# Chipping in at Work: Privacy Concerns Related to the Use of Body Microchip ("RFID") Implants in the Employer–Employee Context

*Dario A. Rodriguez*[*]

*ABSTRACT: The advent of Radio Frequency Identification ("RFID") technology has brought significant change to the global economy and society. While 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. The phenomenon of RFID microchip implants threatens to further erode traditional notions of employee privacy in the employer–employee context. To protect employee privacy, legislators at the state and federal level should draft legislation that prohibits employers from mandating that employees agree to RFID implants. In addition, any legislation that addresses RFID implants should prohibit employers from incentivizing current or potential employees to agree to receive RFID implants. Such legislation should prohibit the use of an employee's implant status in making any determinations related to employment. It should further enable claims for employment discrimination to prevent employers from compelling or incentivizing employees to receive RFID implants, thus safeguarding employee privacy.*



[*] J.D. Candidate, The University of Iowa College of Law, 2019; B.A. in Political Science and Spanish, The University of Wisconsin-Madison, 2011.

## I. INTRODUCTION

"Radio frequency identification ("RFID") technology is a wireless communication technology that enables users to uniquely identify tagged objects or people."[1] The technology requires two physical components: readers and tags. RFID readers "gather information from . . . RFID tag[s], which [are] used to track individual objects. Radio waves are used to transfer

1. V. DANIEL HUNT ET AL., RFID-A GUIDE TO RADIO FREQUENCY IDENTIFICATION xi (2007).

data from the tag to a reader."[2] RFID has become ubiquitous in our modern economy. Uses of RFID technology are seemingly endless—a few examples include retailers tracking apparel,[3] drivers automating payments on the road,[4] hospitals minimizing loss of equipment,[5] corporations optimizing their supply-chain management,[6] and even golfers retrieving lost golf balls.[7] As one author put it, RFID has become "an integral part of our life."[8]

RFID is one of the most revolutionary technologies in society. By tracing RFID use from its post-World War II emergence[9] to its application in the 21st century, the dramatic impact of RFID becomes apparent. Today, RFID chips are no longer limited in application to inanimate objects. RFID chips (which can be combined with GPS technology) are inserted into pets,[10] children,[11]

2. *Radio Frequency Identification Reader (RFID Reader)*, TECHOPEDIA, https://www.techopedia.com/definition/26992/radio-frequency-identification-reader-rfid-reader (last visited Oct. 17, 2018).

3. Rina Raphael, *Interactive "Magic Mirrors" Are Changing How We See Ourselves—And Shop*, FAST COMPANY (Apr. 6, 2017), https://www.fastcompany.com/3066781/can-interactive-mirrors-change-consumer-behavior-retailers-are-bet ("Interactive fitting rooms, for example, automatically recognize products through RFID tags, which sync up to available inventory in the store. Should a customer want a different size or style, she simply requests it from the computerized mirror by pushing a button.").

4. Edson Perin, *Ceitec Delivers 300,000 RFID Chips for Vehicular Tagging*, RFID J. (Sept. 27, 2017), https://www.rfidjournal.com/articles/pdf?16527 ("Ceitec S.A. has announced the sale of 300,000 passive (non-battery-powered) RFID chips for the production of car tags by Q-Free, a Norwegian company that develops intelligent transport systems. The chip will be used, for example, in tags for tolls, parking lots, airports and petrol stations.").

5. *See genereally* THING MAGIC, INC. & INDUSTRIAL PORTALS, GREENVILLE HOSPITAL DEPLOYS INTEGRATED RFID SOLUTION FOR OPERATING ROOM ASSET TRACKING (2009), https://www.healthitoutcomes.com/doc/greenville-hospital-deploys-integrated-rfid-0001.

6. General Steel Holdings, Inc., *General Steel's JV Signs Letter of Intent to Deploy RFID-based Logistics Management at Tewoo Group's Seven Steel Coils Logistic Centers,* PR NEWSWIRE (June 16, 2015, 8:00 AM), http://www.prnewswire.com/news-releases/general-steels-jv-signs-letter-of-intent-to-deploy-rfid-based-logistics-management-at-tewoo-groups-seven-steel-coils-logistic-centers-300099727.html ("General Shengyuan IoT will upgrade Tewoo Group's logistic management system and integrate RFID technology, video monitoring, wire and wireless communications, and other information technologies for steel logistics management.").

7. John Garrity, *A 'Smart' Golf Ball to Track My Shots? Tell Me More!*, GOLF (Feb. 4, 2016), http://www.golf.com/equipment/smart-golf-ball-track-my-shots-tell-me-more ("Prazza—a Dutch company with roots in the lucrative field of commercial-vehicle tracking—devised a ball containing a miniature radio transmitter that sends a beeping sound to your handset.").

8. Jeremy Landt, *The History of RFID,* IEEE POTENTIALS, Oct.–Nov. 2005, at 8, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1549751&tag=1.

9. *See id.* at 9 (discussing the 1940s technological development that laid the groundwork for RFID).

10. Simon Hill, *Top Pet Trackers for Keeping Tabs on Your Furry Friends*, TECHRADAR (Jan. 27, 2016), http://www.techradar.com/news/world-of-tech/top-pet-trackers-for-keeping-tabs-on-your-furry-friends-1313560.

11. Andrew Brown, *Human Microchipping: An Unbiased Look at the Pros and Cons*, FREECODECAMP (July 27, 2016), https://medium.freecodecamp.org/human-microchipping-an-unbiased-look-at-the-pros-and-cons-ba8f979ebd96 ("Between 1.6–2.8 million youth run away from home each year. Being able to track anyone (that gives you permission to do so, of course!) at any time means peace of mind for millions of parents and caregivers across the country.").

and recently, employees in a workplace setting.[12] The implications of retrofitting workers with RFID implants have yet to be fully explored, but the potential impact on employees' ability to retain their privacy and ward off intrusions is massive[13]—indeed, employees' autonomy is undoubtedly minimized through the use of this technology.

This Note demonstrates that current legislation does not sufficiently address the risks presented by RFID body microchipping in the employment context. Part II provides a historical and contextual summary of the development of RFID, explains how RFID is used in the employment context, and provides an analysis of the benefits that use of RFID gives employers. Part II also provides a synopsis of the privacy risks associated with RFID technology. Part III focuses on the likelihood that the technology will gain further appeal among employers, highlights the concerns related to body microchipping, and analyzes the current state of legislation restricting body microchipping. Finally, Part IV proceeds in three parts. First, it outlines the approach that state and federal legislators should take in regulating body microchipping, suggesting that legislatures should flatly prohibit compulsory body microchipping in the employment context because of the potential for abuse by employers and criminal entities—like hackers. Second, it suggests that legislatures should restrict employers' ability to consider body-microchip status when making employment determinations for either potential or current employees. Finally, it proposes model legislation that state and federal governments could adopt. It also argues that employees should have the ability to make employment discrimination claims if they can show that employers have violated these laws; at the federal level, the Equal Employment Opportunity Commission ("EEOC") would manage discrimination claims, and at the state level, local state agencies would oversee these complaints.

## II. CHARTING RFID'S HISTORY FROM INCEPTION TO PRESENT

A review of RFID technology that traces the technology's history from inception to present application, with a description of RFID's associated privacy risks, is critical to determine how the law should react to concerns that arise with this technology's use. Sections A and B of this Part relate to how RFID emerged in the first half of the 20th century and chart the technology's development through the present. Section C informs the reader of RFID's

12. Jeff Baenen, *Wisconsin Company Holds 'Chip Party' to Microchip Workers*, CHI. TRIB. (Aug. 2, 2017, 7:32 AM), http://www.chicagotribune.com/bluesky/technology/ct-wisconsin-company-microchips-workers-20170801-story.html ("A brief sting is all employees of a Wisconsin technology company said they felt Tuesday when they received a microchip implant in their hand that will allow them to open doors, log onto computers or buy breakroom snacks by simply waving their hand.").

13. Joseph Jerome, *Embedded Chip on Your Shoulder? Some Privacy and Security Considerations*, INT'L ASS'N OF PRIVACY PROF'LS: PRIVACY PERSP. (Aug. 1, 2017), https://iapp.org/news/a/embedded-chip-on-your-shoulder-some-privacy-and-security-considerations (explaining how recent efforts to embed employees with RFID chips raise a host of privacy concerns).

applications in the public and private sector. Section D explains how employers began to use RFID to monitor their employees. Finally, Section E describes how some employers are now utilizing body microchipping, a more invasive form of RFID technology.

### *A. RFID, AN EARLY HISTORY*

RFID combines technologies used in radar and radio broadcasting, and the implementation of those monumental breakthroughs provides a lens into the development of RFID.[14] During World War II, warring forces struggled to identify the allegiance of aircraft on their radar systems—radar would merely detect the presence of planes but could not recognize if the aircraft was an enemy or an ally.[15] While German Air Force pilots solved this problem by rolling their planes in concert to signal their friendly status to German radar operators,[16] the Allies later deployed a more sophisticated version of radar labeled Identification Friend or Foe ("IFF"). IFF enabled communication between planes and radar operators on the ground.[17] By utilizing a beacon installed in the aircraft, it created a "long range transponder system[]"[18] to signal the identity of the aircraft to ground-based radar operators.[19] IFF served as a precursor to RFID and shared "the [same] basic requirements of most RFID systems today."[20]

Following the war, both the private and public sector were eager to explore further development and implementation of RFID technology. In 1948, Harry Stockman, a member of the U.S. Air Force Material Command, published a paper entitled *Communication by Means of Reflected Power*.[21] Stockman's essay is credited as one of the first works that explored RFID as a concept.[22] Although he hinted at the enormous potential of the technology, it would be some time before that potential would be realized: "Evidently considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored."[23] True to Stockman's

14. Landt, *supra* note 8, at 9.

15. DANIEL M. DOBKIN, THE RF IN RFID: UHF RFID IN PRACTICE 7 (2d ed. 2013).

16. *Id.*

17. *Id.* at 8.

