Catholic University Journal of Law and Technology

Volume 30
Issue 2 *Spring 2022*

Article 5

2022

The Anomaly That Is Privacy: Data Privacy Concerns Related to the Rise of Microchip Implants in Humans

Kendra Lobban
Catholic University of America (Student)

THE ANOMALY THAT IS PRIVACY: DATA PRIVACY CONCERNS RELATED TO THE RISE OF MICROCHIP IMPLANTS IN HUMANS.

Kendra Lobban[*]

Imagine parking on the street after a long day of work and running through the rain to the front door. While rummaging through a purse in search of the house keys, you remember a neighbor who never worries about losing keys. Instead, she opts for a microchip implant and can unlock the door with a wave of a hand. Not only can she walk through the front door without a drop of rain or scrambling through her purse, but she can walk straight over to the fireplace and light it up, again with the quick wave of a hand. It seems like an easy, convenient way to avoid the situation you currently find yourself in. But you begin to wonder whether the ease of opening the door and turning on your appliances is worth the privacy cost of this technology.

Microchips are already in use in various realms of our everyday lives, such as credit cards, livestock farming, and even household pets for identification

[*] *Juris Doctor* Candidate, Columbus School of Law, 2022; *The Catholic University of America, Journal of Law and Technology*, Managing Editor, 2021-2022; Bachelor of Science in Business Administration – Finance, West Virginia University, *summa cum laude*, 2019. Many thanks to my family and friends for their unwavering support throughout my academic endeavors. My deep gratitude to Professor Megan M. La Belle for her mentorship and assistance with this journey. Lastly, a heartfelt thanks to my mother, Krista Lobban, whose meaningful conversation inspired the exploration of this topic. All that I am, I owe to you.

purposes.[1] Recently, human microchip implantation is increasing in popularity.[2] People worldwide are using the technology to unlock security systems, pay for items, and much more.[3] However, with microchip implementation comes the ability to store information and monitor one's movements each time the microchip is scanned.[4] Moreover, it is unclear where each scan's information is stored, how it is protected, and who can access it.[5]

As with any new technological advancement, the microchip ironically chips away at our ability to maintain privacy in our everyday lives.[6] Consider the data privacy implications arising out of developments such as smartphones, wearables, and healthcare applications.[7] Over time, and with each new advancement, comes less security with respect to our personal information.[8] This concern is heightened with microchip implants because they are always with the wearer and cannot be powered off like other devices with similar capabilities.[9] Rather, when a microchip encounters a reader, the chip's information is automatically collected, and the wearer is not provided the option to decline to share at any time.[10]

This article will discuss why microchipping humans is an invasion of privacy with potentially devastating consequences, as data about the person accumulates over time and is accessible with a simple wave of the hand.[11] Furthermore, this article highlights the inadequacy of current laws with regard to safekeeping our data and protecting our privacy rights.[12] Additionally, it identifies the specific areas of potential impact where human microchipping presents unique

---

1 Richard van Hooijdonk, *Human Microchipping, the Benefits and Downsides*, RICHARDVANHOOIJDONK.COM, https://blog.richardvanhooijdonk.com/en/human-microchipping-the-benefits-and-downsides/ (last visited Mar. 20, 2022).

2 Jessica Malekos Smith, *Fear, Uncertainty, and Doubts About Human Microchips*, CTR. FOR STRATEGIC & INT'L STUD. (June 23, 2020), https://www.csis.org/blogs/technology-policy-blog/fear-uncertainty-and-doubt-about-human-microchips.

3 *Id.*

4 *Id.*

5 *Id.*

6 van Hooijdonk, *supra* note 1.

7 Katherine Britton, *IoT Big Data: Consumer Wearables, Data Privacy and Security*, AM. BAR ASS'N (Nov./Dec. 2015), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/.

8 *Id.*

9 Smith, *supra* note 2.

10 *Id.*

11 *Id.*

12 Charles Smith, *Human Microchip Implantation*, 3 J. TECH. MGMT. INNOVATION 151, 154–55 (2008); *see generally Data Privacy*, EMOTIV, https://www.emotiv.com/glossary/data-privacy/ (last visited Mar. 28, 2022) (explaining the federal laws in the European Union protecting citizens).

concerns.[13]

I. MICROCHIP TECHNOLOGY 'CHIPPING' AWAY AT PERSONAL PRIVACY

A microchip is an implantable radio frequency identification device (RFID) or transponder, about the size of a grain of rice, typically inserted under the skin between the thumb and index finger of humans.[14] The RFID microchip works like a two-way radio; when a digital reader is placed nearby, the microchip communicates with the reader's magnetic field to transmit identity information.[15] These chips are most commonly used to replace keys and passwords.[16] Prior to human implantation, RFID transponders were used in asset tracking to locate merchandise and keep tabs on storage in warehouses.[17] Alternatively, some implants are near field communication chips (NFC), which use electromagnetic radio fields to communicate with readers.[18] This type of microchip technology is already used for mobile payments and virtual credit cards.[19] Both forms of technology operate similarly and present the same ethical concerns with regard to data privacy.[20]

RFID technology is classified as either passive or active depending on the device's power source type.[21] The microchip implant used in humans is considered a passive device.[22] Once scanned, it "allows a small computer chip with no battery or power source to be powered by and communicate with compatible readers using the magnetic field the reader generates" to transmit information to the reader.[23] While readers can be mobile or stationary, one must be placed within 15-20 feet of the passive RFID chip to receive information.[24] Other RFIDs are active devices, meaning they are powered by an internal transponder and can receive, as well as send, information when scanned.[25] Because these devices contain their own power source, they can be scanned from

---

13 van Hooijdonk, *supra* note 1.
14 *Id*.
15 Smith, *supra* note 2.
16 Yael Grauer, *A Practical Guide to Microchip Implants*, ARS TECHNICA (Jan. 3, 2018), https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/.
17 Lindsey O'Brien, *Are NFC Technology in Microchip Implants and RFID Asset Tracking the Same?*, E2B CALIBRATION (Apr. 5, 2017), https://e2bcal.com/nfc-microchip-rfid-asset-tracking/.
18 Smith, *supra* note 2.
19 Grauer, *supra* note 16.
20 *Id.*
21 O'Brien, *supra* note 17.
22 Smith, *supra* note 2.
23 *Id.*
24 O'Brien, *supra* note 17.
25 *Id.*

a broader range and share a larger volume of data.[26]

Currently, between 50,000 and 100,000 people across the globe have microchip implants.[27] Once inserted, the microchip has a variety of capabilities that enhance everyday convenience.[28] It works similar to the microchips in our credit cards, but with a broader range of capabilities than merely financial transactions, such as the ability to access public transportation and breeze through security checkpoints.[29] Furthermore, the microchip allows for a method of easy identification with the scan of the hand, rather than carrying a driver's license, passport, or other identification documents in your wallet.[30] Its use is also readily apparent in the medical industry, as the microchip can store medical records and continually monitor health status to detect potential issues.[31] Among the many conveniences that come with installing a microchip is the ability to link all your technology devices to operate by microchip scan, for example, unlocking your home's security system and powering your appliances.[32] Connecting device operation directly to the microchip allows control over the technology and limits use to persons with the required microchip pairing.[33]

Human microchipping is only beginning to gain traction in the United States. In 2004, the Federal Food and Drug Administration approved the first human microchip, developed by VeriChip Corporation, for use in the medical industry to access patient identification and medical records.[34] However, by 2010, the company stopped marketing microchip implants after sales proved inadequate and privacy concerns from the public arose.[35] Nevertheless, in 2017 the microchip reemerged in the employment sector when Three Square Market, a technology company in Wisconsin, became the first United States employer to use human implants.[36] The company explained in a press release that

---

26 Samuel E. Simpson, *Microchipping Employees and Privacy Implications - Does My Boss Know Where I Am Right Now?*, 20 MARQ. BENEFITS & SOC. WELFARE L. REV. 279, 282 (2019).

