EXAMINING THE LEGALITY OF EMPLOYEE MICROCHIPPING UNDER THE LENS OF THE TRANSHUMANISTIC PROACTIONARY PRINCIPLE

JOSHUA Z. WASBIN*

ABSTRACT

Modern workplaces are beginning to look to implanting their employees with RFID microchips as a replacement for badges and keycards. While both employers and employees stand to benefit from the convenience of this innovation, states have begun to look to legislative options for restricting employers from requiring that their employees get microchipped. This Note will examine some of the state legislation and will argue that Congress must institute a federal law that will provide similar, if not stronger, levels of protection for employees who seek to avoid being microchipped, an argument premised upon the Transhumanistic Proactionary Principle.

INTRODUCTION

Last August, fifty employees of a United States company voluntarily agreed to receive a microchip injected into their skin between their thumb and index fingers.[1] Microchipping is the process of inserting an encased radio-frequency identification ("RFID") transponder subdermally into an employee's hand. This Note argues that, based on balancing the technology against the factors of the Proactionary Principle, Congress must institute a federal law that prevents employers from requiring that their employees receive a microchip implant or "microchipping," as well as protections for employees who, under voluntary schemes, refuse the microchip given the dynamics that might imply pressure even if microchipping is presented as optional.

* Executive Primary Editor, *Washington University Jurisprudence Review*; J.D. Candidate, Washington University in St. Louis Class of 2019; B.S. in English, Creative Writing - Poetry, University of California, Los Angeles Class of 2011.

1. Rachel Metz, *This Company Embeds Microchips in Its Employees, and They Love It*, MIT TECH. REV. (Aug. 17, 2018), http://www.technologyreview.com/s/611884/this-company-embeds-microchips-in-its-employees-and-they-love-it/.

Part I of this Note briefly introduces the technology behind microchipping. Part II examines the Transhumanistic Proactionary Principle as a guiding philosophy in questioning whether employee microchipping warrants protectionary laws. Part III focuses on existing laws in the U.S. and in the European Union ("E.U.") currently affecting implementation of RFID microchipping for employers. Part IV examines the associated risks and benefits of a workplace microchipping scheme in light of privacy concerns. Finally, Part V examines microchipping technology from an overall transhumanist perspective.

I. RFID MICROCHIPPING

In July 2017, Wisconsin-based company Three Square Market announced that it would offer its employees subdermal microchipping at a cost to the company of approximately $300 per chip, which would be inserted between each employee's index finger and thumb.[2] The employees were told which types of information the chip would collect and process and freely consented to it. The chip allowed for the following functions: "allow door access to enter the building, sign into their computer, and pay for snacks – all with a wave of [the employee's] hand on a sensor."[3] Three Square Market's CEO Todd Westby stated that the current chip does not have any GPS functionality nor, given the limitations of the passive nature of the current implants, is such a function likely.[4]

Currently, there is a patchwork of state laws that prohibit companies from requiring that their employees accept a microchip implant.[5] Some states have common law that bans such microchipping, such as New York's allowance of an automated identification procedure insofar as it does not involve "lasers or microchips."[6] Where no such law exists, there exists a question of whether a company could require an invasive procedure. In addition, there exists a moral panic about microchipping people, with easily-refuted rumors that the Affordable Care Act would require them to become chipped (a rumor that a satirical article spawned),[7]

2. Trent Gillies, *Why Most of Three Square Market's Employees Jumped at the Chance to Wear a Microchip,* CNBC NEWS (Aug. 13, 2017), https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html.

3. *Id.*

4. *Id*.

5. CAL. CIVIL CODE § 52.7 (West 2008); MO. REV. STAT. § 285.035.1 (2008); N.D. CENT. CODE, § 12.1-15-06 (2008); OKLA. STAT. tit. 63, § 63-1-1430 (2008); WIS. STAT. § 146.25 (2005); MD. SB 944 (2018). For notes and other regulations, see NAT'L CONF. STATE LEG., RADIO FREQUENCY IDENTIFICATION (RFID) PRIVACY LAWS (Nov. 11, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx.

