⁴⁰ For instance, this technology could make a huge impact on aiding in the tracking and care of Alzheimer patients⁴¹ or contact tracing of those exposed to the coronavirus. The chip would provide the means to grant or deny entrance and exit to the facility, hold each patient's medical records, and even keep record of their vitals.⁴² Not to mention, having the ability to store one's medical records on a tag could mean the difference between life and death for those with severe allergic reactions.⁴³

37. See *All Things Considered*, *supra* note 28 (discussing individual who uses RFID to share LinkedIn details); Weiss, *supra* note 18.

38. Weiss, *supra* note 18 (highlighting prevalence of RFID technology in areas beyond implantable chips).

39. *Cochlear Implants*, NAT'L INST. ON DEAFNESS & OTHER COMM. DISORDERS, <https://www.nidcd.nih.gov/health/cochlear-implants> [<https://perma.cc/EU6A-9FWR>] (last visited July 26, 2020).

40. Charlotte Seckman et al., *The Benefits and Barriers to RFID Technology in Healthcare*, ONLINE J. NURSING INFORMATICS (June 26, 2017), <https://www.himss.org/resources/benefits-and-barriers-rfid-technology-healthcare> [<https://perma.cc/H4XL-XKVE>].

41. See *id.*

42. See *id.*

43. See Associated Press, *FDA Approves Computer Chip for Humans*, NBC NEWS (Oct. 13, 2004), http://www.nbcnews.com/id/6237364/ns/health-health_care/t/fda-approves-computer-

VI. PRIVACY, HEALTH/SAFETY, AND LEGAL ISSUES

While getting an implant may sound like the answer many people have been searching for, we need to first address the risks to security and privacy, the health and safety concerns with getting an implant, and legal issues that could arise with its implementation. Each of these aspects relates to the other, as privacy and health risks can spur legal recourse.

A. *Security and Privacy*

If an embedded chip simply opens a device, like unlocking a door, the privacy risk is low because there is no data created or stored on the chip. However, if the chip does more than that, like storing employment or health information, then a security risk is created. Courts have often tackled issues surrounding an employee's expectation of privacy, finding that it does not exist in work spaces shared by other employees or the public, but that employees do have an expectation of privacy in restrooms and changing areas.⁴⁴ However, the privacy risks related to embedded chips are a bit different.⁴⁵ As with many devices that store sensitive data, RFID implants are subject to security risks, which fall in to five categories:

- Eavesdropping: The act of setting up an additional reader to record tag data.
- Unauthori[z]ed Tag Cloning: Copying tag data onto an additional tag to gain the same privileges.
- Man-in-the-Middle (MIM) Attack: When an external object pretends to be either a tag or reader between actual tags and readers.
- Unauthori[z]ed Tag Disabling: When an external reader disables a tag not allowing it to be utili[z]ed again.
- Unauthori[z]ed Tag Manipulation: Manipulating the tag data using an external reader.⁴⁶

The European Parliament released a study in 2018 on the security issues surrounding the implantation of RFID chips in workers, including Intrusion Detection, defined as “the discovery of foreign attacks upon the system usually utili[z]ing the

chip-humans/#.XMenzuhKjIU [https://perma.cc/YL7R-8HU5] (noting ability of chips to reduce paperwork and speed up treatment time).

44. See, e.g., *Doe by Doe v. B.P.S. Guard Servs., Inc.*, 945 F.2d 1422, 1427 (8th Cir. 1991) (finding models' privacy was violated when they were secretly viewed and videotaped while changing clothes behind curtained area at fashion show); *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1110 (C.D. Cal. 2006) (recognizing employees have reasonable expectation of privacy while using locker room in basement of police station and police department employer violates that privacy by secretly videotaping them as they undress).

45. For further discussion of employee monitoring issues, see *supra* Part III.

46. Peter Darcy et al., *The Challenges and Issues Facing the Deployment of RFID Technology*, in *DEPLOYING RFID—CHALLENGES, SOLUTIONS, AND OPEN ISSUES* 10–11 (Cristina Turcu ed., 2011).

tags that hinder the overall integrity of the data.”⁴⁷ The study listed the following additional security concerns raised by RFID:

- Further Eavesdropping: An intruder reader intercepts the signals between the chip and the legitimate reader.
- Traffic Analysis: The existence and location of a chip is monitored, without necessarily interrogating the chip.
- Spoofing: Also known as satiri[z]ing, where another device is used to simulate a genuine chip.
- Denial of service attack: Chips can be adulterated to disable them.⁴⁸