27 Smith, *supra* note 2.

28 van Hooijdonk, *supra* note 1.

29 *Id.*

30 *Id.*

31 *Id.*

32 *Id.*

33 *Id.*

34 *FDA Approves First Implantable Identification Chip for Medical Use*, CAL. HEALTHLINE (Oct. 14, 2004), https://californiahealthline.org/morning-breakout/fda-approves-first-implantable-identification-chip-for-medical-use/.

35 Jim Edwards, *Down with the Chip: PositiveID Axes Its Scary Medical Records Implant*, CBS NEWS (Sept. 17, 2010), https://www.cbsnews.com/news/down-with-the-chip-positiveid-axes-its-scary-medical-records-implant/.

36 Andrew Keshner, *States Are Cracking Down on Companies Microchipping Their Employees – How Common Is It?*, MKT.WATCH (Feb. 4, 2020),

"[e]mployees will be implanted with a RFID chip allowing them to make purchases in their break room micro market, open doors, login to computers, use the copy machine, etc."[37] What became known as the company's "chip party" facilitated the microchipping of nearly 100 employees.[38] Initially, the RFID chip did not have GSP tracking capabilities.[39] However, the company has indicated a desire to use new innovative technology for "a more sophisticated microchip that is powered by human body heat and includes GPS tracking capabilities and voice activation."[40] Moreover, the microchip may ultimately replace the traditional ID badge with features to enhance building security and simplify computer log-ins.[41] Today, the workplace remains the most common arena for human microchipping in the United States.[42]

Internationally, however, human microchip use is widespread.[43] For example, in technologically advanced Sweden, over 4,000 people are microchipped, and it is currently the country with the most use of RFID implants.[44] The Swedish citizens with microchips use them to access their homes and workplace, and for membership purposes at clubs or activities.[45] Additionally, they use the microchip to store emergency contact information in the event of a situation where the person is unable to communicate.[46] Importantly, data protection in countries within the European Union, like Sweden, is regulated by the General Data Protection Regulations (the "GDPR").[47] The GDPR provides privacy rights and protections by allowing citizens to preserve control over their data and who interferes with it.[48] It is known as the most protective data privacy law and serves

---

https://www.marketwatch.com/story/states-are-cracking-down-on-companies-microchipping-their-employees-how-common-is-it-and-why-does-it-happen-2020-02-03.

37 *Company to Become First in U.S. to Microchip Employees*, WVLT (Oct. 31, 2019), https://www.wvlt.tv/content/news/Company-to-become-first-in-the-US-to-microchip-employees-564202811.html.

38 Peter Holley, *This Firm Already Microchips Employees. Could Your Ailing Relative Be Next?*, WASH. POST (Aug. 23, 2018), https://www.washingtonpost.com/technology/2018/08/23/this-firm-already-microchips-employees-could-your-ailing-relative-be-next/.

39 *Id.*

40 *Id.*

41 Keshner, *supra* note 36.

42 *Id.*

43 Camille Caldera, *Fact Check: Americans Won't Have Microchips Implanted by End of 2020*, USA TODAY (Aug. 1, 2020), https://www.usatoday.com/story/news/factcheck/2020/08/01/fact-check-americans-will-not-receive-micro
chips-end-2020/5413714002.

44 *Id.*

45 *Id.*

46 *Id.*

47 *Data Privacy*, *supra* note 12.

48 *Data Privacy*, *supra* note 12; *see generally* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with

as the model for current state legislation in the United States.[49] The importance of the GDPR's regulations, giving the control of data to individuals, is readily apparent given the microchip's ability to store mass amounts of information.[50] Therefore, having a federal law that provides extensive protections is a significant distinction between countries in the European Union and the United States.[51]

Although microchip implants open the door for a convenient way to conduct our daily lives, issues arise as with any new technology.[52] Among the risks of human microchipping are the unknown health concerns from the long-term use of such technology.[53] Concerns arise surrounding the possibility of the microchip moving within the body cavity.[54] Additionally, "other risks include electrical hazards, adverse tissue reactions, infections and incompatibility with medical equipment such as MRIs machines."[55] However, given that implanting in humans is relatively new, it is too soon to study all potential health-related issues adequately.[56]

Aside from the medical risks of microchipping, concerns associated with the chips' possible impact on our freedom of choice are relevant.[57] For example, with the growing popularity of microchipping, it may become a requirement to use private and public services like riding public transportation or paying for groceries.[58] Although these concerns may seem farfetched, in reality they are closer than we think.[59] Currently, private businesses can choose their own

---

Regard to the Processing of Personal Data and on the Free Movement of Such Data, and on the Free Movement of Such Data (General Data Protection Regulation), art. 7, 2016 O.J. (L 119) (EU).

49 Maria Korolov, *California Consumer Privacy Act (CCPA): What You Need to Know to Be Compliant*, CSO (July 7, 2020), https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html; Stacey Gray et al., *A New U.S. Model for Privacy? Comparing the Washington Privacy Act to GDPR, CCPA, and More*, FUTURE OF PRIV. REFORM (Feb. 12, 2020), https://fpf.org/blog/a-new-model-for-privacy-in-a-new-era-evaluating-the-washington-privacy-act/.

50 Gray, *supra* note 49; van Hooijdonk, *supra* note 1.

51 Gray, *supra* note 49.

52 van Hooijdonk, *supra* note 1.

53 *Id.*

54 *Id.*

55 *Id.*

56 *Id.*

57 *Id.*

58 Elaine M. Ramesh, *Time Enough – Consequences of Human Microchip Implantation*, 8 RISK: HEALTH, SAFETY, & ENV'T 373, 384 (1997) (discussing the possible uses of microchip technology in the future).

59 *Id.* at 407 (warning readers that this technology was emerging and identifying the risks it poses to society).

procedures regarding payment, so long as there is no state law to the contrary; as such, some stores do not accept cash payments while others require card payments by microchip insertion over the traditional swipe method.[60]

An additional concern emerges due to the microchip's vulnerability to potential corruption.[61] With the chip's ability to hold a variety of personal information comes the possibility that our information could be hacked, manipulated, or even sold.[62] Lastly, and of paramount concern, is the privacy intrusion associated with microchip implants.[63] As previously identified, the microchip can relay various amounts of data on a person beyond what may be contemplated,[64] thus, opening the door to data breaches and unauthorized supervision.[65] Considering these potential risks, the use of microchip technology requires diligent security measures and new privacy laws to ensure personal data is protected.[66]

This article focuses on the privacy issues arising out of the microchip's ability to compile mass amounts of data on a person.[67] Although the microchip is a passive device currently incapable of tracking one's location, it monitors and records every instance where a reader scans the chip.[68] Even without GPS capabilities, the microchip can create a detailed log of a person's activity on any given day.[69] As one commentator has explained, "[w]hile possession of this information from a single instance may not seem intrusive, over time [one can] make inferences and discover patterns in your daily routine that many people would find unsettling."[70]

Responding to this concern, supporters of the microchip assert that the chip itself only contains an identification number, and its inadequate and limited capabilities fail to pose a threat to society.[71] However, the American Civil Liberties Union reminds us that "the [serial] number can actually be used as a

---

60 Samantha Putterman, *Are Businesses Required by Law to Accept Cash? It Depends on Where They Are*, POLITIFACT (July 22, 2020), https://www.politifact.com/factchecks/2020/jul/22/facebook-posts/are-businesses-required-law-accept-cash-depends-wh/.