6. Buchanan v. Wing, 664 N.Y.S.2d 865, 866 (App. Div. 1997).

7. Megan Cassidy, *Satirical Article Creates Stir in Wyoming Town*, STAR TRIBUNE (Jul. 30, 2013), http://trib.com/news/local/state-and-regional/satirical-article-creates-stir-in-wyoming-

as well as religious panic that such chipping appeared to be the proverbial "Mark of the Beast."[8] Nonetheless, the uses for these microchips are expansive, and such chipping can provide additional safety and security for the users. For example, such microchip implants have been proposed as a method of security for a wide variety of groups, including Olympic athletes, to detect drug usage.[9] Currently, football players in the National Football League have microchips that are being fitted into their uniforms.[10] These chips, however, are not invasive in the same sense as those seen at Three Square Market or the hypothetical chips considered in this Note, because not only are they embedded in the clothing, but also the televised nature of the sport imputes a lessened expectation of privacy in the players' movements and tracked information. Because of this growing popularity for this form of data gathering, the law must determine the validity of these devices in the context of a workplace setting.

A preliminary explanation of RFID microchipping is required here given the novelty of the process. An RFID transponder is an electronic device that contains information and relies on electromagnetic fields to pass this information along to sensors. RFID is not a new technology; rather, it was used in World War II to identify friendly aircrafts.[11] RFID chips require three core components: a chip, an antenna, and a reader.[12] RFID chips can be broken down into two different classifications based on the mode of data transfer. Active RFID chips have a built-in power source that allows them to transmit data across longer ranges. Passive chips (and consequently, a sub-branch called semi-passive) rely on a method of modulated backscatter to transmit their stored information, effectively utilizing power from the reading device.[13] The microchipping in this Note primarily refers to the passive method, relying on reader devices to supply the bulk of the power in the operation, although active chips are addressed later in this Note for the purposes of looking to the future of such

town/article_bf915e38-98ab-51d5-85f3-9d3825617d60.html.

8. Jim Edwards, *Microchip Implant Controversy: A Mark of the Beast or the Coming "Singularity"?*, CNBC NEWS (Nov. 9, 2010, 3:54 PM), https://www.cbsnews.com/news/microchip-implant-controversy-a-mark-of-the-beast-or-the-coming-singularity/.

9. Martha Kelner, *Call for Athletes to be Fitted with Microchips in Fight Against Drug Cheats*, THE GUARDIAN, (Oct. 10, 2017 5:00 PM), https://www.theguardian.com/sport/2017/oct/10/call-for-athletes-to-be-fitted-with-microchips-fight-against-drug-cheats.

10. Ken Belson, *N.F.L. Expands Use of Chips in Footballs, Promising Data Trove*, N.Y. TIMES, (Sept. 9, 2017), https://www.nytimes.com/2017/09/07/sports/nfl-expands-use-of-chips-in-footballs-promising-data-trove.html?_r=0.

11. FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATION AND IMPLICATION FOR CONSUMERS 6 (2005), https://www.ftc.gov/sites/default/files/documents/reports/rfid-radio-frequency-identification-applications-and-implications-consumers-workshop-report-staff/050308rfidrpt.pdf.

12. *See id.* at 3.

13. *See id.* at 6.

technology. Passive tags rely on a "reader talks first" ("RTF") protocol to send their signal.[14] Thus, these tags are not actively looking for readers; instead, they wait to receive a signal from a reader before sharing the unique identifier number with the reader. In the context of an employer, the reader can store and transmit the identifier number to the data processor where its use is at the discretion of the employer.