The key element tying all of these risks together is that the information stored on RFID chips is subject to potential attack. One journalist detailed how a hacker and a human guinea pig proved RFID chip implants could be hacked.⁴⁹ Hacker Jonathan Westhues teamed up with his human guinea pig, Annalee Newitz, at a Hackers on Planet Earth conference held in New York to show off his hacking skills by cloning a VeriChip RFID chip that was implanted in Newitz’s arm.⁵⁰ Westhues used an RFID reader and a homemade antenna connected to his laptop to clone Newitz’s unique VeriChip ID.⁵¹

This is not the first time the pair has worked together, either. On another occasion, Newitz explained how Westhues used a homemade cloner to copy access code information from an RFID-type smart badge.⁵² After quickly downloading the data from the reader, Westhues used the cloned badge to unlock the door of a secured building and gain entrance.⁵³ An important takeaway is that Westhues only needed to bump into the gentleman whose badge ID he intended to clone to steal the information with his homemade device. Hacking the device was not only trivial for him, but enjoyable.⁵⁴

While both of these instances are quite scary in terms of how easily RFID technology could be hacked, these articles were written back in 2006. Since then, not only has VeriChip gone out of business, but the technology has had time to improve. Even though would-be hackers can purchase RFID cloning kits for under \$20, it has

47. *Id.* at 10 (defining RFID security as “Intrusion Detection”); Richard Graveling et al., Directorate-General for Internal Policies, *The Use of Chip Implants for Workers*, 35–36, IP/A/EMPL/2017-12 [hereinafter *The Use of Chip Implants for Workers*] (Jan. 2018), [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU\(2018\)614209_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU(2018)614209_EN.pdf) [<https://perma.cc/R42T-MZVB>].

48. *The Use of Chip Implants for Workers*, *supra* note 47, at 35.

49. Donald Melanson, *VeriChip’s Human-Implantable RFID Chips Clonable, Sez Hackers*, ENGADGET (July 24, 2006), <https://www.engadget.com/2006/07/24/verichips-human-implantable-rfid-chips-clonable-sez-hackers/> [<https://perma.cc/6TQG-TNRW>].

50. *Id.*

51. *Id.*

52. Annalee Newitz, *The RFID Hacking Underground*, WIRED (May 1, 2006, 12:00 PM), <https://www.wired.com/2006/05/rfid-2/> [<https://perma.cc/P6UK-MXF6>].

53. *Id.*

54. *Id.*

not been documented as to whether the newer chips being used for implants have been hacked.⁵⁵

So what does all of this mean? Should an RFID chip wearer have the chip linked to their personal information or bank accounts, a hacker might be able to use one of the aforementioned techniques to acquire the data. Security of implanted chips needs to be taken seriously by manufacturers and chip wearers as the RFID technology breaks further into the workplace and our daily lives.

B. *Potential Solutions to Security Issues*

As the public becomes more engaged with the idea of utilizing the benefits of an implanted RFID device, greater measures must be taken to ensure their security. The author suggests such proposed measures include heightened encryption of the RFID chips, mutual authentication, and implementing personal identification number (PIN) to add an additional layer to security. For instance, Three Square Market promotes security through a heightened encryption method similar to the encryption used to protect a credit card.⁵⁶ The idea is that the encryption will prevent unwanted interrogations on chips. Mutual authentication would also enforce user privacy and protect against tag cloning. Also, using a regularly updated “secret key value” (that seeks to ensure that only authorized readers can access chip information) would increase security and protect against a variety of attacks, much like regularly changing an online password.⁵⁷ Another line of defense would be incorporating a specific PIN to be used when using the chips to access more sensitive information. Much like a credit card pin, which acts as a final form of identification for personal use, the RFID PIN could be implemented to do the same for those with implants.⁵⁸ As RFID implants gain momentum, a combination of each of these methods, as well as others that have not been invented yet, may need to be in place to ensure the chip’s security for chip wearers.

C. *Health and Safety Risks of Implants*

The next question is regarding the health and safety risks involved with getting the implant. The initial procedure for the implant is safe as long as it is performed by an experienced professional body piercer or body modification expert with proper equipment.⁵⁹ However, side effects suffered by breast and dental implant

55. See Slaowmir Jasek, *A 2018 Practical Guide to Hacking NFC/RFID*, SMARTLOCKPICKING.COM 16 (Apr. 6, 2018), https://smartlockpicking.com/slides/Confidence_A_2018_Practical_Guide_To_Hacking_RFID_NFC.pdf [https://perma.cc/6YVP-DHHH].