61 van Hooijdonk, *supra* note 1.

62 *Id.*

63 *Id.*

64 *Id.*

65 Janitra Haryanto, *Do Microchip Possess Threats to Our Privacy and Data Security?*, CTR. FOR DIGITAL SOC'Y (Feb. 27, 2019), https://cfds.fisipol.ugm.ac.id/2019/02/27/do-microchip-possess-threats-to-our-privacy-and-data-security/.

66 van Hooijdonk, *supra* note 1.

67 *Id.*

68 *Id.*

69 *Id.*

70 Simpson, *supra* note 26, at 284–85 (discussing the privacy implications and potential dangers outside the workplace of employer compelled human microchipping).

71 Haryanto, *supra* note 65.

reference number that corresponds to information contained on one or more Internet-connected databases."[72] In other words, the identification number contained in the microchip may be linked to a larger quantity of information within a cloud database.[73]

Part I explored an overview of the development of human microchipping and its current usage in the United States as well as internationally.[74] It identified the advantages and downside of the RFID implants, particularly highlighting the data collection concerns.[75]

Part II of this article discusses the current state of privacy laws in the United States that protect the rights of citizens against these concerns.[76] Specifically, it explores federal data privacy regulations and state privacy laws governing the collection and sale of personal data.[77] It briefly discusses constitutional privacy protections and highlights why they are unable to provide an adequate safeguard for citizens.[78]

Part III describes the private sector's use of implants to store data and identifies specific areas of concern where our current laws will not suffice.[79] Finally, the article asserts that our federal legislature must step up and develop comprehensive laws to protect our data privacy with the technological world advancing so quickly.[80]

II. THE DANGERS OF DATA SHARING: WHAT COMPANIES REALLY MEAN BY "*WE VALUE YOUR PRIVACY."*

Data privacy deals with how our personal data is handled once acquired to ensure its use is limited to the initially given purpose.[81] Often, data privacy

---

72 *RFDI Position Statement*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/other/rfid-position-statement (last visited Mar. 22, 2022).

73 Haryanto, *supra* note 65; *see RFDI Position Statement*, *supra* note 72 (highlighting the threats to privacy and civil liberties imposed by human microchipping and the power to hold data about the person).

74 Camille Caldera, *supra* note 43.

75 van Hooijdonk, *supra* note 1; Haryanto, *supra* note 65.

76 *See generally* Charles Smith, *supra* note 12.

77 *See generally* Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat 1896 (1974) (codified at 5 U.S.C. § 552(a)); Charles Smith, *supra* note 12, at 152; *Data Privacy*, *supra* note 12.

78 Christopher Hart, *What Is Data Privacy?*, NE. UNIV. (Nov. 26 2019), https://www.northeastern.edu/graduate/blog/what-is-data-privacy/.

79 van Hooijdonk, *supra* note 1; Jeff Petters, *Data Privacy Guide: Definitions, Explanations and Legislation*, VARONIS (Sept. 28, 2020), https://www.varonis.com/blog/data-privacy/.

80 *See* Gray, *supra* note 49.

81 Petters, *supra* note 79.

concerns arise regarding who has access to our data, whether it is shared with others, and how it is collected and stored.[82] Experts estimate that approximately 7.5 septillion gigabytes of data are generated a day.[83] In the private sector, companies acquire personal data from individuals using their apps, websites, and products.[84] While we may not think about the implications of the data collection, it is important to acknowledge that every use of a company's product reveals personal details.[85] For example, companies make inferences about where users live, the income they make, how they spend their free time, and even how many calories a user burns in a day based data points collected in the aggregate.[86]

In addition to collecting data from users, many technology companies exchange that data with third parties.[87] For example, Google uses data observations of its users as the company's primary source of income by "build[ing] individual profiles with demographics and interests, then let[ting] advertisers target groups of people based on those traits."[88] Additionally, Google capitalizes on the ability to "share[] data with advertisers directly and ask[] them to bid on individual ads."[89] Thus, even if a company claims not to sell personal data information, that does not always mean the company does not share such data with third parties, ultimately exploiting user data in other ways.[90]

Users consistently consent to this sharing by checking a little box after a long list of terms and conditions, which stands for an agreement to the company's privacy policies.[91] However, what information will actually be shared is often concealed in a sea of policy, rules, and empty promises.[92] Given this, individuals

---

82 Petters, *supra* note 79 (explaining data privacy generally and the regulatory restrictions on companies that collect or use personal data).

83 *Companies Collect a Lot of Data, But How Much Do They Actually Use?*, PRICEONOMICS (Aug. 7, 2019), https://priceonomics.com/companies-collect-a-lot-of-data-but-how-much-do/ (Explaining that a septillion is denoted as 1,000,000,000,000,000,000,000,000).

84 *Id.*

85 Jared Willis, *How Much Data Do the Big Tech Companies Have on You?*, MEDIUM (Oct. 29, 2018), https://medium.com/@jaredwillis24/how-much-data-do-the-big-tech-companies-have-on-you-bf47377785f.

86 *Id.*

87 Katharine Schwab, *How Widely Do Companies Share User Data? Here's a Chilling Glimpse*, FAST CO. (Jan. 19, 2018), https://www.fastcompany.com/90157501/how-widely-do-companies-share-user-data-heres-a-chilling-glimpse.

88 Bennett Cyphers, *Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.*, ELEC. FRONTIER FOUND. (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and.

89 *Id.*

90 *Id.*

91 *See generally*, Katharine Schwab, *supra* note 87 (noting the broad scope agreements in privacy policies).

92 *Id.*

turn to legislation to protect them from the injustice and dangers of unethical data use.[93] But can the law adequately protect the most personal, sacred information compiled with every scan of a microchip?[94]

A. The United States' Weak Attempts to "Update its Privacy Policy."

The Constitution of the United States protects certain privacy rights through the Fourth Amendment; particularly it protects against unreasonable searches and seizures by the government.[95] In addition, courts interpret the Fifth and Fourteenth Amendment Due Process Clauses to provide an individual privacy right with regard to certain intimate activities and decisions of personhood.[96] While these Constitutional safeguards can offer protection against government action, they do not extend to private actors.[97] Notably, there is no general right to privacy with regard to personal information through the United States Constitution.[98]

Federal laws exist to address specific types of data collection, such as the Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act (ECPA), and the Children's Online Privacy Protection Act (COPPA).[99] These laws provide limited protection over certain aspects of medical data (HIPPA), government interception of electronic communications (ECPA), and parental regulation over collection of their children's data (COPPA).[100] However, because many data privacy issues fall outside the scope of these specific regulations, and data privacy is a subset of privacy, citizens must turn to the general privacy laws of our nation for privacy protections.[101] The problem is that the United States lacks a comprehensive federal privacy law.[102]

---

93 *See* Gray, *supra* note 49.