II. TRANSHUMANISM AND THE PROACTIONARY PRINCIPLE

Transhumanism is simultaneously a modern movement and a philosophy that seeks to improve the human condition through reliance on technology and innovations. Transhumanism does not blindly applaud emerging technologies; instead, it focuses on critically analyzing and weighing the risks and benefits of any given advancement. In this vein, British philosopher and futurist Max More developed a principle that was designed to encourage and advance technological progression and to perform analysis of the risks and benefits upon the inception of the technology, rather than before its use. More calls this the "Proactionary Principle"[15] as a direct response to a more precautionary method of adopting and creating new technologies. The Proactionary Principle is broken down into seven factors:

> 1. People's freedom to innovate technologically is valuable to humanity. The burden of proof therefore belongs to those who propose restrictive measures. All proposed measures should be closely scrutinized.
>
> 2. Evaluate risk according to available science, not popular perception, and allow for common reasoning biases.
>
> 3. Give precedence to ameliorating known and proven threats to human health and environmental quality over acting against hypothetical risks.
>
> 4. Treat technological risks on the same basis as natural risks; avoid underweighting natural risks and overweighting human-technological risks. Fully account for the benefits of technological advances.
>
> 5. Estimate the lost opportunities of abandoning a technology, and take into account the costs and risks of substituting other credible

14. Grishma Khadka & Suk-Seung Hwang, *Tag-to-Tag Interference Suppression Technique Based on Time Division for RFID*, 17 SENSORS 78 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5298651/.

15. Max More, *The Proactionary Principle*, THE EXTROPY INSTITUTE (2005), http://www.extropy.org/proactionaryprinciple.htm.

> options, carefully considering widely distributed effects and follow-on effects.
>
> 6. Consider restrictive measures only if the potential impact of an activity has both significant probability and severity. In such cases, if the activity also generates benefits, discount the impacts according to the feasibility of adapting to the adverse effects. If measures to limit technological advance do appear justified, ensure that the extent of those measures is proportionate to the extent of the probable effects.
>
> 7. When choosing among measures to restrict technological innovation, prioritize decision criteria as follows: Give priority to risks to human and other intelligent life over risks to other species; give non-lethal threats to human health priority over threats limited to the environment (within reasonable limits); give priority to immediate threats over distant threats; prefer the measure with the highest expectation value by giving priority to more certain over less certain threats, and to irreversible or persistent impacts over transient impacts.[16]

This Note relies on the Proactionary Principle in determining the proper level of restrictiveness, if any, that should be applied to laws restricting both mandatory and voluntary microchipping at a federal and state level. In order to do so, this Note forays into relevant employee privacy laws and countervailing corporate interests.

Transhumanism is fundamentally rooted in Enlightenment humanism.[17] It exists as a life philosophy and as an intellectual movement. Its ultimate goal is technological progression to transcend human weaknesses—a state dubbed "post-human."[18] Transhumanism recognizes the modern trend of storing memories externally, relying on technology to record and create avatars. This extension of the mind fuzzes the boundaries between what the human mind consists of. Transhumanism, however, does not leap forward blindly, promoting the use of all technological improvements to man. While principles such as the Proactionary Principle strive to generally err on the side of progress, Transhumanism as a philosophy shies away from technologies that do not exist to further the pursuit of the post-human condition. Whether or not RFID microchipping would suffice in the question of transhumanist

16. *Id*.

17. Max More, *The Philosophy of Transhumanism*, *in* THE TRANSHUMANIST READER: CLASSICAL AND CONTEMPORARY ESSAYS ON THE SCIENCE, TECHNOLOGY, AND PHILOSOPHY OF THE HUMAN FUTURE 4 (Max More & Natasha Vita-More eds., 2013).

18. *Id.*

progress is the fundamental question that belies the inquiry of this Note. Admittedly, the Proactionary Principle is usually applied to technologies that directly implicate the human condition and seek to improve upon deficiencies in the human form. Nonetheless, this Note posits that workplace improvements can be directly correlated to human improvements. As further discussed below, where a company is capable of operating at a higher level of efficiency, ignoring any potential negative ramifications on the morale or mind of the employee, society as a whole stands to benefit. Ultimately, an improved efficiency will lend itself to increased production and innovation. This increase, in turn, is the precise type of progress transhumanist philosophers like More envisioned.[19]

Thus, to determine the worthiness of the technology, it is paramount to examine it under the auspice of each of the tenets of the Proactionary Principle. The first point weighs the burden in favor of the demand to halt progress. Here, regardless of how microchipping fares on the remainder of the tenets, it holds a strong advantage: where such progress exists, the technology should be assumed to be valuable as an innovation. The second tenet requires analysis of the new technology to focus on the basis of the actual, scientific risk and not popular perception. These risks are further expounded upon in Part IV below; however, the scientific risks, allowing for common reasoning biases, impute a concern about the stress and mental hardships that less-intrusive monitoring technologies can cause and thus weigh against microchipping.