56. *Microchip Technology and Three Square Market*, 32MARKET.COM (Apr. 1, 2019), <https://32market.com/public/images/QA.pdf> [https://perma.cc/U2XV-S5MK].

57. See *The Use of Chip Implants for Workers*, *supra* note 47, at 30.

58. *Id.*

59. See *X-Series Implantable Transponder FAQ*, DANGEROUS THINGS (May 2016), <https://forum.dangerousthings.com/t/x-series-implantable-transponder-faq/28> [https://perma.cc/4JTX-PZQZ].

patients indicate there are risks of infection and nerve damage at the implant site.⁶⁰ Also, potential long-term health risks associated with the inserted tags are unknown since they are still so new. The four primary areas of medical risk are carcinogenic effects, effects of Magnetic Resonance Imaging (MRI) use for wearers of an RFID, adverse effects from potential migration of the unit, and efficacy issues with pharmaceuticals.⁶¹

The European Parliament acknowledged the potential carcinogenic effects of RFID implants, citing a study that compiled eleven studies performed from 1990 through 2006 into a review of carcinogenesis in laboratory animals caused by RFID chips.⁶² Eight of the eleven studies found cancer forming at the site of the chip, and the percentage of animals to contract cancer ranged from .8% to 10.2%.⁶³ The European Parliament, however, took great note of the fact that many of the studies used a specific strain of mice that was genetically susceptible to carcinoma—and these mice in particular were associated with cancer forming.⁶⁴ The studies also reviewed older RFID technology, which may have affected outcomes.⁶⁵ While the FDA has already cleared chips to be safe for implantation into the human body, there is not enough evidence to prove or disprove the potential for carcinogenesis in humans.⁶⁶

Another area of interest is a possible negative interaction with MRI scanning.⁶⁷ Due to the magnetic forces produced by an MRI, there is a fear the metal contained in the chip could have adverse effects from its exposure.⁶⁸ Potential outcomes include the scan not performing properly in the area where the chip is located, migration of the unit, and the unit potentially being ripped completely out of the body due to the strong magnetic forces—a worst case scenario.⁶⁹ While some of the studies cited did show a greater elevation in heat displacement due to the device, it was ruled that this took place because of the types of RFID chips used in the study.⁷⁰ The chips, in fact, were much larger and quite a bit more powerful than the chips used for human implants. Aside from the additional heat generated, it was also noted that the MRI did not have a clear scan around the area of the implant.⁷¹ This, however, was thought to have been because of the types of chips used.⁷² Overall, the European Union concluded that, “[a]lthough restricted by the lack of specific *in vivo* studies (where objective measurement of factors such as force and temperature

60. *Ten Reasons to Never Get a Microchip*, HAPPYPREPPERS.COM, <https://www.happypreppers.com/chips.html> [<https://perma.cc/3583-8E5V>] (last updated Nov. 26, 2018) (noting twenty-six risks of breast implants and separate risks associated with dental implants, including nerve damage or sinus problems).

61. See *The Use of Chip Implants for Workers*, *supra* note 47, at 30.

62. See *id.*; Katherine Albrecht, *Microchip-Induced Tumors in Laboratory Rodents and Dogs: A Review of the Literature 1990–2006*, 2010 IEEE INT’L SYMP. ON TECH. & SOC’Y 337, 337 (2010).

63. Albrecht, *supra* note 62, at 338.

64. *The Use of Chip Implants for Workers*, *supra* note 47, at 31.

65. *Id.*

66. *Id.* at 32.

67. *Id.* at 32–33.

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.* at 33.

72. See *id.*

would be problematic) the available evidence appears to suggest that any negative impact of an RFID on subsequent MRI scanning of the individual would be minimal.⁷³ In a more recent study, fifty-three subjects with microchips were put through an MRI to test the efficacy of the chips after the magnetic exposure.⁷⁴ The study found that the chips functioned normally for all fifty-three subjects.⁷⁵ Even with this in mind, more research needs to be completed on the matter.