94 *See id.* (explaining the similarities and differences in the data privacy laws that may be applicable to this technology's data collection).

95 U.S. CONST. amend. IV; JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS 208–10 (9th ed. 2019).

96 U.S. CONST. amend. V; U.S. CONST. amend. XIV; *see generally* Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVESCIENCE (June 12, 2013), https://www.livescience.com/37398-right-to-privacy.html (explaining generally the right to privacy as protected by the U.S. Constitution and through the Supreme Court's judicial opinions interpreting such).

97 Hart, *supra* note 78.

98 Hart, *supra* note 78 ("It can be surprising to learn that there is no overarching federal law governing data privacy. Instead, data privacy is a fragmented legal concept.").

99 *Data Privacy*, *supra* note 12.

100 Petters, *supra* note 79; *Data Privacy*, *supra* note 12.

101 *See generally* Petters, *supra* note 79.

102 Charles Smith, *supra* note 12, at 155.

1. The United States Federal Privacy Laws Are Too Specific in Context and Too Narrow in Scope.

The United States federal government is trailing far behind other nations with the development of comprehensive privacy laws.[103] While lacking a general privacy law, the United States has developed privacy laws geared toward specific industries such as HIPAA, ECPA, and COPPA, as discussed above.[104] The most comprehensive law enacted regarding privacy is The Privacy Act of 1974, which provides in relevant part, "the right to privacy is a personal and fundamental right protected by the constitution of the United States," however, notably, this is only applicable against federal government action.[105] Thus, similar to the Fourth, Fifth, and Fourteenth Amendments, it is of little help with regard to private companies who "are not bound by the fair information practices, open-access rules, and data-ownership principles embodied in the Act."[106] In sum, the aforementioned limitations actively demonstrate that not only does the United States lack a comprehensive privacy law to protect its citizens, but even where such rights are explicitly protected, the protection is limited to specific contexts or violations by the government.[107]

2. State Microchipping Laws Leave Citizens Vulnerable to the Data Privacy Implications from Third Party Use of the Microchip's Stored Data.

As has been explicitly indicated by the United States Supreme Court, although there are constitutional protections over privacy, "the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."[108] However, regarding microchipping, only 11 states have enacted applicable legislation banning mandatory human microchipping.[109] Other states have declined to ban the use of microchips outright but require written informed consent before implantation can occur.[110] Informed consent is

---

103 *Id.*; *see generally Data Privacy*, *supra* note 12 (explaining the federal laws in the European Union protecting citizens).

104 *Data Privacy*, *supra* note 12.

105 Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat 1896 (1974) (codified at 5 U.S.C. § 552(a)).

106 Charles Smith, *supra* note 12, at 155.

107 Charles Smith, *supra* note 12, at 155; Hart, *supra* note 78.

108 Katz v. United States, 389 U.S. 347, 350–51 (1967).

109 Smith, *supra* note 2.

110 Mack Wilding, *States Are Banning Microchip Implants in Employees (But Who Is Implanting Their Employees with Mircochips?)*, FORTIS L. PARTNERS (Mar. 9, 2020), https://www.fortislawpartners.com/blog/states-are-banning-microchip-implants-in-employees-but-who-is-implanting-their-employees-with-microchips; s*ee e.g.*, S.B. 286 (Mont. 2019); S.B. 2220 (Fla. 2007) (declaring it a felony to perform implantation without

generally defined as "a person's agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives."[111] When it comes to microchip installation, there is a potential issue with informed consent given the unknown implications with microchip company's collection of data.[112] On one hand, a person might understand the risks associated with the microchip and not care.[113] On the other hand, however, some may not consider the possible uses of their personal information when pondering the risks.[114] Therefore, even though these laws require informed consent, it is unlikely to be a very high bar, given that agreeing to the terms and conditions or signing a medical release at installation can satisfy these requirements.[115] As a result, we must consider whether these actions truly constitute full knowledge of the risks involved.[116]

The states with active legislation outright banning mandatory human implants include California, Wisconsin, Maryland, New Hampshire, North Dakota, Oklahoma, and Utah.[117] Specifically, within the employment context, four additional states have passed statutes banning employers' compelled human microchipping of employees.[118] States with such legislation include Missouri, Arkansas, Indiana, and Montana.[119]

Lastly, and of significance, is the legislation passed in Nevada prohibiting:

> an officer or employee of this State or any political subdivision thereof or any other person from: (1) requiring another person to undergo the implantation of a microchip or other permanent identification marker of any kind or nature; (2) establishing a

---

informed written consent).

111 *Informed Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019).

112 *California Consumer Privacy Act*, BRYAN CAVE LEIGHTON PAISNER, https://ccpa-info.com/faqs/definitions/ (last visited Mar. 23, 2022) (providing, as an example of consent, "[i]f a company chooses to adopt a cookie banner that provides notice and solicits the opt-in consent (e.g., 'I agree') of website users, the company would have a strong argument that it does not need to disclose that it has sold information, does not need to forward deletion requests to the providers of its third party cookies, and does not need to include an 'opt out of sale' link on its website.").

113 *See* Smith, *supra* note 2.

114 *Id.*

115 *Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, esp. given voluntarily by a competent person; legally effective assent."); *California Consumer Privacy Act*, *supra* note 112 ("CCPA does not require that a company obtain the consent (or the 'opt-in') of a person before collecting or using their personal information" since "consent only arises within the CCPA if a company intends to sell information.").

116 *Consent*, *supra* note 115; *Informed Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019).

117 Smith, *supra* note 2.

118 *Id.*

119 *Id.*

> program that authorizes a person to voluntarily elect to undergo the implantation of such a microchip or permanent identification marker; or (3) participating in a program established by another person, if the program authorizes a person to voluntarily elect to undergo the implantation of such a microchip or permanent identification marker.[120]

This statute is the most restrictive on human microchipping and extends to forbid programs that allow voluntary human implantation.[121] Importantly, however, the statute is limited in application to government actors and employer mandated programs which may not provide adequate protection from external pressures in the private sector.[122] Moreover, a few states have proposed legislation for addressing human microchipping, including Indiana, Tennessee, and Iowa.[123]

Nevertheless, issues arise with the enactment of state legislation as each law is inherently distinct.[124] In *The Legal Ramifications of Microchipping People in the United States of America – a State Legislative Comparison*, Angelo Friggieri describes the root of the issue by stating, "[t]he problem with state laws, as demonstrated in the U.S.A is that legislation is not uniform, at least at the state level."[125] For example, the Oklahoma and Wisconsin statutes pose an initial $10,000 fine and an additional $10,000 fine for each consecutive day that the violation persists.[126] In contrast, the Ohio legislation poses an initial $150 fine and no additional fine thereafter.[127] Moreover, each statute uses different language and prohibits different conduct.[128] For example, California and Ohio's microchip laws permit parents of minor children to force microchip implantation.[129] In contrast, legislation in Colorado, Florida, North Dakota, Oklahoma, and Wisconsin does not contemplate parents' ability to microchip their minor children.[130] These discrepancies make enforcement arbitrary since potential violators, such as government actors or employers, have little

---

120 *Id.*; NEV. REV. STAT. ANN. § 200.870 (West 2021).