18. C.M. Roberts, *Radio Frequency Identification (RFID)*, 25 COMPUTERS & SECURITY 18, 19 (2006).

19. DOBKIN, *supra* note 15, at 8.

20. *Id.* at 9.

21. *See generally* Harry Stockman, *Communication by Means of Reflected Power*, 36 PROC. INST. RADIO ENGINEERS 1196 (1948) (explaining point-to-point communication mechanisms, including RFID).

22. Landt, *supra* note 8, at 9.

23. Stockman, *supra* note 21, at 1204.

prescient words, the technological and theoretical infrastructure necessary to support widespread RFID use would not exist for another 30 years.[24]

The 1950s and 1960s saw increased discussions among researchers and scientists regarding the academic theory behind RFID. The end of this period also witnessed the development of RFID prototypes.[25] Major commercial and academic contributions from these decades include the limited introduction of tags used in retail stores as anti-theft devices[26] and R.F. Harrington's paper, *Theory of Loaded Scatterers*, which delved into the scientific theory and its potential application to RFID.[27] The 1970s ushered in an era of development and testing of early RFID technology and a heightened exploration of the technology's potential commercial and non-commercial uses. Examples of corporations that invested resources during this period to develop the technology include Raytheon, RCA, and Fairchild,[28] and industrial applications included "animal [tagging], vehicle tracking, and factory automation."[29] The public sector, led by The Port Authority of New York and New Jersey,[30] also began to test and utilize RFID systems designed for electronic toll collection.[31] The rapidly expanding interest in RFID technology foreshadowed its explosive growth.

### *B. THE 1980S AND 1990S—INCREASED ADOPTION OF RFID*

The 1980s signaled a turning point for RFID technology—RFID devices entered the mainstream and have not receded since. In that decade, RFID spread to highway tolls, smart ID cards, and expanded further into animal tracking.[32] These applications drove considerable interest in developing RFID to control personnel access to workplaces.[33] The availability of personal computers ("PCs") also contributed to the dramatic rise in the popularity of RFID. PCs provided an apt mechanism for collecting and managing the data that RFID devices would produce. As a result, more users were able to take advantage of RFID's many potential applications by merging tagging

24. Landt, *supra* note 8, at 9.

25. *Id.*; Roberts, *supra* note 18, at 18–19.

26. Roberts, *supra* note 18, at 18–19.

27. *See* Roger F. Harrington, *Theory of Loaded Scatterers,* 111 PROC. INSTITUTION ELECTRICAL ENGINEERS 617, 621–22 (1964).

28. LI YANG ET AL., DESIGN AND DEVELOPMENT OF RADIO FREQUENCY IDENTIFICATION (RFID) AND RFID-ENABLED SENSORS ON FLEXIBLE LOW COST SUBSTRATES 2 (Amir Mortazawi ed., 2009), https://www.morganclaypool.com/doi/pdf/10.2200/S00172ED1V01Y200905MRF001.

29. Landt, *supra* note 8, at 9.

30. The Port Authority of New York and New Jersey "builds, operates, and maintains critical transportation and trade assets. . . . [T]hroughout the New York/New Jersey region." THE PORT AUTHORITY OF N.Y. & N.J., http://www.panynj.gov (last visited Oct. 6, 2018).

31. Landt, *supra* note 8, at 9.

32. *Id.* at 10.

33. *Id.*; *see also infra* Section II.D.1 (providing an in-depth explanation of this application of RFID).

technology with PCs.[34] Other technical advancements decreased the physical size of tags and proportionally increased the adaptability of RFID devices to more commercial applications.[35] Both the public and private sectors could now use tags to track moving objects with relative ease, which reduced reliance on more cumbersome and inaccurate tracking systems.[36]

The 1990s saw continued expansion of RFID and adoption of the technology by more commercial and government entities.[37] In particular, RFID transformed North American transportation infrastructure.[38] Over three million tags were installed on rail cars in North America, electronic tolling systems with RFID technology were introduced in Oklahoma, Texas, Kansas, and Georgia, and the E-Z Pass Interagency Group was formed to create a regional electronic toll collection system.[39] RFID technology continued to advance as well. Now, a single RFID tag could be used with multiple RFID reader devices, thus allowing one tag to have multiple uses, such as the ability to pay tolls and access parking structures.[40] Ultra-high frequency RFID systems were introduced into the market, offering "longer read range and faster data transfer."[41] In the late 1990s, further technical advancements led to the capability to store unique serial numbers within RFID system databases.[42] This development created tag tracking ability,[43] which revolutionized business—for the first time, businesses could track individual goods and merchandise through their supply chains, allowing for greater efficiency by creating more visibility and control.

34. Mohamed K. Watfa et al., *RFID Applications in E–Healthcare*, *in* E-HEALTHCARE SYSTEMS AND WIRELESS COMMUNICATIONS: CURRENT AND FUTURE CHALLENGES 70, 73 (Mohamed K. Watfa ed., 2012).

35. Landt, *supra* note 8, at 10.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.* This technology was successfully implemented, for instance, in Texas:

> In the Dallas–Ft. Worth metroplex, a first was achieved when a single TollTag on a vehicle could be used to pay tolls on the North Dallas Tollway, for access and parking payment at the Dallas/Ft. Worth International Airport, the nearby Love Field [Airport], and several downtown parking garages as well as access to gated communities and business campuses.

*Id.*

41. YANG ET AL., *supra* note 28, at 3.

42. *Id.*

43. *Id.*

### *C. RFID IN THE 21ST CENTURY*

The modern era of RFID has seen massive growth of the technology with new and innovative uses of tagging too extensive to be covered by this Note.[44] Notable progressions include technical innovations, expanded public and private interest, development of industry standards, as well as deeper and broader research aimed at augmenting RFID's current capabilities.[45] One of the most remarkable technical innovations of this century is the continued reduction of RFID tag size. Presently, some RFID tags are virtually unnoticeable to the human eye.[46] Tags can now be small stickers on car windows,[47] human body implants the size of a grain of rice,[48] and hair-sized inserts that can be placed in currency (although no country is known to have embedded RFID chips within their currency at this time).[49] This Section includes a description of the increased availability of tags, which has led retailers and the government to integrate RFID technology into their supply chains and businesses more broadly. Additionally, this Section describes the creation and adoption of industry-wide RFID standards and examines concerns related to the future uses of RFID technology.

#### 1. Retailer Use of RFID in the 21st Century

During the current century, RFID use by commercial retailers has expanded to a global level, and the functions that tagging serve have become increasingly diverse. Walmart's RFID program provides an example of some of the technology's limitations which stunted the widespread rollout of RFID

---

44. For a more extensive analysis of RFID technology, see generally KLAUS FINKENZELLER, RFID HANDBOOK: FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS, RADIO FREQUENCY IDENTIFICATION AND NEAR-FIELD COMMUNICATION (Dörte Müller trans., 3d ed. 2010) (offering a complete overview of RFID technology for end-users and practitioners).

45. *See, e.g.*, Helen Coffey, *Swedish Commuters Can Use Futuristic Hand Implant Microchip as Train Tickets*, INDEPENDENT (June 16, 2017, 2:35 PM), http://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html; Megan Greenwalt, *How RFID Technology Is Evolving in the Waste and Recycling Industry*, WASTE 360 (Oct. 4, 2017), http://www.waste360.com/fleets-technology/how-rfid-technology-evolving-waste-and-recycling-industry; Claire Swedberg, *IoT Aims to Track Free-Ranging Reindeer in Finland*, RFID J. (Jan. 19, 2018), https://www.rfidjournal.com/articles/pdf?17106.

46. *Hitachi Unveils Smallest RFID Chip*, RFID J. (Mar. 14, 2003), https://www.rfidjournal.com/articles/pdf?337.

47. Landt, *supra* note 8, at 11.

48. Jena McGregor, *Some Swedish Workers Are Getting Microchips Implanted in Their Hands*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-implanted-in-their-hands (describing the choice by some workers "to have a chip the size of a grain of rice implanted in their bodies").

49. *RFID Frequently Asked Question: Can RFID Be Embedded in Money?*, RFID J., https://www.rfidjournal.com/faq/show?29 (last visited Oct. 18, 2018).

in the 2000s.[50] In 2003, Walmart announced that its suppliers would be required to adopt RFID in the near future to continue their relationships with the retail giant.[51] However, the effort was abandoned in 2009 due to cost sensitivities (barcodes were still a cheaper alternative) and practical obstacles which limited the use of RFID.[52] Despite Walmart's initial lack of success, there have been calls for the retailer to wholeheartedly adopt a tagging system and apply the technology to help resolve the company's persistent inventory management problems.[53]

Other retailers have had more success implementing RFID. In 2016, Macy's announced plans "to track every item across its fleet of stores and fulfillment centers by the end of 2018."[54] According to Macy's executives, RFID implementation has resulted in "both financial and operating gains" for the retail giant.[55] Undoubtedly, the dramatic drop in the cost of tagging technology contributed to Macy's decision to adopt it—"a[n] RFID tag was priced at about $1 in 2003, and is roughly 10 cents today."[56]

Macy's use of RFID is intriguing for two reasons. First, Macy's has recently experienced financial difficulties and has made substantial efforts to improve its economic position.[57] RFID can be used to pinpoint the location of products and drive those products into the hands of customers faster. This technology, which has become increasingly affordable, is likely to help the company's bottom line and may play a non-negligible role in returning the company to financial health. In an era where large department stores are struggling

50. Paula Rosenblum, *How Walmart Could Solve Its Inventory Problem and Improve Earnings*, FORBES (May 22, 2014, 11:59 AM), https://www.forbes.com/sites/paularosenblum/2014/05/22/walmart-could-solve-its-inventory-problem-and-improve-earnings.

51. *Id.*

52. *Id.* The radio frequencies needed for RFID to function did not "pass through liquids and metal well." Currently, RFID is still hampered by the presence of liquids and metals. For a more detailed discussion on this issue, see M. Periyasamy & R. Dhanasekaran, *Assessment and Analysis of Performance of 13.56 MHz Passive RFID in Metal and Liquid Environment*, 2014 INT'L CONF. ON COMM. & SIGNAL PROCESSING 1122, 1124 (finding that proximity to different metals and liquids, such as copper, affected RFID performance).