The third tenet seeks to give precedence to proven threats to human health. Studies seeking to understand the effect of surveillance in the workplace have been plentiful and the results often align: monitoring employees can produce beneficial effects for the workplace when the employees are aware of the monitoring system. A recent study on implementing an anti-theft monitoring system in restaurant place of service terminals showed a significant reduction–though not a complete removal–of revenue theft from the till.[20] Beyond just reducing the amount of theft, the monitoring system seemingly pushed employees who might have engaged in revenue theft to redirect their efforts towards more productively upselling customers to increase their own financial state.[21] Other studies confirm the conclusion that monitoring employees can result in a more efficient workforce.[22] However, such monitoring can lead to an

19. *Id*. ("When transhumanists refer to "technology" as the primary means of effecting changes to the human condition, this should be understood broadly to include the design of organizations, economies, polities, and the use of psychological methods and tools.").

20. Lamar Pierce et al., *Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity* 16 (2013), https://olin.wustl.edu/docs/Faculty/Pierce_Cleaning_House.pdf.

21. *Id*. at 4.

22. *See, e.g.*, Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-*

increase in stressors that can subsequently decrease workforce morale and efficiency.[23] Even the Supreme Court of the United States has found that the use of newer technologies can increase employee anxiety.[24] There is, additionally, uncontroverted evidence that stress, especially in the workplace, can have a damaging effect on people, be it mental or even physical harm.[25] There have not been sufficient studies on the effects of RFID microchipping on the mental or physical health of the employees affected, given the novelty of the process. Nonetheless, a parallel might be drawn between alternate forms of monitoring, such as those in the above studies, which might significantly hamper the mental wellness of the workforce, depending on their exposure to the monitoring, their involvement, and the level of discipline being exercised in the office. Thus, a balance must be found: a workplace environment where the employees are monitored, but not to the extent where they might feel discomforted by the amount of surveillance. Ultimately, this factor weighs heavily in favor of prohibiting mandatory implantation. Given the nature of a true voluntary scheme of usage, such a system of monitoring would prove largely ineffectual in order to discipline employees, given that not all employees would likely opt in. However, where mandatory, the stressors involved in the process of maintaining an omnipresent RFID microchip should logically be greater than those attached to a smart badge, where the remedy of simply removing it can provide at least emotional and mental comfort.

Fourth, the transhumanist principles ask those proposing restriction of new technologies to treat technological risks on the same basis as natural risks. This tenet, also referred to as "symmetrical treatment," serves the purpose of ridding the discussion of an anti-technological bias. The natural risks have been outlined in the remainder of this Note. While there is no cognizable risk from the insertion process, the natural risk stems from potential stressors or related mental burdens the tracking causes. This is purely hypothetical and beyond the scope of this Note. The technological risks, on the other hand, include the susceptibility of the data to theft, the permanence of the implant, and the potential advancement in chip technology or through the creation of a broad network of RFID receivers

world Setting, BIOL. LETT. 412–14 (Sept. 22, 2006), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1686213/. (2006).

23. Mahmoud Mousa, *Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America*, SAGE OPEN 2 (2015), http://journals.sagepub.com/doi/pdf/10.1177/2158244015580168; *see also* Smith et al., *Employee Stress and Health Complaints in Jobs with and Without Electronic Performance Monitoring*, 23 APPL. ERGON 17–27 (1992).

24. NLRB v. J. Weingarten, Inc., 420 U.S. 251, n.10 (1975).

25. Robert M. Sapolsky, *Why Stress Is Bad for Your Brain*, 273 SCIENCE 749 (1996).

that would allow employers to gather significantly more information than merely entrance into the building and access to the computer and lunchroom. As a result, it is imperative to treat the potential increase in stressors similar to the potential increase in the scope of tracking. So, this factor does not weigh in favor of increasing regulation or not; rather, it merely informs the remainder of the discussion by providing clear guidelines as to what must be considered when deciding how to legislate, or whether to legislate at all, concerning RFID microchipping.