121 Smith, *supra* note 2.; NEV. REV. STAT. ANN. § 200.870.

122 Smith, *supra* note 2; NEV. REV. STAT. ANN. § 200.870.

123 *See States Just Saying No to Employee Microchipping*, LEXIS NEXIS https://www.lexisnexis.com/en-us/products/state-net/news/2020/03/13/states-just-saying-no.page (last visited Mar. 11, 2022).

124 *See* Angelo Friggieri et al., *The Legal Ramifications of Microchipping People in the United States of America - A State Legislative Comparison*, UNIV. OF WOLLONGONG, https://ro.uow.edu.au/commpapers/3020/ (last visited Mar. 11, 2022).

125 *Id.*

126 *Id.; see also* OKLA. STAT. ANN. tit. 63, § 1-1430(B) (West 2021); WIS. STAT. ANN. § 146.25(2) (West 2022).

127 Friggieri, *supra* note 124.

128 *See id.*

129 *See id.*

130 Friggieri, *supra* note 124.

understanding of what action is explicitly prohibited and how the law assesses the violations.[131] Additionally, the differences open the door for inconsistent enforcement, punishments, and protections, which exacerbate the legislation's uncertainty in general.[132] Additionally, even in states regulating microchipping, there is minimal legislation pertaining to the data collected by the microchip.[133]

3. State Data Privacy Laws Are the Last Hope for Consumers Data Privacy Protection but Exceptions Leave Room for Companies to Avoid Compliance with the Regulation.

In the United States, when it comes to data collection generally, some members of the privacy industry presume that companies can collect and share data on individuals.[134] In contrast, in the European Union, the presumption resides with the individual having control over companies' ability to collect their data.[135] Under the GDPR, this approach allows individuals to limit sharing and provides comfort when using a company product.[136]

Currently, three states have data privacy legislation that lobbyists are pushing the federal government to substantively adopt.[137] In June of 2018, the California Consumer Privacy Act was signed into law and became the first data privacy law in the United States (CCPA).[138] It is modeled after the European Union's GDPR but is not as protective with regard to the security of data.[139] On the other hand, the law interprets private data to encompass more information; therefore, it subjects the company to regulation more easily.[140]

On March 2, 2021, Virginia enacted the Consumer Data Protection Act (CDPA), becoming the second state to successfully develop data privacy legislation.[141] The CDPA is modeled after both the CCPA and GDPR but has

---

131 *Id.*

132 *See generally id.*

133 Smith, *supra* note 2.

134 *See generally* Gray, *supra* note 49.

135 *Id.*

136 *Id.*

137 In January of 2021, the Washington Privacy Act of 2021 failed in the state's House for the third time. This framework was supported by members of the privacy industry as a potential outline for federal legislation. However, because of its failure, discussion of the bill has been removed from the scope of this article. For discussion, *see generally* David Stauss, *2021 Washington Privacy Act Released*, JDSUPRA (Jan. 11, 2021), https://www.jdsupra.com/legalnews/2021-washington-privacy-act-released-2010940/; *see also* Gray, *supra* note 49.

138 Korolov, *supra* note 49.

139 *Id.*

140 *Id.*

141 *Virginia Becomes the Second State to Pass a Comprehensive Privacy Law*, DAVIS

significant differences.[142] For example, the CDPA's definition of "personal data" is narrower than the CCPA, leaving information linkable to a household, rather than an individual, outside the regulatory scope.[143] Moreover, the CDPA's consumer rights and data processing restrictions are similar to the GDPR.[144]

Most recently, Colorado enacted the Colorado Privacy Act (CPA) in July of 2021.[145] The legislation resembles the CDPA and CCPA but has more limited applicability criteria.[146] Additionally, the CPA does not include a private right of action for alleged violations.[147] Regardless of these distinctions, until a comprehensive federal data privacy law is enacted, we should anticipate continued state legislation in this area.[148] Exploring the subtle differences amongst these approaches exposes various weaknesses in consumer data protection and highlights the need for overarching federal legislation.

i. The Majority View: Shall in California Consumer Privacy Act Does Not Mean Must.

Although the CCPA is a California state law that targets companies that collect data on California consumers, many large technology companies strive to satisfy the law's requirements for all consumers, regardless of their physical location.[149] The reason for this circumstance is largely because companies seek to provide uniform protection and to comply with the most restrictive law.[150] Moreover, companies, especially technology-based companies like microchip vendors, will have difficulty avoiding the California market.[151]

A company is subject to compliance with the California Consumer Privacy Act if it (1) is for-profit; (2) does business in California; and (3) has a "gross annual revenue of over $25 million; or buys, receives, or sells personal information of 50,000 or more California residents, households, or devices; or derives fifty percent or more of its annual revenue from selling California

---

GILBERT, https://www.dglaw.com/virginia-becomes-the-second-state-to-pass-a-comprehensive-privacy-law/ (last visited Mar. 8, 2022).

142 *Id.*

143 *Id.*

144 *Id.*

145 David O. Klein, *United States: How does the Colorado Privacy Law Compare to the CCPA?*, KMT (July 14, 2021), https://www.mondaq.com/unitedstates/data-protection/1090446/how-does-the-colorado-privacy-law-compare-to-the-ccpa.

146 *Id.*

147 *Id.*

148 *Id.*

149 *CCPA's Impact on Non-California Businesses*, SIXFIFTY (Aug. 9, 2019), https://www.sixfifty.com/ccpas-impact-on-non-california-businesses/.

150 *Id.*

151 *Id.*

resident's personal information."[152]

Once a company is subject to the CCPA, the law puts some power back into the hands of individuals concerning their data.[153] Under the CCPA, personal information is defined as that which "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[154] Furthermore, the Act includes specific examples of personal information such as email address, online handles, IP address, biometric information, geographic location, and browsing and search history.[155]

Specifically, the law provides that California consumers shall have certain rights that include (1) the right to know what personal information a company collects; (2) the right to know whether their personal data is being sold or disclosed to other, and if so, to whom; (3) the right to delete personal data collected, subject to exceptions; (4) the right to opt-out of the sale of their data; (5) the right to exercise their CCPA rights without discrimination; and (6) in the event of a data breach, the right to initiate a private cause of action.[156] On December 16, 2020, an amendment to the CCPA took effect and is known as the California Privacy Rights Act (CPRA).[157] The CPRA provides two additional rights to the aforementioned list including (6) the right to correct inaccurate personal information; and (7) the right to restrict the use and disclosure of some sensitive personal data.[158] Accordingly, companies collecting data must inform consumers which categories of data they collect and why.[159]

While the promise of consumer rights sounds attractive and helpful, the CCPA is not as protective as it appears at first blush.[160] These rights are subject to exceptions and caveats. More specifically, the statute's language demanding

---

152 CAL. CIV. CODE § 1798.140(c)(1)(A)-(C) (2018); *California Consumer Privacy Act (CCPA)*, ST. OF CAL. DEP'T OF JUST., https://oag.ca.gov/privacy/ccpa (last visited Mar. 30, 2022).