53. Rosenblum, *supra* note 50. The author describes the problems Walmart faces: "[T]he company lost $3 billion in 2013 sales due to out of stock merchandise while its inventory grew at a faster rate than its sales." *Id.*

54. Barbara Thau, *Is the 'RFID Retail Revolution' Finally Here? A Macy's Case Study*, FORBES (May 15, 2017, 8:45 AM), https://www.forbes.com/sites/barbarathau/2017/05/15/is-the-rfid-retail-revolution-finally-here-a-macys-case-study.

55. *Id.*

56. *Id.*

57. *See, e.g.*, Rachel Abrams & Sapna Maheshwari, *Macy's to Close 100 Stores as E-Rivals and Discounting Hit Legacy Retailers*, N.Y. TIMES (Aug. 11, 2016), https://www.nytimes.com/2016/08/12/business/macys-q2-earnings-store-closings.html; Michael Corkery, *Grand Buildings Help Keep Macy's Afloat*, N.Y. TIMES (Nov. 22, 2017), https://www.nytimes.com/2017/11/22/business/macys-retail-real-estate.html; Michael Corkery, *Macy's Sales Keep Dropping, and Investors Are Unforgiving*, N.Y. TIMES (Aug. 10, 2017), https://www.nytimes.com/2017/08/10/business/dealbook/macys-stock-price-sales-decline.html.

(Sears,[58] JCPenney,[59] and Bon-Ton Stores[60] for example) to compete effectively with nimbler online retailers, such brick-and-mortar businesses might consider widespread adoption of RFID to stem their declines. Furthermore, massive retailers like Macy's have significant influence over their suppliers; in fact, Macy's decision to adopt RFID technology has already pushed some suppliers to implement the technology.[61] Macy's example suggests that large retailers who equip their supply chains with RFID may have a ripple effect and cause other suppliers to consider the technology.

### 2. The Public Sector's Use of RFID in the 21st Century

The public sector has also embraced the utility of RFID technology, adapting chipping to its needs. In 2003, the Department of Defense ("DoD") announced it would require suppliers to adopt RFID technology by 2005.[62] DoD has since narrowed its RFID implementation plan to require tags from only those specific supplies or suppliers that DoD views as necessitating RFID tags. DoD suppliers required to utilize RFID technology meet three criteria: (1) they have entered into contracts with provisions that require RFID technology; (2) they supply equipment which falls under a class of supply where DoD requires tagging; and (3) the equipment is being supplied to an RFID-enabled DoD location.[63] DoD's RFID plan has allowed the Department to reap the benefits of tagging technology while avoiding the cost of immediate widespread implementation.

---

58. *See* Michael Corkery, *Sears, the Original Everything Store, Files for Bankruptcy*, N.Y. TIMES (Oct. 14, 2018), https://www.nytimes.com/2018/10/14/business/sears-bankruptcy-filing-chapter-11.html.

59. Chris Isidore, *JCPenney Warns: Losses Are Growing*, CNN (Oct. 27, 2017, 12:06 PM), http://money.cnn.com/2017/10/27/news/companies/jcpenney-losses/index.html.

60. Laura J. Keller & Lauren Coleman-Lochner, *Bon-Ton is Preparing for Bankruptcy*, BLOOMBERG (Feb. 1, 2018, 6:31 PM), https://www.bloomberg.com/news/articles/2018-02-02/bon-ton-is-said-to-prepare-bankruptcy-as-rescue-plan-collapses.

61. Carrie Brunner, *Mojix Brings Innovative Blockchain Solution to Auburn University RFID Lab Project Zipper*, NB HERARD (Jan. 12, 2018), http://nbherard.com/business/mojix-brings-innovative-blockchain-solution-to-auburn-university-rfid-lab-project-zipper. One such supplier, prompted by Macy's, implemented RFID across its operation:

> Last year, Macy's announced plans to expand the use of RFID to track every item across its fleet of stores and fulfillment centers by the end of 2018. Herman Kay, a leading manufacturer of coats and outerwear for women and men, and a key supplier to Macy's, has implemented RFID at every step of their internal fulfillment process—optimizing operations and increasing internal confidence levels that the right garments, in the right sizes and colors, have been delivered to the right customers.

*Id.*

62. Roberts, *supra* note 18, at 21.

63. *RFID Supplier Info & FAQs*, OFF. ASSISTANT SEC'Y DEF. FOR LOGISTICS & MATERIAL READINESS, http://www.acq.osd.mil/log/sci/rfid_FAQs.html (last visited Oct. 18, 2018).

The universality and advantages of RFID are nowhere as apparent as in the United States Army. In addition to requiring some suppliers to utilize RFID technology, DoD has published an information guide for RFID suppliers to familiarize themselves with the Department's RFID requirements. Within this guide, DoD lists the numerous benefits of RFID implementation: "RFID technology . . . enables automated data capture, resulting in efficient recording of material. RFID technology will facilitate . . . realization of business benefits in the areas of inventory management and visibility, operational improvements, shrinkage and asset tracking."[64] DoD summarizes the benefits of RFID by stating that it views the technology "as a means to facilitate accurate, automated data capture in support of business processes in an integrated DoD supply chain enterprise."[65] Authors have also noted the extensive benefits of RFID technology when applied in a military setting. "A major benefit of RFID . . . is the ability for faster read rates—particularly when the items are embedded, hard to reach or enclosed in a container. All of these scenarios are typical operating or storage conditions for the military."[66]

### 3. Development of RFID Standards

As RFID technology became increasingly refined, organizations and bodies concerned with the technology began to emerge and draft standards for its design and use. In 1999, international organizations and private corporations joined forces to establish the Auto-ID Center at MIT.[67] The Auto-ID Center was organized "to bring together RFID manufacturers, researchers, and users to develop standards, perform research, and share information for supply chain applications."[68] The work at the Auto-ID Center led to the creation of the Electronic Product Code ("EPC") and EPCglobal.[69] The EPC "is a universal identifier that gives a unique identity to a specific physical object."[70] Thus, "EPCs are encoded on RFID tags [and] can be used to track all kinds of objects."[71] EPCglobal is an "initiative to innovate and develop industry-driven standards for the [development of EPC] to support the use of [RFID]."[72] EPCglobal focuses on developing industry standards for the use of EPC, and "covers global e-business communications standards, numbering

64. U.S. DEP'T OF DEF., UNITED STATES DEPARTMENT OF DEFENSE SUPPLIERS' PASSIVE RFID INFORMATION GUIDE VERSION 15.0, at 6, https://www.acq.osd.mil/log/SCI/.AIT.html/DoD_Suppliers_Passive_RFID_Info_Guide_v15update.pdf (last visited Oct. 18, 2018).

65. *Id.* at 8.

66. Peter Collins, *The Next Big App for the Military: RFID*, RFID J. (June 4, 2017), http://www.rfidjournal.com/articles/view?16195/2.

67. YANG ET AL., *supra* note 28, at 3.

68. Landt, *supra* note 8, at 11.

69. Roberts, *supra* note 18, at 19, 22.

70. *EPC Information*, EPC-RFID INFO, https://www.epc-rfid.info (last visited Oct. 18, 2018).

71. *Id.*

72. *EPCglobal*, GS1, https://www.gs1.org/epcglobal (last visited Oct. 18, 2018).

schemes, uniqueness management, and bar code symbology standards."[73] EPCglobal's standardization of RFID technology provided the burgeoning industry with a platform to continue developing and implementing the technology at a worldwide level.

### 4. Concerns Related to RFID in the 21st Century

Recent literature on RFID has identified potential issues that will need to be addressed as RFID's footprint widens. Privacy and security concerns are the central issues dominating the current debate.[74] The American Civil Liberties Union ("ACLU") has advocated for restrictions on the use of RFID with regards to its privacy and safety implications.[75] In one recent example reflecting the technology's safety risks, the ACLU objected when Contra Costa County, California, schools began outfitting preschoolers with RFID-equipped jerseys to help track those preschoolers' whereabouts.[76] Nicole Ozer, the Technology and Civil Liberties Director for the ACLU of California, discussed some of the potentially serious repercussions the jerseys could lead to: "Someone who wants to do children harm could . . . . cop[y the tag information] easily to [create] a duplicate chip. A child could be taken off campus while the duplicate chip continues to tell RFID readers that the child is safely at school."[77]

The criticisms that privacy and civil liberty advocates have lodged against RFID technology can be grouped into five generalized themes. First, the concealed nature of some tags: "RFID tags can be embedded into/onto objects and documents without the knowledge of the individual who obtains those items."[78] Second, the ability to mass-identify objects: "The use of unique ID numbers could lead to the creation of a global item registration system in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer."[79] Third, the ability to collect massive amounts of data: "[Databases with tag data] could be linked with personal identifying data, especially as computer memory and processing capacities expand."[80] Fourth, the opportunity to track and profile individuals: "If personal identity

73. Roberts, *supra* note 18, at 22.

74. C. Mutigwe & F. Aghdasi, *Research Trends in RFID Technology*, 6 INTERIM: INTERDISC. J. 68, 69, 71–72 (2007), https://journals.co.za/docserver/fulltext/interim/6/1/112.pdf.

75. For an overview of the ACLU's stance on RFID, see *RFID Chips*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/rfid-chips (last visited Oct. 18, 2018).

76. Nicole Ozer, *Don't Let Schools Chip Your Kids*, ACLU (Sept. 1, 2010, 11:03 AM), https://www.aclu.org/blog/dont-let-schools-chip-your-kids.

77. *Id.*

78. *RFID Position Statement*, ACLU, https://www.aclu.org/other/rfid-position-statement (last visited Oct. 18, 2018) ("As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.").