Transhumanism requires consideration of the lost opportunities that would arise should the technology be abandoned or disallowed. Here, such abandonment would result in a trove of data not being collected—data that exceeds what a company or data scientist might reveal from a data set derived from smart badges. This portion of the principle demands pontification of what might be were there no legislation banning mandatory implants. Indeed, given a guarantee that all employees could be required to bear these chips, companies could heavily invest in data scientists to increase productivity and create data sets to improve on work conditions generally.

While such a loss would be detrimental to the future of the workplace, it is not without replacement. Modern smart badge usage obviates the necessity for an implanted tracking mechanism by providing similar data points. Additionally, an interested corporation could simply mandate usage of a smart badge that would unlock doors, pay for food, access computers and be able to collect and process all the same data points. Thus, the question must be posed: What advancement does the RFID microchip truly pose? Fundamentally, the mechanism is the same as a smart badge, albeit an employee cannot inadvertently leave his or her implanted microchip in a car, at home, or misplace it. The core difference, therefore, must be broken down into two pieces: 1) that an implanted microchip is inherently more convenient and impossible to misplace, thereby lowering potential safety risks; and 2) that an implanted microchip can increase functionality via an increased amount of data collection that a company could not achieve via strictly active scans of a smart badge. It is not farfetched to assume increased functionality might include higher degrees of tracking, even without a shift in technology. A company could, for example, monitor employees' drinking habits by paying local pubs to install scanners on their door. This information, linked with the following day's productivity, could provide a higher degree of insight into how employee habits affect companies' bottom lines.

Fundamentally, a smart badge allows the user to effectively "opt out" of such tracking by removing his or her badge prior to going out or when he or she does not want to be tracked (e.g. when he or she goes to the restroom). This functionality is missing in the implanted chips, barring

some advancement in consumer-level RFID blocking, which potentially increases the aforementioned monitoring stressors. When such broad tracking is available, the implanted microchips more closely resemble company-issued device privacy issues. An apt comparison is that of *Robbins v. Lower Merion School District* in which a school provided high school students with laptops and then, without permission, remotely activated the installed webcams.[26] Although the civil case eventually settled, the FBI's inquiry into the incident found that no violation of the law had occurred.[27] When a school can track and monitor underage students after hours through laptops without criminal prosecution, a company doing so might fare no worse with their adult employees. While such an act might bring about common law invasion of privacy cases, this remains an open question that the courts have yet to decide.[28] As it stands, though, this type of tortious claim is essentially the only recourse that employees have against overly broad monitoring program as there exist few, if any, federal legislative schemes that can protect employees from pervasive but expected workplace surveillance.

Next, the Proactionary Principle requires consideration of restrictive measures, such as the statute this Note proposes, only if the potential impact of an activity has both significant probability and severity. Such a statute should be proportional to the extent of the probable effects. Here, rather than examining the hypothetical future of the technology, the Proactionary Principle demands examination of only the likely effects, which include increased productivity at the potential cost of employee wellbeing or morale. This portion of the principle ignores highly speculative results, such as a widened network of RFID receptors, always-on tracking, or other equally invasive methods of tracking. Thus, the ultimate question is whether the results of an anti-mandatory chipping statute would be proportional to the potential risk of the probable results and not the speculative risks.

Because the likely result generates efficient benefits, the consideration next turns toward adaptation to the adverse effects of the stressors. In efforts to address elevated stress, corporations should develop protocols and systems to maintain workplace stability. Potential solutions to the increased stressors are better management styles designed to ensure

26. Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 U.S. Dist. LEXIS 89524, at *1 (E.D. Pa. Aug. 30, 2010).

27. *See* Press Release, Philadelphia Division, FBI, No Criminal Charges Filed Following Lower Marion School District Student Computer Monitoring Investigation (Aug. 17, 2010), https://archives.fbi.gov/archives/philadelphia/press-releases/2010/ph081710.htm.