153 *Id.*

154 CAL. CIV. CODE § 1798.140(o)(1) (2018); Andy Green, *California Consumer Privacy Act (CCPA) Compliance Guide*, VARONIS (Oct. 17, 2019), https://www.varonis.com/blog/california-consumer-privacy-act-ccpa.

155 CAL. CIV. CODE § 1798.140(o)(1)(a)-(k) (2018); Green, *supra* note 154.

156 CAL. CIV. CODE § 1798.100 (2018); CAL. CIV. CODE § 1798.115 (2018); CAL. CIV. CODE § 1798.105 (2018); CAL. CIV. CODE § 1798.120 (2018); CAL. CIV. CODE § 1798.125(a)(1) (2018); *California Consumer Privacy Act (CCPA)*, *supra* note 152.

157 *CCPA v. CPRA: What's the Difference?*, BLOOMBERG LAW (July 13, 2021), https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/.

158 *Id.*

159 *California Consumer Privacy Act (CCPA)*, *supra* note 152.

160 Gray, *supra* note 49.

that companies *shall* inform consumers does not always mean they *must* do so.[161] For example, certain actions do not fall within the 'sale' of data under the CCPA's explicit statutory language.[162] These include transfers by the consumer, alerting third party companies when a person elects to opt-out, data disclosed to a service provider, and transfers where the receiving company assumes control of the sending company.[163] Moreover, these regulations do not apply to "personal information collected for a single, one-time transaction, if such information is not sold."[164] Thus, leaving vulnerable areas, perhaps intentionally, that the CCPA fails to cover.[165]

The law's applicability also depends upon the context in which the data is collected.[166] Specifically, on its face, the CCPA provides additional restrictions for the collection of a minor's data, in conjunction with the COPPA.[167] Additionally, companies subject to HIPAA are not required to comply with the CCPA.[168] These particular caveats will be explored in Part III of this article under the applicable area of impact.[169]

ii. An Alternative Approach: The Virginia Consumer Data Protection Act and its Exclusions for Pseudonymous Data

The Virginia Consumer Data Protection Act passed into law and takes effect in January of 2023.[170] From an industry perspective, this law is less appealing than the CCPA because its protections are more limited, and many companies prefer to comply with the most restrictive laws.[171] Specifically, the law extends to companies conducting business in the state as well as those who produce products and services targeting residents.[172] Beyond those broad requirements, to be subject to the CDPA, a company must control or process data from at least (1) "100,000 [Virginia] consumers during a calendar year; or (2) 25,000 [Virginia] consumers and derive[] over 50 percent of gross revenue from the sale

---

161 *Id.;* Dennis Dayman, *CCPA "Sell" Definition*, OSANO (Jan. 15, 2021), https://www.osano.com/articles/ccpa-definition-sell.

162 Dayman, *supra* note 161.

163 Dayman, *supra* note 161.

164 CAL. CIV. CODE § 1798.100(e) (2018).

165 Dayman, *supra* note 161.

166 Mark Diamond, *Quick Overview: Understanding the California Consumer Privacy Act (CCPA)*, ASS. OF CORP. COUNS. (July 26, 2019), https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa.

167 *Id.*

168 *California Consumer Privacy Act (CCPA)*, *supra* note 152.

169 *See infra* Part III.

170 *Virginia Becomes the Second State to Pass a Comprehensive Privacy Law*, *supra* note 141.

171 *Id.*

172 S.B. 5062, 67th Leg., Reg. Sess. (Wash. 2021); Gray, *supra* note 49.

of personal data."[173] Notably, the CDPA does not include a broad annual gross revenue requirement, like the CCPA, which subjects entities collecting data from a small number of state consumers to the law.[174] Thus, the number of entities falling within the Virginia law's reach is restricted.[175]

Another significant distinction between the CCPA and the CDPA is the latter's definition for the "sale of personal data."[176] To constitute a sale under the Virginia legislation, such exchange must result in *monetary consideration*.[177] Whereas, under the California legislation a sale can result from an exchange for *any valuable consideration*. [178] Thus, under the CDPA certain data disclosures fall outside the law's scope including those made to affiliates, third parties performing services or processing data for the entity, and transactions in which a third party assumes control of the collecting entity.[179] While subtle, this distinction leaves a range of data transactions exempt from regulation.

Notably, the CDPA offers similar but slightly broader range of rights to consumers with respect to their personal data.[180] Distinguishable from the CCPA, this law allows individuals asserting their opt-out rights to prohibit profiling and targeted advertising as well as the sale of data.[181] Lastly, the law requires individuals to opt-in in order for companies to collect sensitive information such as "racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status… biometric data… or precise geolocation data."[182] The opt-in provision generally requires consumer consent.[183]

Excluded from protection under the CDPA is pseudonymous data, or that which "cannot be attributed to a specific consumer without the use of additional information."[184] While de-identifying information poses less risk to consumers

---

173 *Virginia Becomes the Second State to Pass a Comprehensive Privacy Law*, *supra* note 141.

174 *What Is the Virginia Consumer Data Protection Act (VCDPA)?*, BLOOMBERG LAW (Aug. 4, 2021), https://pro.bloomberglaw.com/brief/what-is-the-vcdpa/.

175 *See generally id.*

176 Daniel Ilan et al., *The "New" Dominion of Privacy Law: Virginia Becomes Second State to Pass Comprehensive Consumer Data Privacy Act*, CLEARY GOTTLIEB (Apr. 14, 2021), https://www.clearygottlieb.com/-/media/files/alert-memos-2021/the-new-dominion-of-privacy-law-virginia-becomes-second-state.pdf.

177 *Id.*

178 *Id.*

179 *Id.*

180 *Id.*

181 *Id.;* Additionally, the CDPA includes the right to alter incorrect personal information, which the CCPA does not. *Id.*

182 *Id.*

183 *Id.*

184 Gray, *supra* note 49.

if shared without consent, the risk of data privacy invasion is still prevalent.[185] Moreover, exercising the rights given to consumers under the act becomes increasingly more difficult the further companies decrease the identifiability of collected data.[186]

In sum, despite its weaknesses, the CCPA is more protective of data privacy than the CDPA and closer to the GDPR's broad privacy protections.[187] Substantive adoption of this law on the federal level could serve as the basis for limiting the collection and sharing of data gathered via the human microchip.[188]

III. IMPLICATIONS OF MICROCHIP USE IN SPECIFIC CONTEXTS

Microchipping presents a multitude of general privacy concerns, as laid out in Part I of this article.[189] In addition, however, the implants present unique consequences in the private employment sector and in the context of a parent's right to protect their children.[190]

As the discussion of prior existing privacy laws and protections indicates, lawmakers must enact federal legislation that works to encompass private actors in addition to the restrictions on government actors.[191] Moreover, such legislation must be directly responsive to the data privacy implications of microchips and protect against unauthorized collection and sharing.[192]

A. Employers May Mandate Employees be Microchipped and Data Monitoring Doesn't End When Employees Clock Out.

Currently, a common use of human microchipping in the United States occurs in the workplace to enhance convenience with building security, computer log ins, and more ultimately replacing the traditional ID badge.[193] Once Three Squares Market brought the microchip technology to the Unites States employment realm, it opened a Pandora's box of potential concerns regarding employee privacy.[194] As Dario Rodriguez indicated in his article, *Chipping in at Work: Privacy Concerns Related to the Use of Body Microchipping in the Employer-Employee Context*, "[t]he advent of Radio Frequency Identification

185 *Id.*
186 *Id.*
187 *See generally id.;* Ilan, *supra* note 176.
188 *See generally* Gray, *supra* note 49; Ilan, *supra* note 176.
189 *See supra* Part I.
190 van Hooijdonk, *supra* note 1.
191 Gray, *supra* note 49.
192 Friggieri, *supra* note 124; Haryanto, *supra* note 65.
193 Keshner, *supra* note 36.
194 *Id.*; *Company to Become First in U.S. to Microchip Employees*, *supra* note 37.