Migrating units is also an issue because the chips could move to an area in which there would be greater difficulty in extracting the chip.⁷⁶ Migration may occur in animals that are exposed to the magnetic force from an MRI.⁷⁷ A remedy was suggested, in a study done by Baker and Macdonald, to allow three months for connective tissue to form around the chip before exposing an animal to an MRI.⁷⁸ The issue remains that studies are sparse to provide conclusive evidence for the potential migration in human subjects. The European Parliament stated that “[t]o date there is no formally collated information or systematic study available to document the extent to which sub-dermal chip migration is possible in humans, or the extent of any migration should it occur, although it seems to be a minimal risk.”⁷⁹

Efficacy of pharmaceuticals used for patients with RFID implants has been a concern. Researchers used the five most common RFID frequencies to subject multiple products to radiation twice that permitted by the Federal Communications Commission.⁸⁰ The products included hormones, vaccines, and immunoglobulins. Researchers tested for purity and potency after continuously subjecting the products to irradiation for twenty-four hours and, “found no detectable deterioration in any product.”⁸¹ Given the evidence from the studies, there is little justification for any concerns regarding contraindication of the use of pharmaceuticals by an implanted chip wearer.⁸²

With all of these factors in mind (carcinogenic effects, MRI interaction, migration, and efficacy of pharmaceuticals), the main correlating factor is that there has not been enough research. Over the years, studies increasingly show RFID implants do not pose a serious threat to their wearers. Even still, hard evidence should be produced to demonstrate the safety of the devices with minimal negative health risks.

73. *Id.*

74. See Katherine A. Haifley & Silke Hecht, *Functionality of Implanted Microchips Following Magnetic Resonance Imaging*, J. AM. VETERINARY MED. ASS'N 577, 578 (Mar. 1, 2012), <https://www.ncbi.nlm.nih.gov/pubmed/22332627> [permalink unavailable].

75. *Id.*

76. *The Use of Chip Implants for Workers*, *supra* note 47, at 33–34.

77. *Id.* at 34.

78. See *id.* at 34 (noting studies indicate chips may take up to three months to “orient” themselves in human body); see also Martin A. Baker & Iain MacDonald, *Evaluation of Magnetic Resonance Safety of Veterinary Radiofrequency Identification Devices*, 52 VET. RADIOLOGY & ULTRASOUND 161, 166 (2011).

79. *The Use of Chip Implants for Workers*, *supra* note 47, at 34.

80. *Id.*

81. *Id.*

82. See *id.*

D. *Legal Issues Related to RFID Implants*

Some argue that an employer requesting that an employee endure an invasive procedure to embed a chip is a violation of basic human rights.⁸³ However, healthcare workers and teachers must provide proof of various vaccinations in order to work, and during the current pandemic, many employees are required to take a COVID-19 test to see if they are infected before reporting to work and to continue working. That test, in particular, must be continually repeated, which is both repeatedly invasive and time-consuming for the employee.

As of 2020, only seven states have outlawed mandatory microchipping for any human.⁸⁴ This law is set in place to protect employee rights and to keep employers from basing acceptance of employment or continued appointment on receiving an implant.⁸⁵ While employers can legally implement the use of chips within the workplace, employees in those states retain the right to refuse the chip and must freely and willingly choose to be implanted.⁸⁶ Because RFID implants are just beginning to “pick up steam,” laws are not in place to protect the rights of wearers. As the number of uses for RFID implants increases, so will the law develop to protect those with an RFID chip.

A few considerations for law involve the removal of employer-sponsored chips after termination or exit from a company, privacy law for unlawful access to employee information due to malicious attack or unauthorized cloning of an RFID device by a third party, as well as for the everyday chip user, unauthorized tracking of chip wearers, and replacement of malfunctioning employer-sponsored chips to name a few. Much of the consideration comes from the security risks that face chip wearers. The fact remains that those utilizing the benefits of having an RFID implant need laws in place to protect their right to privacy.

VII. OVERALL BENEFITS V. RISKS

A. *Benefits*

When it comes to having a RFID chip implanted into one’s body, the only limitation is his or her imagination. Chips allow users to simplify their daily lives through programming the chips to perform specific tasks with the wave of their hand.⁸⁷ In the workplace, chips allow for greater security measures for access to secured areas of the facility, grant secured access to Informational Technology (IT) or computer networks, and allow for quick and effortless purchases at vending

83. See Amit Rahav, *Microchipping Your Employees Will Always Be Dehumanizing—and Pointless*, NEXT WEB (Aug. 17, 2019), <https://thenextweb.com/podium/2019/08/17/microchipping-your-employees-will-always-be-dehumanizing-and-pointless/> [https://perma.cc/77P6-TP6H].