28. Lewis Maltby, *Employment Privacy: Is There Anything Left?*, 39 HUMAN RIGHTS MAGAZINE (May 02, 2013), https://www.americanbar.org/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/employment_privacy.html.

employee mental wellbeing while still optimizing workflow. Nonetheless, given the lack of studies performed to determine the amount of stress that implanted tracking causes compared to external tracking, it is difficult to determine the practicality or extent required for such offsetting to occur. Given the lack of certainty that a system devoid of anti-mandatory chipping regulations could exist except at the detriment of employees, the measures of such a regulation must be proportionate to the potential negative effects. For example, banning all RFID microchipping clearly denies the technology room to grow and is too heavy-handed in comparison to the risk of increased workplace stressors. Banning mandatory RFID microchipping ultimately settles a better balance, but it can still deny corporations the power to greatly improve their workplace efficiency. Increased workplace efficiency should theoretically benefit society as a whole, because products and services could be offered with a tighter margin and less waste. Thus, an inquiry of the balance between the stressors and increased efficiency is required as an economic concern.

Such an inquiry factors into the last portion of the principle, which seeks to maximize expectation values while minimizing harm, predominantly against humans. This Note does not presuppose such an inquiry to be viable without significantly more data than currently exists. Thus, the standing principle should be to proceed with caution: the law should allow the technology, but should also provide safeguards for individuals who do not wish to partake in the experiment—a mentality that resembles this Note's proposed anti-mandatory RFID microchipping legislation.

In light of the above factors, it is clear that microchipping should be handled with caution. Though it is crucial to let technology breathe and determine its merit in a practicable environment, society must factor in the risks that it faces should such microchipping be mandatory for employees. Thus, a proper statutory scheme ought to protect an employer's right to run such a program and an employee's right to voluntarily consent to microchipping, while being cautious of the potential harm that such surveillance might cause. This Note now examines such statutory provisions, considering this balance in light of how the states or even the federal government should apply the Proactionary Principle.

III. EXISTING LAW IN THE UNITED STATES AND IN THE EUROPEAN UNION

The current state of the law prohibiting mandatory microchipping the U.S. is a patchwork. Some states have enacted laws preventing employers from requiring that their employees be microchipped. Even so, these states have a limited set of protections available for employees who are pressured into voluntarily accepting the microchipping or those who refuse

microchipping under a voluntary scheme. Under the General Data Protection Regulation ("GDPR"), passed in the E.U. in April of 2016, such employees receive a series of fundamental protections against schemes of pseudo-voluntary microchipping.[29] European law should inform American legal developments on protections from employer overreach, such as potentially terminating an at-will employee as a result of—although not expressly because of—his or her refusal to consent to a company microchipping scheme.

The California statute that prevents mandatory microchipping provides that "a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device."[30] Specifically, the statute goes on to define the phrase "require, coerce, or compel" to include "physical violence, threat, intimidation, retaliation, the conditioning of any private or public benefit or care on consent to implantation, including employment, promotion, or other employment benefit, or by any means that causes a reasonable person of ordinary susceptibilities to acquiesce to implantation when he or she otherwise would not."[31] This definition provides strong protections for at-will employees who might be concerned that their ability to move up in a company is premised upon their willingness to accept the microchip. Nonetheless, this functions like many other issues that at-will employees suffer: proving the causation behind their termination or why they did not receive a promotion is difficult and often leaves the power in the hands of the employer to terminate the at-will employee at the employer's discretion.[32] Despite this weakness, the California statute remains the strongest protection amongst the current state statutes that prevent mandatory microchipping.

Missouri's statute simply prevents "requir[ing] an employee to have personal identification microchip technology implanted into an employee for any reason" with no additional protections against coercive pseudo-voluntary implanting schemes.[33] Nor do North Dakota's, Oklahoma's, or Wisconsin's statutes have such a protection. Most recently, Maryland

29. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter "GDPR"], (Article 43 finding that an imbalance between the data subject and the controller can affect the consent).

30. CAL. CIV. CODE § 52.7(a).

31. Cal. Civ. Code § 52.7(h)(4).

32. Clyde W. Summers, *Employment at Will in the United States: The Divine Right of Employers*, 3 U. PA. J. LAB. & EMP. L. 65, 77 (2000) ("The dominant judicial perspective is that employers should have unfettered freedom to determine who should be employed and that workers are subordinate to the employer's decisions-however arbitrary they may be.").