('RFID') technology has brought significant change to the global economy and society."[195] Further, Rodriguez found that "[w]hile much of the change has improved citizens' quality of life and resulted in tremendous economic growth, some developments have come at the cost of reduced employee privacy."[196] This concern is heightened given the company currently using this technology has indicated it wishes to expand upon the microchip's capability, which would allow for an increase in monitoring of employees.[197] Since the microchip is unable to be removed and the chip can be scanned involuntarily by any reading close by, the issue becomes at which point have employers gone too far.[198] Is this an invasion of employees' private lives with access to information about employees after hours and outside the workplace?[199]

As previously discussed, the constitutional protections and Privacy Act of 1974 will be of little help in ensuring employees right to privacy is not violated, unless they are employed by the government.[200] Therefore, employees in the private sector must turn to unstable and often unavailable state legislation for protection against compelled human microchipping.[201] With this technology, employers have the ability to monitor movement within the building as an employee swipes through security stations within the four walls of the company, thereby indicating the amount of time one spends in the break room or how frequently an employee uses the restroom.[202] Moreover, this information could impact employment decisions based on productivity, hiring decisions based on employee's willingness to be implanted, and more.[203] At what point does this ability and data collection infringe on the employees' right to privacy?[204]

Moreover, not only is state privacy legislation radically different in the few states where it's been enacted, those states that do have legislation have failed to account for protection of the personal data that is collected by the microchip.[205] Many employers using microchip data will be subject to

---

195 Dario A. Rodrigues, *Chipping in at Work: Privacy Concerns Related to the Use of Body Microchip ("RFID") Implants in the Employer-Employee Context*, 104 IOWA L. REV. 1581, 1582 (2019).

196 *Id.*

197 Holley, *supra* note 38.

198 Smith, *supra* note 2.

199 Rodrigues, *supra* note 195, at 1582.

200 Privacy Act of 1974, Pub. L. No. 93–579, 88 Stat 1896 (1974) (codified at 5 U.S.C. § 552(a)); Hart, *supra* note 78.

201 Friggieri, *supra* note 124.

202 *Company to Become First in U.S. to Microchip Employees*, *supra* note 37.

203 Rodrigues, *supra* note 195, at 1584.

204 *See generally id.*

205 *See e.g.*, NEV. REV. STAT. ANN § 200.870 (West 2019) (failing to account for anything other than the compelled implantation).

provisions similar to the CCPA, if mirrored legislation is enacted federally.[206] Accordingly, it is likely that the use of microchip information by employers will not be subject to the legislation's requirements given that transfers of data by the consumer are exempted.[207] This exception dictates that, "[a] sale does not occur when a consumer intentionally directs or uses a business to disclose their personal information."[208] This is relevant in the employment context because, the employer will likely require that the employee allow their personal information to be shared with the employer in exchange for using the microchip services, like accessing the building or computer log ins, during the course of employment.[209] Thereby, the transfer of personal data falls outside the scope of the CCPA since it is directed by the consumer.[210] While in this limited circumstance employees may not mind the data transfer, what happens once he clocks out?[211] It is not clear whether the CCPA will protect the data acquired after hours since the microchip opens the door for continued monitorization.[212]

In sum, to respond to these concerns Congress needs to develop a comprehensive law banning human microchipping in the employment context.[213] Contrary to this solution, some may argue that laws need only ban the involuntary use of such devices.[214] However, given the privacy consequences and potential for employment discrimination on this basis, the best solution is to prohibit the use of this technology in employment.[215] At the very least, restrictions should be considered regarding an employer's use of the microchip data capabilities outside the employer's company.[216] Additionally, adoption of a federal data privacy law, such as the CCPA or WPA, could protect against the collection of data outside of the workplace, although certain exceptions may make the legislation unapplicable in this context.[217]

B. The Limited Privacy Rights of Children to Protect their Freedom and Data from Compelled Microchipping with Parental Consent.

Another area of potential use for the human microchip implant arises from a

---

206 CAL. CIV. CODE § 1798.100 (2018)*; California Consumer Privacy Act (CCPA), supra* note 152.
207 Dayman, *supra* note 161.
208 *Id.;* CAL CIV. CODE § 1798.140(t)(2)(A) (2020).
209 *Company to Become First in U.S. to Microchip Employees*, *supra* note 37.
210 Dayman, *supra* note 161.
211 Rodrigues, *supra* note 195, at 1597–98.
212 *Id.* at 1596, 1604.
213 Smith, *supra* note 2.
214 *See generally* van Hooijdonk, *supra* note 1.
215 Dayman, *supra* note 161.
216 Rodrigues, *supra* note 195, at 1607.
217 Dayman, *supra* note 161; Korolov, *supra* note 49.

parent's desire to protect their children's safety by inserting microchips in them for supervision.[218] Although microchip implants in human flesh have not yet reached this context, the RFID chip has been used in children's school ID cards and backpacks for similar purposes.[219] In reaction to this use, Missouri passed legislation that provided, "[n]o school district shall require a student to use an identification device that uses radio frequency identification technology, or similar technology, to identify the student, transmit information regarding the student, or monitor or track the location of the student."[220] Outside of this legislation however, other states do not have regulations addressing the use of microchips in this context.[221] State laws that ban involuntary microchipping of *any person* may provide some protection for children who resent this implantation.[222]

Interesting conflicting rights are generated from this situation under the Due Process Clause of the Fourteenth Amendment.[223] The first of these conflicting rights is acknowledged in *Troxel v. Granville* where the United States Supreme Court recognized that the fundamental due process liberty interest of parents in the "care, custody, and control of their children— is perhaps the oldest of the fundamental liberty interests recognized by this Court."[224] Moreover, the United States Supreme Court has recognized that "'liberty of parents and guardians'" includes the right "'to direct the upbringing and education of children under their control.'"[225] Lastly, the United States Supreme Court bolstered the importance of this right and its reluctance to allow governments to interfere with it in *Prince v. Massachusetts*, stating "[i]t is cardinal with us that the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder."[226] These cases display the Court's reluctance to allow the government to interfere with the parents right to raise their child in the manner they see fit.[227]

In conflict with this due process right of parents to the care, custody, and control of their children is the child's own due process right to privacy and

---

218 van Hooijdonk, *supra* note 1.

219 Stefan P. Schropp, *Biometric Data Collection and RFID Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy*, 94 N.C. L. REV. 1068, 1074 (2016).

220 MO. REV. STAT. § 167.168(1) (2014).

221 Schropp, *supra* note 219, at 1074.

222 Smith, *supra* note 2.

223 *See, e.g*, Troxel v. Granville, 530 U.S. 57, 65 (2000).