79. *Id.*

80. *Id.*

were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent."[81]

Finally, the limited visibility of some tag readers has created privacy concerns: "Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate."[82] Critics of the technology have not exaggerated their worries associated with RFID. Indeed, some of these concerns have also been expressed as the technology's primary attribute —"[t]he main feature of RFID technology is its ability to identify, locate, track, and monitor people and objects without a clear line of sight between the tag and the reader."[83]

### *D. RFID's Application in the Workplace and Employee Monitoring*

RFID use within businesses has expanded beyond tracking goods and supply chains. Employers are now using the technology to monitor employees. Access cards utilizing RFID technology grant employees entry to the workspace. RFID has also been adapted to ensure the safety of employees working in dangerous conditions.[84] Other uses include recording and reviewing employee productivity. Finally, vehicles and employees outside of the workplace are also subject to RFID monitoring.

This Section discusses the emergence of RFID—first, as a device to secure entry and exit into the physical workspace; second, as a means to create a safer work environment in hazardous conditions; and third, as a tool for tracking employee productivity. Lastly, this Section illustrates the uses of RFID as a means to track employees outside of the physical workspace.

#### 1. RFID as a Tool to Access the Workplace

Businesses were some of the initial adopters of RFID technology. In fact, personnel access to worksites was one of the earliest applications of tagging.[85] A common example of RFID tagging in a professional setting is the use of employee access cards. Employee access cards enable employers to monitor the movements of their employees and secure offices from potential intruders or designate sections of offices inaccessible to certain employees.[86]

---

81. *Id.* ("For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies.").

82. *Id.* ("RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being 'scanned.'").

83. HUNT ET AL., *supra* note 1, at xiv.

84. *See infra* Section II.D.2.

85. Landt, *supra* note 8, at 10.

86. Ron Fiedler, *ID Badges Can Do More Than You Think*, ROCKWELL AUTOMATION: J. 23, 24, https://www.rfideas.com/files/downloads/docs/TheJournal_ID_Badges_Do_More_Than_You

Employee access cards function by programming a reader to read the access cards which then interfaces with software that verifies the information in the employee database.[87] However, employers' use of RFID technology in the workplace has not been without controversy.[88] While worksite access via RFID technology has been implemented with little media coverage, controversy has resulted from employers' expansion of RFID use into other spheres.

### 2. Application of RFID to Employee Safety

RFID monitoring of workers has two underlying rationales—employee safety and employee productivity. This Section discusses the former's rationale, while the following Section analyzes the latter's. PervCom Consulting's RFID system, PervTrack, is an example of RFID technology being utilized to improve employee safety—the system tracks people, assets, and changing environmental conditions.[89] Mining companies have adopted systems similar to PervTrack to track their workers while they work in mines and to ensure the safety of the work environment by tracking environmental conditions.[90] Similarly, recent patent filings have revealed that Amazon is considering implementing RFID technology to track its warehouse workers.[91]

The patents cover a "wristband and receiver system" and "would rely on radio frequencies or ultrasonic pulses to monitor the device's specific location."[92] The technology "would use haptic feedback . . . to alert a [warehouse] worker that they are in the wrong location, or guide them to the right one."[93] One author describes the alerts the devices would send as "an

---

_Think_2015.pdf. (last visited Sept. 6, 2018) ("With an RFID-enabled badge reader, the employee's ID is sent to application software that verifies it against an employee database on the network."). ID badges are used to quickly verify and admit staff to appropriate areas:

> When employees tap their existing ID badge against the reader, that employee's ID is scanned and sent to the application software that quickly verifies it against an employee database on the network. Depending on the system, which can include training, certification, access privileges, and other authentications, the qualified employee will be authorized to proceed to complete his or her task.

*Id.* at 23.

87. Landt, *supra* note 8, at 8.

88. *See infra* Sections II.D.3–.4, II.E.

89. Dave Friedlos, *Indian Mine Monitors Workers and Toxic Gases*, RFID J. (Sept. 5, 2008), http://www.rfidjournal.com/articles/view?4310. For an additional example of a similar system see *Personnel & Asset Tracking and Tagging in Underground Hard Rock Mines*, MINE SITE TECHS., http://mstglobal.com/solutions/asset-people-tracking/underground-hard-rock (last visited Oct. 23, 2018).

90. *Id.*

91. Camila Domonoske, *Wrist Watching: Amazon Patents System to Track, Guide Employees' Hands*, NPR (Feb. 1, 2018, 2:03 PM), https://www.npr.org/sections/thetwo-way/2018/02/01/582370715/wrist-watching-amazon-patents-system-to-track-guide-employees-hands.

92. *Id.*

93. *Id.*

invisible slap, so to speak[, g]entle, but a slap nonetheless."[94] While Amazon's system is still in an early stage, there are examples of RFID employee tracking programs which are already in place.

Sociometric Solutions, now rebranded as Humanyze, markets "sensors [which are] placed in employee identification badges that gather real-time information to help companies measure productivity." [95] The sensors are based on RFID technology, but also serve as tracking and recording devices —they identify a person's tone of voice, movement and even their posture when communicating with others. The sensors' data translates into actionable items for employers. Bank of America adopted the sensors in their call centers and realized that providing employees with overlapping lunches would lead to some positive results:

> Network cohesiveness, which measures how well [employees] communicate[,] went up 18 percent. This reduced stress (as measured by tone of voice) by 19 percent. All of this led to happier employees and lower turnover rates, which went down 28 percent. The key metric though, call completion time improved by 23 percent. These are numbers that on a scale of Bank of America could translate into billions in savings.[96]

Despite the potential cost savings of monitoring employees with RFID technology, its application violates what had previously been a private sphere of an employee's existence, and "companies . . . must balance the business interests of the company with the reasonable expectations of privacy of its employees."[97] In fact, Humanyze's sensor program acknowledges worries over intrusions to personal privacy—the program is designed to anonymize the individual information that it collects. Instead of providing the company with specific data about individuals, the program provides metadata to employers

94. Dom Galeon, *Amazon Patents Tracking Wristbands That Spy on Warehouse Workers*, FUTURISM (Feb. 2, 2018), https://futurism.com/amazon-patents-tracking-wristbands-spy-warehouse-workers.

95. Vivian Giang, *Companies Are Putting Sensors on Employees to Track Their Every Move*, BUS. INSIDER (Mar. 14, 2013, 6:23 PM), http://www.businessinsider.com/tracking-employees-with-productivity-sensors-2013-3.

96. Ron Miller, *New Firm Combines Wearables and Data to Improve Decision Making*, TECHCRUNCH, https://techcrunch.com/2015/02/24/new-firm-combines-wearables-and-data-to-improve-decision-making (last visited Oct. 24, 2018) (noting that a key indicator of a call worker's productivity was the extent to which the call workers would talk to one another, because the "employees shared information and techniques," resulting in a corresponding increases in measures of productivity).

97. *Managing Workplace Monitoring and Surveillance*, SOC'Y FOR HUM. RESOURCE MGMT., https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx (last visited Oct. 24, 2018) ("Employers also have a duty to their employees to protect the privacy and confidentiality of the personal information gathered and maintained in the course of employment.").

to make recommendations about how the company as a whole can operate more efficiently.[98]

### 3. GPS Tracking and its Application to RFID Employee Tracking Beyond the Office

In recent examples, Global Positioning System ("GPS") technology has been merged with tagging technology to enable employers to expand the reach of their employee monitoring beyond the traditional four walls of an office. Employers now utilize GPS technology installed in employer-assigned vehicles or cell phones to track employees' locations.[99]

Although not all GPS devices contain tagging technology, GPS technology is compatible with RFID technology. Indeed, employer monitoring of employee movements is on the rise. In a study conducted by The Aberdeen Group, a market intelligence company,[100] it was noted that "in 2008 . . . 30% of organizations had invested in fleet management and vehicle tracking tools"; however, that number had more than doubled in 2012, when "62% of [organizations] indicated that they were currently monitoring at least a proportion of their service vehicles remotely."[101] Experts have also discovered that "[c]ompanies are increasingly requiring staff to consent to GPS phone tracking."[102] The increased employer control from GPS monitoring suggests that this type of surveillance is unlikely to be curtailed without significant public pressure or legislative involvement.

---

98. Giang, *supra* note 95 ("The sensors are intended to measure when and how employees are truly productive. While individual information is collected, it's anonymized to provide metadata and hedge against privacy concerns. The information is then used to suggest how employees, and the company as a whole, can work more efficiently.").

99. Nicole Lyn Pesce, *5 Ways Your Employer Is Tracking You*, MONEYISH (July 25, 2017), https://moneyish.com/ish/5-ways-your-employer-is-tracking-you.

100. ABERDEEN, https://ww.aberdeen.com (last visited Oct. 24, 2018).

101. SUMAIR DUTTA, ABERDEEN GROUP, FIELD SERVICE 2012: GPS AND FLEET MANAGEMENT 1 (2012), http://www.teletrac.com/teletrac.com/assets/aberdeen-%20research-%20pack.pdf.

102. Walaika Haskins, *Who's Watching You at Work*, TECHNEWSWORLD (Apr. 14, 2008, 6:00 AM), https://www.technewsworld.com/story/62528.html (quoting Simon Davies, director at Privacy International). For more evidence of this trend, see Sally F. Barron, *Monitoring Employees in the Modern Workplace – Can a GPS Result in TMI?*, HR PROFS. MAG., http://hrprofessionalsmagazine.com/monitoring-employees-in-the-modern-workplace-can-a-gps-result-in-tmi (last visited Oct. 24, 2018). The article describes one example of a dispute over GPS monitoring that went to litigation:

> In the *Cunningham* case, the New York Department of Labor attached a GPS to the employee's car, without the employee's knowledge, because it suspected the employee of submitting false time reports; naturally, the GPS seemed an effective way to accurately determine whether the employee was at his office during the times he claimed or, as suspected, having an out-of-office rendezvous with his secretary.

*Id.* The New York Court of Appeals held in *Cunningham* that the GPS tracking at issue, which was conducted by the state Inspector General, was unreasonable and thus violated the state and federal constitutions, requiring that the evidence be suppressed in a subsequent employee discipline hearing. Cunningham v. N.Y. State Dep't of Labor, 997 N.E.2d 468, 472–74 (N.Y. 2013).