33. MO. REV. STAT. § 285.035.1 (2008).

passed SB 944, which took effect on October 1, 2018. Maryland prohibited "requiring, coercing, or compelling an individual", defining that as, "including the use of physical violence, threat, intimidation, retaliation, the conditioning of any private or public benefit, including employment, promotion, or other employment benefit, and any other means to cause a reasonable individual of ordinary susceptibilities to acquiesce when the individual otherwise would not."[34] This mirrors the California statute and, consequently, provides a similarly high level of protection.

Outside of California and Maryland, an employer can create a "voluntary" microchipping scheme and coerce employees into allowing the implant to maintain good standing in the company and be available for promotions. The California statutes echoes the policies behind Title VII of the Civil Rights Act of 1964 of an "actionable employer action" in its prevention of discriminatory retaliation. The California and Maryland statutes should be held as the baseline level of protection provided to American employees who face risks of retaliation by employers for not volunteering to be microchipped.

Where American workplaces view issues of employee consent liberally, European workplaces provide more fundamental protections for employees. Such protections become clearly evinced in the recently enacted GDPR in the E.U. The GDPR focuses on providing protections for European citizens' data from global and domestic processing, thereby including the processing that would occur through a process like microchipping. The GDPR provides that "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."[35] This provision provides a hefty roadblock to employers seeking to merely garner consent by pressuring employees to agree to their terms. American employers are free to effectively force consent by threatening to fire the employee for failure to comply.[36] Employers still maintain the bulk of the power in the relationship by being able to fire at-will employees for "any reason or no reason."[37] Thus, even under the protections of California and Maryland's anti-mandatory chipping statute, Cal. Civ. Code § 52.7, an employer can simply terminate the employee for no reason or any other reason where such an employee refused microchipping.

The difficulties here are symptoms of wider employment law issues and are not specific to RFID microchipping. However, if enforcement lacks the needed teeth, even the best statutes prove ineffectual. This

34. Md. General Assemb. S.B. 944, Reg. Sess. (Feb. 5, 2018).

35. GDPR, art. 42.

36. *See, e.g.*, Jennings v. Minco Tech. Labs, Inc., 765 S.W.2d 497, 502 (Tex. App. 1989) (where a court upheld an employer's voluntary drug test or get fired rule).

37. Geary v. U.S. Steel Corp., 319 A.2d 174 (1974).

creates a fundamental difficulty in the laws surrounding RFID microchipping: while California and Maryland arguably have the most comprehensive anti-mandatory or pressured microchipping laws currently in place, an employee cannot be refused promotion for failing to obtain a microchip. Few courts, if any, will be capable of finding that such a promotion was denied for failure to comply with the microchipping protocol.[38] It is easy to conjure reasons for termination where someone has failed to volunteer for microchipping: not a team worker, inefficient, not forward thinking, or simply no reason provided. Given that at-will employment is a foreign concept to European workers, the protections for European workers prove significantly more fruitful.[39] French law, for example, provides a complex labyrinth of protections for employees that heavily restrict, or at least delay, employers' abilities to terminate them.[40] Because of this complexity, it becomes difficult to terminate an employee merely for his or her unwillingness to volunteer for microchipping. However, there is no legal protection that can cause an employer not to frown upon or dislike an employee for his or her failure to comply. Thus, even under the most protectionist legal agenda, employers can pressure employees to accept the microchipping.

The GDPR is not inherently a protective regulation in regards to employment, although some of its terms apply and protect employees in the context of their workplace. The GDPR only is in effect where there is data being processed and that data is personal information (often referred to as "personally identifiable information," or "PII") of a person in the E.U. The GDPR seemingly prohibits companies from mandatorily implanting RFID chips, unless there is a legitimate reason that would balance against the countervailing employee interest of maintaining the employee's own agency. Given the fact that the GDPR has not come into effect, there exists no substantive case law, leaving a lingering question as to what might constitute a "legitimate interest."