224 *Id.*

225 *Id.* at 65 (quoting Pierce v. Society of Sisters, 268 U.S. 510, 534–535 (1925)).

226 Prince v. Mass., 321 U.S. 158, 166 (1944).

227 *Troxel*, 530 U.S. at 65; *Prince*, 321 U.S. at 166.

freedom to be left alone.[228] The United States Supreme Court in *Planned Parenthood of Missouri v. Danforth*, recognized with regard to a child's due process rights that, "[c]onstitutional rights do not mature and come into being magically only when one attains the state-defined age of majority. Minors, as well as adults, are protected by the Constitution and possess constitutional rights."[229] In some limited cases courts have recognized that a child's substantial liberty interest perseveres over the parental right to control; however, such instances are limited.[230]

Given the courts' reluctance to interfere with parental rights and the presumption that such rights trump the child's liberty interest, even if legislatures wanted to prevent involuntary microchipping of children by parents, they would need to surpass the high levels of scrutiny required to interfere with a fundamental due process right.[231] Importantly, however, at present, no state legislatures have acted with regard to this issue despite the attempts to use microchipping within this context although not inserted under the skin.[232] It is inevitable that this technology will rear its head directly in this context and without proper government action the impact on privacy of children will be affected.[233]

Microchipping in this context also presents data collection concerns.[234] When it comes to using the data collected on a child's microchip, the CCPA, if adopted, will place additional restrictions on companies collecting a minor's personal information.[235] Specifically, the CCPA prohibits sale of personal information of persons under seventeen without their consent.[236] Children from the ages of thirteen to sixteen are eligible to provide direct consent while children under thirteen years old require parental consent for data sharing.[237] It is unclear what constitutes adequate consent under CCPA.[238] For instance, if accepting the terms

---

228 *See e.g.*, Planned Parenthood of Mo. v Danforth, 428 U.S. 52, 74 (1976); Matter of Andrew R., 115 Misc. 2d 937, 939 (N.Y. Fam. Ct. 1982).

229 *Planned Parenthood of Mo.*, 428 U.S. at 74.

230 *See Matter of Andrew R.*, 115 Misc. 2d at 938 (holding that voluntary placement of a child by a parent into a care facility without review by a neutral fact finder violated the child's fundamental liberty interest under the Fourteenth Amendment); *see also* Parham v. J. R., 442 U.S. 584, 600 (1979) ("It is not disputed that a child, in common with adults, has a substantial liberty interest in not being confined unnecessarily for medical treatment . . . under the Fourteenth Amendment).

231 *See Troxel*, 530 U.S. at 65.

232 Smith, *supra* note 2.

233 Schropp, *supra* note 219, at 1095.

234 *See generally* Smith, *supra* note 2 (explaining the downside to human microchipping and the microchip's ability to gather personal information about the implanted person).

235 Diamond, *supra* note 166.

236 *Id.*

237 *Id.*

238 *California Consumer Privacy Act*, *supra* note 112 (acknowledging that "CCPA does

and conditions for using the microchip constitutes adequate consent, we need to consider whether these restrictions really accomplish the purpose of providing additional protection for personal information about minors.[239] Therefore, even if the federal government adopts the CCPA or WPA, its ability to provide genuine protection is significantly impaired.[240]

Another area of potential protection in this context can be found in the Children's Online Privacy Protection Act (COPPA).[241] According to the Federal Trade Commission's rule summary, "COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age."[242] Specifically, the Act requires company's subject to regulation to comply with the following requirements: (1) display privacy policy for collected personal information; (2) provide notice and obtain parent consent before collecting; (3) make clear whether the data can be shared with third parties; (4) allow parental review and deletion; (5) opportunity to stop further collection; (6) keep information confidential and secure; (6) abstain from retaining information past the point necessary; and (7) not condition participation on disclosure more than necessary.[243]

Furthermore, COPPA applies to "operators of… online services… directed to children under 13 that collect, use, or disclose personal information from children, or on whose behalf such information is collected or maintained… and operators of with actual knowledge that they are collecting, using, or disclosing personal information from children under 13, and to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.[244] Thus, at

---

not require that a company obtain the consent (or the 'opt-in') of a person before collecting or using their personal information" since "consent only arises within the CCPA if a company intends to sell information.").

239 *Consent*, *supra* note 115 (defining consent as "[a] voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, esp. given voluntarily by a competent person; legally effective assent.").

240 Korolov, *supra* note 49; Gray, *supra* note 49.

241 *Data Privacy*, *supra* note 12.

242 *Children's Online Privacy Protection Rule ("COPPA")*, FED. TRADE COMM., https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (last visited Mar. 30, 2022); 16 C.F.R. § 312.1 (2021).

243 15 U.S.C. § 6502 (1998); *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM., https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0 (last visited Mar. 30, 2022).

244 15 U.S.C. § 6501 (1998); *Complying with COPPA: Frequently Asked Questions*, *supra* note 243.

first glance, COPPA appears to provide protection for children from collection by the company whose services the child implores and disclosure by that company to third parties.[245]

A readily apparent limitation of this Act stems from its applicability only to children under the age of 13, rather than all minor children which is generally interpreted as under the age of 18.[246] Moreover, COPPA as written requires the collector of data to have actual knowledge that the person whose data they are collecting is under the age of 13 before a violation has occurred.[247] As demonstrated, this scienter requirement limits COPPA's applicability while the technological world continues to advance, and children are becoming increasingly more active on these platforms.[248] This limitation reflects the primary purpose of COPPA, which seeks to balance the need to protect children from unauthorized use of personal data, with the nature of the technological world we live in, mainly the Internet.[249] Additionally, the Act allows for parental consent to waive the restrictions on use of their child's data; thus, allowing little protection for the data of a microchip child, implanted at the behest of their parent.[250]

IV. CONCLUSION

Although the use of human microchip implants will add convenience aspects to one's life and the simple tasks we do every day, the potential privacy implications far outweigh any benefits.[251] Microchipping presents issues with data collection and sharing, while opening the door for unauthorized surveillance.[252] The current state of privacy legislation in the United States is ill equipped to protect citizens from data breaches, unwanted monitorization, and the selling of their personal information.[253] If we wish to maintain privacy in our lives the federal government will need to act quickly in response with robust

---

245 15 U.S.C. § 6501 (1998); *Complying with COPPA: Frequently Asked Questions*, *supra* note 243.

246 16 C.F.R. § 312.2 (2021); *Children's Online Privacy Protection Rule ("COPPA")*, *supra* note 242.

247 16 C.F.R. § 312.3 (2021); *Children's Online Privacy Protection Rule ("COPPA")*, *supra* note 242.

248 16 C.F.R. § 312.3 (2021); *Children's Online Privacy Protection Rule ("COPPA")*, *supra* note 242.

249 16 C.F.R. § 312.1 (2021); *Complying with COPPA: Frequently Asked Questions*, *supra* note 243.

250 16 C.F.R. § 312.5 (2021); *Complying with COPPA: Frequently Asked Questions*, *supra* note 243.

251 van Hooijdonk, *supra* note 1.

252 *Id.*

253 *Id.*

data privacy laws specifically addressing the use of data obtained from human microchipping.[254]

254 Gray, *supra* note 49.