Employers' desires to track employees through GPS technology reflects the expanding scope of employer monitoring, which is showcased by the monitoring treatment telecommuting workers receive. Some workers who telecommute from off-site locations are monitored by their employers through applications that do not incorporate RFID technology.[103] Employers can easily review their employees' activity through various means, including software that tracks employees' keystrokes and mouse movements or web applications that track overall employee productivity based on desktop application and website usage.[104] Monitoring of employees who telecommute has resulted in noticeable gains in productivity in many instances.[105] In one such case, the amount of time that telecommuting employees of an insurance provider spent away from their computer was reduced "immediately and dramatically" after the employer informed the employees that they were being monitored.[106] While the type of technology used to track telecommuting workers does not employ RFID tagging, it is emblematic of the general trend of increased employer surveillance of employees—a trend that has tremendous implications for the use of RFID in the workspace.

Traditional temporal, locational, and practical limits on employer monitoring of employee activities have slowly disintegrated. Physical and logistical barriers that previously would have prevented employers from tracking employee movements and actions outside of the workplace no longer

---

103. Haskins, *supra* note 102 ("[O]ff-site workers who telecommute can be monitored—even though they may be working on a personal device—simply because they are using the network provided by the employer.").

104. Cynthia Boris, *3 Web Tools for Managing Employees Who Work from Home*, ENTREPRENEUR (June 13, 2013), https://www.entrepreneur.com/article/226996. Employers have various software tools they may elect to use to monitor telecommuting workers. "For business owners who prefer a less heavy-handed approach, there's MySammy. This application is all about balance. As long as an employee's bar graph is mostly green (active) you can forgive the 10 percent that's red (non-productive.)" *Id.* Another example allows more extensive monitoring. "If you need more detail, there's Worksnaps. This tool takes screenshots every 10 minutes and logs keyboard strokes and mouse movement." *Id.* For a list of more examples of types of monitoring software, see *How to Monitor Employees Who Telecommute*, PRESS8 TELECOM, https://www.press8.com/monitor-employees-telecommute (last visited Oct. 24, 2018) (listing some ways in which employers can monitor telecommuting employees, including "[b]lock selected Internet sites and limit access to other sites[;] [m]onitor websites visited and how long telecommuters are on certain sites[;] [c]ollect computer screenshots for 'real-time' updates on project status").

105. Allison Linn, *Working from Home? Boss May Be Peeking Over Your Shoulder*, CNBC (June 19, 2013, 11:14 AM), https://www.cnbc.com/id/100826081.

106. *Id.* Employee productivity immediately followed from employer monitoring of telecommuting employees:

> In the first few months [the telecommuting employees] were monitored . . . researchers found that the home-based workers did have more idle time . . . than their office-based colleagues. Then, the employer told the workers that they were being monitored. The home-based workers' idle time fell immediately and dramatically, while the office-based workers idle time stayed relatively steady.

*Id.*

exist. Not only has employee monitoring increased, but the consequences that result from employee monitoring have become more severe. The Electronic Monitoring & Surveillance Survey produced in 2007 noted that 66% of employers monitor internet connections,[107] 28% of employers have fired employees for e-mail misuse,[108] and 30% of employers have fired employees for internet misuse.[109] Despite the increasingly harsh repercussions, all indicators suggest that monitoring activity will continue to grow as technological advancements provide for additional tracking abilities and industry awareness of the technology grows.

### *E. RFID Body Microchip Implants and Their Use in the Workspace*

Technical advancements have dramatically increased the scope of monitoring capabilities. Some commentators have noted that "[t]he potential number of [RFID] workplace uses—not to mention off-site uses—is limited only by an employer's lack of imagination."[110] The latest and perhaps most controversial use of RFID in the workplace is embedding an RFID tag underneath an employee's skin, also known as a body microchip or human microchip implant.[111]

#### 1. Early Body Microchip Implant Uses

The early years of the 21st century marked the first instance of body microchipping.[112] A South Florida family with a history of medical ailments elected to have Applied Digital Solutions, a corporation that specializes in microchips, insert the microchips into their bodies.[113] The family was hopeful that if they found themselves in a medical emergency, emergency technicians would be able to scan the chip in their body and access important data quickly,

107. AMA/ePOLICY INST. RES., 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 1 (2007), http://www.plattgroupllc.com/juno8/2007ElectronicMonitoringSurveillanceSurvey.pdf ("Employers are primarily concerned about inappropriate Web surfing, with 66% monitoring Internet connections.").

108. *Id.* at 8.

109. *Id.* at 9.

110. Marisa Anne Pagnattaro, *Getting Under Your Skin—Literally: RFID in the Employment Context*, 2008 U. ILL. J.L. TECH. & POL'Y 237, 238.

111. Mary Bowerman, *Wisconsin Company to Install Rice-Sized Microchips in Employees*, USA TODAY (July 24, 2017, 7:46 AM), https://www.usatoday.com/story/tech/nation-now/2017/07/24/wisconsin-company-install-rice-sized-microchips-employees/503867001.

112. Dan Collins, *Fla. Family Takes Computer Chip Trip*, CBS NEWS (May 10, 2002, 12:32 PM), https://www.cbsnews.com/news/fla-family-takes-computer-chip-trip ("The [Jacobs] family became the first to be implanted with tiny computer chips that researchers hope will advance the way people carry medical information with them in case of emergencies.").

113. *Id.* (explainining that the husband in the family "ha[d] suffered through cancer, a car crash, a degenerative spinal condition, chronic eye disease and abdominal operations. His injuries have forced him to quit his dental practice").

which might save their lives.[114] The data stored on the chip consisted of "telephone numbers and information about previous medications."[115] At the time, the Food and Drug Administration ("FDA") declared that it would not regulate the chips, provided the chips did not contain any medical data.[116] Subsequently, in 2004, the FDA gave Applied Digital Solutions permission to market the chips to the public.[117] When the FDA made its announcement, approximately 1,000 individuals globally had adopted the use of body microchipping technology.[118]

Following application of body chipping to private citizens with unique needs,[119] the public sector embraced the technology. In 2004, Mexican government officials took an interest in RFID body microchips and implanted the microchips in a select group of approximately 160 individuals.[120] According to officials, the body microchip was to be used exclusively for access to "a new federal anti-crime information center" and to "provide more certainty about who accessed sensitive data at any given time."[121] In addition to the Mexican government officials who received implants, it has been rumored that "the country's military and police are reportedly next in line for

114. *Id.* ("It's great what [the chip] can do, it can save a lot of lives, including my dad's because he has a lot of medical problems and I want him to be around for a while . . . ." (quoting Derek Jacobs, then age 14)).

115. *Id.*

116. *Id.* ("The Food and Drug Administration said in April that it would not regulate the implant as long as it contains no medical data. Company officials said they were free to proceed because the implant contains identification numbers that correspond to personal medical information in a separate database.").

117. *FDA Approves Computer Chip for Humans*, NBC NEWS (Oct. 13, 2004, 6:38 PM), http://www.nbcnews.com/id/6237364/ns/health-health_care/t/fda-approves-computer-chip-humans ("The Food and Drug Administration said Wednesday that Applied Digital Solutions of Delray Beach, Fla., could market the VeriChip, an implantable computer chip about the size of a grain of rice, for medical purposes.").

118. *Id.* (noting that at the time the article was published in October 2004, "just 1,000 people across the globe have had the devices implanted, very few of them in the United States").

119. Recently, the possibility of widespread application of RFID technology for medical and other purposes has been suggested: "RFID tagging could become the base of vast, sensor-driven networks, taught to detect not only health-related changes in a body, but chemicals such as carbon monoxide, or ammonia." Charlie Osborne, *RFID Tags Transformed to Become Detectors of Chemicals and Disease*, ZDNET (June 14, 2018, 10:55 AM), https://www.zdnet.com/article/rfid-tags-transformed-to-become-detectors-of-chemicals-and-disease.

120. Will Weissert, *Microchips Implanted in Mexican Officials*, NBC NEWS (July 14, 2004, 9:21 PM), http://www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials ("Security has reached the subcutaneous level for Mexico's attorney general and at least 160 people in his office—they have been implanted with microchips that get them access to secure areas of their headquarters.").

121. *Id.*; *see also* Kevin Sullivan, *Mexican Official has Microchip Put in Arm*, CHI. TRIB. (July 16, 2004), http://articles.chicagotribune.com/2004-07-16/news/0407160200_1_rafael-macedo-mexican-distributor-jose-antonio-ortega ("The chips also function as an electronic identification that grants [Mexico's attorney general] and about 160 of his lieutenants access to a suite of offices on the third floor of the attorney general's headquarters, which houses a state-of-the-art, $30 million computerized database of crime . . . .").

chipping."[122] Outside of Mexican government officials, private entities have also expressed an interest in marketing microchip implants to citizens concerned about the child kidnapping threat in Mexico. In 2003, Solusat, a Mexican company, "launched a service to implant microchips in children as an anti-kidnapping device."[123] The program hoped to foil potential abductions of children and "garnered the backing of Mexico's National Foundation of Investigations of Robbed and Missing Children, which . . . agreed to promote the service."[124]

An additional example of early body microchipping appeared in Europe in 2004. Patrons of a Barcelona nightclub, Baja Beach Club, were "offer[ed] . . . the opportunity to have a syringe-injected microchip implanted in their upper arms that not only g[ave the patrons] special access to VIP lounges, but also act[ed] as a debit account from which they [could] pay for drinks."[125] Patrons who elected to receive the implants would benefit from no longer needing to carry wallets or purses to pay for drinks.[126]

Baja Beach Club, the Mexican government, and Solusat's microchipping programs served as early examples of inserting RFID chips in bodies, but their scope was quite limited in comparison to the full potential of RFID implementations. Subsequent usage of body microchipping has seen an increase of applications, particularly in the employment context.

### 2. Expansion of Body Microchipping to Employees

While RFID usage is booming and expanding, human microchip implants have not yet reached a level of widespread appeal or acceptance, and the employment context is no exception. There have been limited reports of employers making body microchips available to their employees, although a few examples have surfaced. NewFusion, a Belgian technology and marketing company,[127] has created a program where its employees "can opt for a

122. Iain Gillespie, *Human Microchipping: I've Got You Under My Skin*, SYDNEY MORNING HERALD (Apr. 16, 2014, 1:36 PM), http://www.smh.com.au/digital-life/digital-life-news/human-microchipping-ive-got-you-under-my-skin-20140416-zqvho.