84. See IND. CODE § 22-5-8-2 (2020) (prohibiting employers from requiring implantation of microchips as condition of employment); Keshner, *supra* note 3. Indiana ensures that “[e]mployers cannot condition a job offer on chip insertion and if workers lose their job for allegedly refusing to implant one, the bill lets them sue for damages.” Keshner, *supra* note 3.

85. Keshner, *supra* note 3.

86. *Id.*

87. See Weiss, *supra* note 18.

machines.⁸⁸ In regard to healthcare, chips can store a wearer's personal health history to aid in proper care.⁸⁹ This could come in handy where quick action needs to be taken in life or death situations.⁹⁰ An implant could also be incorporated to allow greater freedom to patients with Alzheimer's or dementia.⁹¹ Chips can be programmed to grant or deny access to certain areas of a building.⁹² This could be helpful in adding an extra layer of security. This same concept translates to the penal system. While the ethics of this would be brought into question, inmates could receive implants to further add to security protection.

For the rest of the public, embracing this new trend of bio-hacking is where the possibilities really grow. Imagine keyless entrance to a home or vehicle, medical information and contacts for emergencies, or programming the chip to turn on the lights in one's home. During the pandemic, countless business have advertised efforts to reduce contact with customers by passing credit cards on trays rather than hand-to-hand. If customers had embedded chips, they could simply swipe their hand—even a gloved hand—across a reader to pay for a purchase. The true capabilities of having an RFID implant are only just beginning to be explored.

B. *Risks*

While all of this this sounds exciting, there are still risks to be explored. A main risk is that of invasion of privacy. Even though companies are utilizing special encryptions to protect the data on the chips, in the author's opinion, there may still be the potential of hacking the system. The potential for RFID hacking would generate security risks at facilities where chips are used for special access, and it would also leave payment information accessible if programmed into the chip. While the FDA has approved chip implants, the full scope of health risks is still unknown as there is not enough data to know the real risks.⁹³ The significant health risk involves the potential for cancer to develop around the chip.⁹⁴ While shown to be a minute chance of developing, there is not enough evidence to fully debunk the carcinogenic risk.⁹⁵ New studies need to be conducted with current technology. Legislation also needs to be tied to implantable RFID chips to protect the rights of workers and people who have opted for the convenience the chip provides.⁹⁶

Another practical concern is updating the chip technology. For most people, a cell phone is already out of date the day it is purchased. There are constant software updates and—at least annually—a hardware update. The same is true for computers and smart watches. With those pieces of equipment, it is an economic decision whether to upgrade as well as a time commitment to make the transition. However, updating embedded chip hardware would require another invasive procedure. How

88. Gillies, *supra* note 19.

89. Seckman et al., *supra* note 40.

90. *Id.*

91. *Id.*

92. *Id.*

93. *See id.* at 31.

94. Albrecht, *supra* note 62, at 348.

95. *See id.* at 345–46. *But see The Use of Chip Implants for Workers*, *supra* note 47, at 32 (finding carcinogenic risk to humans “minimal” despite animal studies).

96. Keshner, *supra* note 3.

many people would be willing to have a surgical procedure on an annual basis to upgrade the hardware? And, who would pay for that procedure? Likely the employer would work with its insurance provider to have the procedure covered by insurance, but either the employee or employer, or a combination of the two, pay those premiums. Those insurance and procedure costs would ultimately be passed on to consumers through increased product and service costs.

CONCLUSION

The Bible may have prophesized implantable chips when it said, “[i]t also forced all people, great and small, rich and poor, free and slave, to receive a mark on their right hands or on their foreheads, so that they could not buy or sell unless they had the mark”⁹⁷ Amal Graafsra, CEO of both a manufacturer and a distributor of implantable chips, has stepped up to acquire that “mark” by embedding four chips in his left hand and two in his right.⁹⁸ While his personal and professional life are dependent on the chips, he understands those who may not be ready. “I’d say you’re acting like regular human who’s skeptical of something they are unaware of. . . . With any technological change, there’s always a ‘this is crazy’ crowd.”⁹⁹

Before the coronavirus pandemic, maybe the number in the “this is crazy” crowd would have far outnumbered people like Graafsra and the Three Square market employees who were willing to receive implanted chips. However, as we adapt to life during a pandemic embedded chips may be one solution to reducing contact that will become part of our new normal.

97. REVELATION 13:16–17 (New International); *see also Ten Reasons to Never Get a Microchip*, *supra* note 60.

98. Keshner, *supra* note 3.

99. *Id.* (internal quotation marks omitted).