123. Julia Scheeres, *Tracking Junior with a Microchip*, WIRED (Oct. 10, 2003, 2:00 AM), https://www.wired.com/2003/10/tracking-junior-with-a-microchip (explaining that Solusat is "the Mexican distributor of VeriChip," the same technology that Applied Digital Solutions had marketed in Florida).

124. *Id.*

125. Simon Morton, *Barcelona Clubbers Get Chipped*, BBC NEWS (Sept. 29, 2004, 8:17 AM), http://news.bbc.co.uk/2/hi/technology/3697940.stm.

126. *Id.* (noting that the chip technology could be beneficial for clubgoers, because "[t]his sort of thing is handy for a beach club where bikinis and board shorts are the uniform and carrying a wallet or purse is really not practical").

127. *Just Who Are We?!*, NEWFUSION, http://www.newfusion.be/en (last visited Oct. 24, 2018). New Fusion describes its business goals as follows:

> We are a Digital Media Agency that's bringing something new and exciting to the table: a unique approach to cater to all your media and marketing needs. By fusing

microchip implant in their hands to gain access to the company's HQ and computer systems."[128]

NewFusion's program was replicated in Sweden, where Epicenter, a startup hub, "offer[ed] to implant its workers and startup members with [rice-sized microchips] that function as swipe cards: to open doors, operate printers, or buy smoothies with a wave of the hand."[129] The company reported that approximately 150 employees, or 7.5% of the workforce, had agreed to have the implants inserted in their hand.[130]

### 3. Employee Microchipping in the United States

Although the initial adopters of body microchipping technology were limited to a few companies in Europe, the technology has recently found its application in the United States. Starting in August of 2017, Wisconsin technology company Three Square Market offered employees a voluntary microchip implant program.[131] According to the company's leadership, "this is the first U.S. appearance of [the] technology."[132]

The chips would allow the implantee to perform "any task involving RFID technology—swiping into the office building, paying for food in the

---

> technology and marketing together, we create exciting experiences with a personal touch and design the necessary tools to bring your message across.

*Id.*

128. Brett Williams, *An Implanted Microchip ID Could Be Your Next Work Perk*, MASHABLE (Feb. 7, 2017), http://mashable.com/2017/02/07/belgian-company-microchips-employees. For employees that agree to use the RFID technology, the company provides two options:

> Employees can choose between a full-on electronic radio frequency identity (RFID) chip hand implant, which is inserted between the thumb and index finger, or a chipped ring if they aren't quite ready to join the transhumanist movement. The chips contain their owner's personal data, along with allowing access to the company's assets.

*Id.*

129. James Brooks, *A Swedish Start-Up Has Started Implanting Microchips Into its Employees*, CNBC (Apr. 3, 2017, 10:50 AM), https://www.cnbc.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html ("'The biggest benefit I think is convenience,' said Patrick Mesterton, co-founder and CEO of Epicenter. As a demonstration, he unlocks a door by merely waving near it. 'It basically replaces a lot of things you have, other communication devices, whether it be credit cards or keys.'"). The Swedes have been early and eager adopters of bio-implants—recently it was reported that approximately "3,000 cyber-Swedes have small, rice-sized chip implants." Daily Hodl Staff, *'Cyborg' Technology Can Put Bitcoin in Every Body*, DAILY HODL (May 22, 2018), https://dailyhodl.com/2018/05/22/cyborg-technology-can-put-bitcoin-in-every-body.

130. Brooks, *supra* note 129.

131. Baenen, *supra* note 12.

132. *Id.* Interestingly, there are reports that body microchipping technology in the employment context appeared previously in 2006 in the United States. Alec Magnet, *Ohio Company Implants Security Chips into Employees*, N.Y. SUN (Feb. 14, 2006), http://www.nysun.com/national/ohio-company-implants-security-chips-into. Despite this, Three Square Market's spokesperson states that they are the first employer to bring body microchipping technology into the employment context in the United States. Baenen, *supra* note 12.

cafeteria—[all] with a wave of the hand."[133] The program has received extensive coverage by the news media, along with mixed reactions.[134]

Three Square Market has broken ground as the first employer to offer body microchipping in the United States. As a result, the path has been paved for a body microchipping industry to emerge in this country. Dangerous Things, founded by biohacker[135] Amal Gaafstra, is a new American supplier of gadgetry and microchips for use with the body.[136] Gaafstra claims that attitudes towards body microchipping are changing as the technology has begun to emerge, asserting that curiosity has replaced traditional negative attitudes towards the technology.[137] It is remarkable that a biohacking

---

133. Maggie Astor, *Microchip Implants for Employees? One Company Says Yes*, N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html. The tasks accomplished by these RFID chips are quite similar to the scope of functionalities previous RFID chips in the employment setting have accomplished. *See supra* Section II.E.2.

134. Likely because of the novelty of the technology and its use in the employment context, the Three Square Market story has been widely reported. For just a few examples of the media coverage, see Mary Bowerman, *Wisconsin Company to Install Rice-Sized Microchips in Employees*, J. SENTINEL (July 24, 2017, 6:46 AM), https://www.jsonline.com/story/tech/nation-now/2017/07/24/wisconsin-company-install-rice-sized-microchips-employees/503867001 ("[M]icrochipping employees may sound like something out of a horror film . . . ."); Jefferson Graham & Laura Schulte, *Wisconsin Workers Embedded with Microchips*, USA TODAY (Aug. 1, 2017, 2:16 PM), https://www.usatoday.com/story/tech/talkingtech/2017/08/01/wisconsin-employees-got-embedded-chips/529198001; Chris Morris, *Wisconsin Company Holds Party to Implant Workers With Microchips*, FORTUNE (Aug. 2, 2017), http://fortune.com/2017/08/02/wisconsin-company-holds-party-to-implant-workers-with-microchips; Erik Ortiz, *Wisconsin Company Three Square Market Offers to Install Microchips in Employees*, NBC NEWS (July 25, 2017, 9:06 PM), https://www.nbcnews.com/tech/tech-news/wisconsin-company-three-square-market-offers-install-microchips-employees-n786266.

135. Biohackers are individuals that implant devices, such as RFID tags, into human bodies. *See* Ben Popper, *Cyborg America: Inside the Strange New World of Basement Body Hackers*, VERGE (Aug. 8, 2012, 10:37 AM), https://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers (profiling the backgrounds and attitudes of some American biohackers).

136. DANGEROUS THINGS, https://dangerousthings.com/products (last visited Oct. 24, 2018). For a more detailed profile on Dangerous Things and its founder, see Meghan Neal, *For Sale: A Biohacking Chip You Can Implant on Your Own*, MOTHERBOARD (Apr. 10, 2014, 2:46 PM), https://motherboard.vice.com/en_us/article/bmjm85/now-on-sale-a-biohacking-chip-you-can-implant-on-your-own ("Dangerous Things' [founder] Amal Graafstra plans to 'continuously find and develop new devices, software, and services you can use your xNT implant with. Whenever possible, these projects will be open-sourced, allowing the community to customize systems and build new solutions.'").

137. Ariel Bogle, *One 'Killer App' Will Bring Biohacking to the People, Says Transhumanist*, MASHABLE (Aug. 25, 2016), http://mashable.com/2016/08/25/bio-hacking-amal-graafstra. Dangerous Things Founder Amal Graafstra remarked on peoples' evolving attitudes towards implants:

> Attitudes are changing as people become more familiar with the idea of implants. "In the beginning it was people just saying 'you're crazy, or you're working for the government or the devil, or both,'" [said Graafstra].
>
> Now their objections are more mundane: "That's well and good for you, but it's not for me."

*Id.*

industry, which includes employers like Three Square Market and retail shops like Dangerous Things, has already emerged in the United States. The industry is likely to grow as body microchipping continues to receive attention, and more individuals and employers begin to adapt the technology for their uses.

## III. EMPLOYER MICROCHIP IMPLANT PROGRAMS AND LEGISLATIVE RESPONSES

Body microchipping presents a host of new possibilities and applications for RFID within the employment context. However, it is unclear how the law should respond, if at all, to this new technology. Section A of this Part identifies the potential for growth of employer RFID body microchipping, Section B summarizes existing legislation and discusses potential legislation among the states that regulates this technology, and Section C mentions some of the challenges that these devices will present to employees who are reluctant or unwilling to agree to implants.

### *A. HOW POPULAR WILL BODY MICROCHIPPING BECOME IN THE EMPLOYMENT CONTEXT?*

It is difficult to predict how popular body microchipping technology may become in the employment context. However, if current trends continue, the use of the technology is likely to expand beyond the relatively few instances already reported. Support for the belief that body microchipping practices might expand has been found in academia. Vincent Conitzer, a Professor of Computer Science at Duke University, claims that the technology could become standard in the workplace and that future iterations of the technology could add more functionalities while increasing the amount of data collected from the chips, raising privacy concerns.[138] "If most employees agree, it may become a workplace expectation. Then, the next iteration of the technology allows some additional tracking functionality. And so it goes until employees are expected to implant something that allows them to be constantly monitored, even outside of work . . . ."[139] Noelle Chesley, an Associate Professor of Sociology at the University of Wisconsin-Milwaukee, agrees with Conitzer's assessment: "Many of those at the edge of developing those technologies 'believe we are going to be combining technology in our bodies.'"[140] Conitzer and Chesley's predictions should lead legislatures to closely monitor all relevant developments.

---

138. Ortiz, *supra* note 134.

139. *Id.* (quoting Professor Conitzer). For a full profile of Professor Conitzer, see *Vincent Conitzer*, DUKE COMPUT. SCI., https://users.cs.duke.edu/~conitzer (last visited Oct. 26, 2018).

140. Baenen, *supra* note 12 (quoting Professor Chesley). For a full profile of Professor Chesley, see *Noelle Chesley*, COLL. LETTERS & SCI., U. WIS.-MILWAUKEE, https://uwm.edu/sociology/people/chesley-noelle (last visited Oct. 26, 2018). Professor Chesley has published literature related to this subject matter. *See, e.g.*, Noelle Chesley, *Workplace Technology Use May Increase Both*

### *B. THE CURRENT STATE OF BODY MICROCHIPPING LAW*

Neither state nor federal law has paid sufficient attention to the body microchipping phenomenon. Until recently, state and federal lawmakers had not taken any steps towards regulating body microchips. Unfortunately, the measures that legislatures have passed do not achieve a level of uniformity that is crucial in the employment setting. Five states have laws on the books that ban the mandatory implanting of RFID devices: California,[141] Missouri,[142] North Dakota,[143] Oklahoma,[144] and Wisconsin (home of Three Square Market).[145] While all these states prohibit mandatory RFID implants in employees, each state has employed unique statutory language and different punishments for violations of the statutes. For example, "[i]n California for each day the [offense] occurs after the initial [offense] a $1000.00 fine exists whereas in a state like Oklahoma and Wisconsin each day the [offense] continues an additional principal fine ($10,000) is charged."[146] As one author succinctly states, "[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."[147] While it is laudable that a handful of states have passed measures to limit employers' ability to mandate RFID implants, the legislation that does exist has taken many forms and will likely lead to confusion among employers and employees who are attempting to ascertain their rights and responsibilities.

---

*Employees' Distress and Productivity*, LONDON SCH. ECON. US CTR., http://blogs.lse.ac.uk/usappblog/2014/03/24/workplace-technology-use-may-increase-both-employees-distress-and-productivity (last visited Oct. 26, 2018) ("[I]ncreased technology use, especially when it extends work into personal life, is linked with higher levels of worker distress [in employees].").

141. CAL. CIV. CODE § 52.7(a), (g) (West Supp. 2018) (prohibiting, except under narrow circumstances, any person from "requir[ing], coerc[ing], or compel[ling] any other individual to undergo the subcutaneous implanting of an identification device").

142. MO. REV. STAT. § 285.035(1) (2016) ("No employer shall require an employee to have personal identification microchip technology implanted into an employee for any reason." (footnote omitted)).

143. N.D. CENT. CODE § 12.1-15-06 (2012) ("A person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device.").

144. OKLA. STAT. tit. 63, § 1-1430 (2011) ("No person, state, county, or local governmental entity or corporate entity may require an individual to undergo the implanting of a microchip or permanent mark of any kind or nature upon the individual.").

145. WIS. STAT. § 146.25(1) (2016) ("No person may require an individual to undergo the implanting of a microchip.").

146. Angelo Friggieri et al., *The Legal Ramifications of Microchipping People in the United States of America—a State Legislative Comparison*, 2009 IEEE INT'L SYMP. ON TECH. & SOC'Y § 13.2.

147. *Id.* § 14.

In addition, ten states have considered adopting similar laws banning mandatory workplace RFIDs: Colorado,[148] Florida,[149] Georgia,[150] Maryland,[151] Nevada,[152] New York,[153] Ohio,[154] Virginia,[155] and Pennsylvania.[156] However, as of this writing, none of these states' legislatures has passed RFID implant legislation. In what can perhaps be attributed to now-outdated societal views, some of the earlier efforts to pass bills in these states failed and were ridiculed. For example, the Georgia legislative proposal was mocked by former Governor Roy Barnes, presumably because RFID implants were not viewed as a credible threat.[157] In addition, Virginia's proposed bill was characterized by bizarre statements by a state delegate, who was concerned that RFID implants were the "'mark of the beast' worn by Satan's minions."[158] Despite early

148. *States Regulate Use of Microchips as Tracking Device*, CCH HUM. RES.: MGMT. IDEAS & TRENDS, Mar. 7, 2007, at 34, https://www.littler.com/files/press/pdf/16166.pdf.

149. David Royse, *Bill Takes on Future Problem: Involuntary Microchip Implants 1*, OCALA STAR–BANNER (Mar. 23, 2007, 12:01 AM), http://www.ocala.com/news/20070323/bill-takes-on-future-problem-involuntary-microchip-implants-1.

150. Alan Greenblatt, *Lawmakers Are Working on Anti-Brain-Chip Bill*, NPR (Apr. 15, 2010, 3:29 PM), https://www.npr.org/sections/alltechconsidered/2010/04/15/126023516/breathe-easy—ga—lawmakers-are-working-on-anti-brain-chip-bill.

151. Kelsi Loos, *Frederick Senator Proposes Ban on Mandatory Microchipping*, FREDERICK NEWS–POST (Mar. 14, 2018), https://www.fredericknewspost.com/news/politics_and_government/frederick-senator-proposes-ban-on-mandatory-microchipping/article_dd754d27-74e7-59c7-b504-1375f98c23c3.html.

152. Sandra Chereb, *Outlawing Microchipping Humans Not So Far-Fetched, Nevada Senator Says*, LAS VEGAS REV. J. (Feb. 13, 2017, 4:14 PM), https://www.reviewjournal.com/news/politics-and-government/nevada/outlawing-microchipping-humans-not-so-far-fetched-nevada-senator-says ("Senate Bill 109 would make it a Class C felony to require someone to be implanted with a radio frequency identifier, such as microchips placed in pets.").

153. Glenn Blain, *State Pol Proposes Legislation to Ban Employers from Planting Microchips in Workers*, N.Y. DAILY NEWS (Sept. 21, 2017, 6:14 PM), http://www.nydailynews.com/news/politics/n-y-pol-reveals-bill-ban-employers-microchipping-workers-article-1.3512050. To be clear, the bill proposed in the article is not one that would completely prohibit the implementation of microchips in the employment context; rather, the bill would prohibit compulsory body microchipping "as a condition of employment." *Id.*

154. *Newly Introduced Bill Would Protect Privacy: ACLU Calls on Legislators to Support Restriction on Radio ID Tags*, ACLU OHIO (July 20, 2006), http://www.acluohio.org/archives/press-releases/newly-introduced-bill-would-protect-privacy.

155. Stephanie Condon, *Va. Lawmakers Oppose Forced Microchip Implantation, and the Antichrist*, CBS NEWS (Feb. 10, 2010, 6:08 PM), https://www.cbsnews.com/news/va-lawmakers-oppose-forced-microchip-implantation-and-the-antichrist.

156. Steve Esack, *Alarmed Pa. Lawmaker Offers Bill to Limit Microchip Implants in Workers*, PHILA. INQUIRER (Aug. 7, 2017), http://www.philly.com/philly/business/alarmed-pa-lawmaker-offers-bill-to-prevent-microchip-implants-in-workers-20170807.html.

157. Willoughby Mariano, *Former Gov. Roy Barnes Said Georgia Passed Laughable Legislation*, POLITIFACT GA. (July 11, 2010, 6:00 AM), http://www.politifact.com/georgia/statements/2010/jul/11/roy-barnes/former-governor-roy-barnes-said-georgia-passed-lau.

158. Daniel Tencer, *Virginia Delegates Pass Bill Banning Chip Implants as 'Mark of the Beast'*, RAW STORY (Feb. 10, 2010, 3:58 PM), https://www.rawstory.com/2010/02/virginia-passes-law-banning-chip-implants-mark-beast.

skepticism towards RFID implant legislation, there has been an uptick in the number of state legislatures that have discussed passing anti-mandatory RFID implant bills in recent years. In fact, state legislators in four out of the ten states mentioned above have called for such legislation during 2017 and 2018 and it appears that the skeptical voices denouncing these types of legislative proposals have diminished.[159]

### C. *POTENTIAL EMPLOYMENT DECISIONS THAT MAY RESULT FROM EMPLOYER MICROCHIPPING PROGRAMS*

If body microchipping becomes pervasive within workplaces and reaches a point of near ubiquity, employees who wish to opt out of body microchip programs are likely to face internal pressure to agree to receive microchips. For example, at Three Square Market, over 60% of all workers agreed to receive body microchips in the first batch of microchipping.[160] It is possible that remaining employees at Three Square Market, along with employees at other businesses who are reluctant to embrace body microchipping technology, may be passed up for promotion or suffer in other related ways because they are viewed as uncooperative or not acting as team players. At companies with significant populations of microchipped employees (like Three Square Market), the potential exists for management to treat any 'uncooperative' employees unfavorably and remove them from consideration for promotions, or even disqualify potential employees who are reluctant to accept body microchips.[161]

## IV. AMERICAN LAW SHOULD TAKE AN ACTIVE APPROACH TO REGULATING EMPLOYER BODY MICROCHIP PROGRAMS

Without proper regulation, body microchip programs are likely to expand, which may further deteriorate employee privacy protections, and could result in other adverse consequences not contemplated by this Note. This Part argues that state and federal law should proactively attempt to curtail the potentially harmful effects of employee body microchip programs.

---

159. *See* Blain, *supra* note 153; Chereb, *supra* note 152; Esack, *supra* note 156. These media reports discuss potential legislative measures in New York, Nevada, and Pennsylvania, and are largely free of the incredulous statements that characterized media reports on similar proposed legislation just a few years earlier.

160. Trent Gillies, *Why Most of Three Square Market's Employees Jumped at the Chance to Wear a Microchip*, CNBC (Aug. 13, 2017, 9:00 AM), https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html ("50 of the 80 employees at Three Square Market, a provider of self-service breakroom vending machines, voluntarily agreed to be 'chipped.'").

161. Examples of companies marginalizing employees who do not wish to receive RFID implants are lacking, likely due to the limited instances of the technology's use. However, employees who resist change are often dismissed. *See* Vivian Giang, *4 Signs It's Time to Fire an Employee*, BUS. INSIDER (May 5, 2013, 3:40 PM), https://www.businessinsider.com/4-signs-its-time-to-fire-an-employee-2013-5 ("If an employee—even one who used to be a high performer—can't keep pace or move in the same direction as the company, then he or she is no longer the right fit.").

Legislatures can achieve this goal by prohibiting mandatory employee microchipping, preventing employers from making employment determinations based on an individual's microchip status, and looking to current legislation with similar underlying goals to use as models for potential legislative enactments.

### *A. THE LAW SHOULD PROHIBIT MANDATORY EMPLOYEE MICROCHIPPING*

Compulsory body microchip programs in the employment setting should be flatly prohibited by state and federal legislation. The intrusive nature of body microchips and the debilitating effects on employee privacy should lead legislatures to act preemptively and with a heavy hand. Legislators in five states have taken action and have banned any entity (including private employers and government bodies) from mandating or forcibly implanting body microchips.[162] However, the existing legislation is undermined by inconsistencies among the states; to remedy this, Congress should consider passing uniform legislation which would apply to the states and the federal government. The public would benefit from consistency, and this would also ensure that employers would not have to adopt 51 different RFID body implant policies for all potential jurisdictions. Employees would also benefit from a clear and stable approach to legislation.

When proposing potential legislation, lawmakers should consider that, while body microchips currently in existence have been limited to passive RFID chips, the potential exists for GPS and other more intrusive technologies to be paired with RFID. More intrusive technology could be combined with body microchips to extract more data from employees' lives, even outside the workplace. Additionally, the risk of nefarious action —including hacking and misusing data for illegal purposes—is high. Hannes Sjöblad, a technology lecturer and biohacker explains: "It's very easy to hack a chip implant, so my advice is don't put your life secrets on an implant."[163] For these reasons, it is critical that the law take a strict and forward-looking approach to regulating this technology.

### *B. EMPLOYERS SHOULD BE PROHIBITED FROM UTILIZING BODY MICROCHIP STATUS TO MAKE DETERMINATIONS ON EMPLOYMENT STATUS*

Legislatures should regulate companies that offer ostensibly optional body microchipping programs to their employees by ensuring that these programs are truly optional and voluntary. Employers may offer employees the option of voluntarily consenting to any RFID body implant programs, but "the ethical implications of consent in a context where there is a large power asymmetry" give reason to view any voluntary consent programs through a

162. *See supra* Section III.B.

163. *Microchips Implanted in Humans: Practical or Perilous?*, CBS NEWS (Apr. 12, 2017, 6:54 AM), https://www.cbsnews.com/news/microchips-privacy-implants-biohacking.

skeptical lens.[164] The potential for companies to take advantage of their favorable power asymmetry is high, and companies will have a strong incentive to outfit as many employees as possible with body implant microchips.[165]

Employers' desire for widespread adoption of body microchipping among their workforce may result in companies disfavoring current or potential employees who express reluctance to opt into RFID body microchipping programs.[166] In addition, "[e]mployees who refuse to participate in a program . . . face the stigma of being marked as not being a team player."[167] As a result, the law should react to employers' strong incentives to pressure employees into RFID implant programs. Because of the imbalance of power between employers and employees, and employees' understandable reluctance to agree to potential privacy invasions, the law should bolster employees' ability to reject microchipping. Thus, state and federal legislatures should protect employees who choose to opt out of, or are reluctant to opt into, an employer-controlled RFID microchipping program. This protection could manifest itself in different forms—including, but not limited to, ensuring that companies have a process for employees to file internal grievances related to microchipping programs or discouraging employee body implants by taxing employers who offer these programs. Most critically, any such legislation should give employees an avenue to make employment discrimination claims if those employees can show that their current or potential employers have used an employee's body microchipping preference to make decisions on an employee's employment status.

### *C. SUGGESTED MODEL LEGISLATION*

Model legislation that jurisdictions adopt could be drafted and distributed by the American Law Institute ("ALI"). The ALI has ample experience in creating and publishing model statutes that have subsequently been adopted by the states and the federal government.[168] Some examples of ALI model statutes include the Model Penal Code,[169] the Model Land Development Code,[170] and perhaps the most famous example, the Uniform Commercial Code.[171]

---

164. Joseph Jerome, *Embedded Chip on Your Shoulder? Some Privacy and Security Considerations*, IAPP (Aug. 1, 2017), https://iapp.org/news/a/embedded-chip-on-your-shoulder-some-privacy-and-security-considerations.

165. *See supra* Section II.D.

166. *See supra* Section III.C.

167. Jerome, *supra* note 164.

168. *About ALI*, AM. L. INST., https://www.ali.org/about-ali (last visited Oct. 23, 2018).

169. *See generally* MODEL PENAL CODE (AM. LAW INST. 1985) (codifying substantive criminal law).

170. *See generally* MODEL LAND DEV. CODE (AM. LAW INST. 1975) (codifying land use and development regulations).

171. *See generally* U.C.C. (AM. LAW INST. & UNIF. LAW COMM'N 2012) (codifying a uniform standard for commercial transactions).

Legislatures and the ALI can look to current employment discrimination law to model future legislation that addresses worries over body microchipping. A particularly germane statute, which was enacted to respond to changing technology, is the Genetic Information Nondiscrimination Act ("GINA"). Passed in 2008, GINA "prohibits the use of genetic information in making employment decisions in any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoffs, training, fringe benefits, or any other term or condition of employment."[172] GINA proscribes a wide range of potential employer conduct—in particular, Section 202(a) forbids employers from discriminating based on an employees' genetic makeup.[173] The spirit behind Section 202(a) is especially applicable in the microchipping context because the section seeks to restrict the kind of activities that an employer, who abuses a microchipping program, might engage in. Any legislation that attempts to regulate employer body microchipping programs should include a similar section to be effective. Model legislation crafted to reduce the potential of employer abuse of microchipping programs should include a provision that looks very similar to Section 202(a) of GINA, which follows below (with bracketed edits to reflect its new, potential application):

> (a) Discrimination based on [RFID Microchip Implant Status]
>
> It shall be an unlawful employment practice for an employer—
>
> > (1) to fail or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee with respect to the compensation, terms, conditions, or privileges of employment of the employee, because of [RFID microchip implant status] with respect to the employee; or
> >
> > (2) to limit, segregate, or classify the employees of the employer in any way that would deprive or tend to deprive any employee of employment opportunities or otherwise adversely affect the status of the employee as an employee, because of [RFID microchip implant status] with respect to the employee. [174]

In addition to prohibiting specific forms of discrimination, any legislation adopted by state or federal governments should include a provision for remedies and damages. Section 207(a)(1) of GINA provides a relevant example for remedies and damages that could be modified as necessary.[175]

---

172. *What You Should Know: Questions and Answers About the Genetic Information Nondiscrimination Act (GINA) and Employment*, EEOC, https://www.eeoc.gov/eeoc/newsroom/wysk/gina_nondiscrimination_act.cfm (last visited Nov. 1, 2018).

173. Genetic Information Nondiscrimination Act of 2008 § 202(a), 42 U.S.C. § 2000ff–1(a) (2012).

174. *See* 42 U.S.C. § 2000ff–1(a).

175. Genetic Information Nondiscrimination Act of 2008 § 207(a)(1), 42 U.S.C. § 2000ff-6(a)(1). The section provides:

Section 207(a)(1) of GINA authorizes parties to seek remedies under Title 42 of the U.S. Code, Section 1981a which allows for "compensatory and punitive damages"—proposed microchipping legislation should allow employees to seek the same types of damages.[176] Section 207 of GINA also authorizes the Equal Employment Opportunity Commission ("EEOC") to administer and review complaints made pursuant to its provisions.[177] At the federal level, the EEOC has the expertise and experience necessary to properly adjudicate and enforce legislation that Congress could pass based on the recommendations in this Note.[178] In addition, the process to file a formal complaint for alleged employment discrimination related to body-microchip decisions could follow the procedure already set out for filing other complaints.[179] The EEOC has the institutional knowledge and procedural mechanisms to create a coherent regulatory framework to review any discrimination claims that result from employer microchipping programs. At the state level, local state agencies would manage any employee complaints —for example, in Iowa, the Iowa Civil Rights Commission "receives, investigates, and resolves individual complaints alleging discrimination."[180]

## V. CONCLUSION

The state of the law as it pertains to RFID body microchipping and other invasive tracking methods in the employment context does not sufficiently protect employee rights, nor does it address the underlying risks of the technology. Although RFID has been a boon to society and the economy, use of RFID in the employment space has come at the cost of privacy and liberties. The likelihood of an increase in employer microchipping suggests a potential

> The powers, procedures, and remedies provided in sections 705, 706, 707, 709, 710, and 711 of the Civil Rights Act of 1964 [42 U.S.C. § 2000e-4 to 2000e-6, 2000e-8 to 2000e-10] to the Commission, the Attorney General, or any person, alleging a violation of title VII of that Act (42 U.S.C. 2000e et seq.) shall be the powers, procedures, and remedies this chapter provides to the Commission, the Attorney General, or any person, respectively, alleging an unlawful employment practice in violation of this chapter against an employee described in section 2000ff(2)(A)(i) of this title, except as [modified with respect to costs and damages].

*Id.*

176. 42 U.S.C. § 1981a; *see* Genetic Information Nondiscrimination Act of 2008 § 207(a)(3), 42 U.S.C. § 2000ff-6(a)(3).

177. 42 U.S.C. § 2000ff-6.

178. *See EEOC Subregulatory Guidance*, EEOC, https://www.eeoc.gov/laws/guidance/index.cfm (last visited Nov. 1, 2018). The EEOC webpage provides examples of manuals, directives, and policy statements related to employment discrimination legislation that the EEOC has distributed and enforced.

179. *See Filing a Formal Complaint*, EEOC, https://www.eeoc.gov/federal/fed_employees/filing_complaint.cfm (last visited Nov. 1, 2018). The EEOC webpage includes a detailed description on filing a formal complaint with the EEOC. *See id.*

180. *File a Complaint*, IOWA C.R. COMM'N, https://icrc.iowa.gov/file-complaint (last visited Nov. 2, 2018).

for abuse of the technology in the employment-status determinations context. Further intrusion on employees' private lives is too risky and warrants legislative action. Congress—and state legislatures, if necessary—should preclude employers from creating mandatory microchipping programs and should restrict employers' ability to use microchipping status in determining how to treat current or potential employees. The legislative solutions this Note suggests will provide the necessary protection to employees to ensure their privacy remains intact.