---

38. Only insofar as the employer does not specifically write or say that the failure to comply with the microchipping was the reason for the employee's termination.

39. The Littler Report, LITTLER MENDELSON 14 (Feb. 2013), https://www.littler.com/files/press/pdf/WP-2012-Global-Employer-3-25-13.pdf.

40. Craig S. Smith, *Letter from Paris: 4 Simple Rules for Firing an Employee in France* (Mar. 28, 2006), http://www.nytimes.com/2006/03/28/world/europe/letter-from-paris-4-simple-rules-for-firing-an-employee-in.html.

Nonetheless, given the examples of legitimate interests laid out in the GDPR,[41] it seems unlikely that improvements to efficiency would constitute such a legitimate interest. Even if there were found to be a legitimate interest in increasing the efficiency of the company, the baseline level of monitoring that RFID microchipping enables would still push the balancing test to the side of unacceptability.

Another concept that the GDPR explores that has not been successfully addressed in U.S. law is the concept of consent. While Recital 155 of the GDPR[42] ostensibly leaves it up to the E.U. member states to determine what constitutes valid employee consent, the GDPR generally looks cynically at consent, unless such consent is freely given.[43] In other words, there would be no consequences when an employee declines microchip implantation. This bars false consent, namely that if one does not consent, he or she can find other employment. As a result, mandatory chipping is completely outlawed in the E.U. Even consented-to microchipping requires a heightened level of security over the data captured.

Employers seeking additional information about the behaviors of their employees is nothing new. Whether it was Pinkerton agents following someone around in the nineteenth-century[44] to contemporary monitoring technology, there is value in measuring and examining employee behavior. Monitoring can promote workplace effectiveness, efficiency, and timeliness. An employee found to be coming in early and staying too late can be met with if his or her productivity does not reflect his or her hours, encouraging a more productive, shorter work period. Worksite wellness programs have already been used to encourage employees to reduce addictions, such as smoking.[45] A company can use the RFID microchips to

41. GDPR Article 47 contains the examples of direct marketing and fraud prevention. Article 48 contains the example of personal data with a group of undertakings for the purpose of administrative oversight. Article 49 contains the example of network and information security. Article 50 contains the example of reporting possible criminal actions.

42. GDPR Article 155 allows member states to provide "specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship."

43. Specifically, Article 43 of the GDPR questions whether consent exists where "there is a clear imbalance between the data subject and the controller."

44. RHODRI JEFFREYS-JONES, CLOAK AND DOLLAR: A HISTORY OF AMERICAN SECRET INTELLIGENCE (2003).

45. *See, e.g.*, Heirich M, Sieck C.J., *Worksite Cardiovascular Wellness Programs as a Route To Substance Abuse Prevention*, 42 J. OCCUP. ENVIR. MED. 47–56 (2000); D.B. Gold, et al., *Impact of a Telephone-Based Intervention on the Reduction of Health Risks*, 15 AM. J. HEALTH PROMOT. 97–106 (2000).

track smoking breaks by keying access to the smoking area and checking entrance and exit times from the area. Then, by attaching incentives, the company can encourage and track reduction of time spent in the area without manually tracking usage. Unlike with smart badges, an employee cannot simply remove his or her badge before exiting, as RFID receivers would detect his or her entrance and exit from the area. This advantage means it is difficult, albeit not impossible, to circumvent measures the corporation puts into effect, whether they are meant to improve employee welfare or increase workplace efficiency. Thus, the costs to the employer remain limited, while providing a trove of data to comb through with the hopes of finding something to increase productivity.

For the employee, however, the costs become far steeper. Ellen Bayer of the American Management Association noted that "privacy in today's workplace is largely illusory."[46] Indeed, there are few laws protecting an employee's privacy from excess surveillance in the workplace,[47] especially when compared to the overarching protections in the E.U. Because, for example, the employer often owns an employee's machine, that employer can search the employee's computer. As "bring-your-own-device" policies come into vogue, employers can gain easy access to information normally outside the boundaries of the job, such as photos, texts, personal e-mails, and notes.

While the amount of information RFID microchipping currently gathers is miniscule in comparison to the other data that can be collected, the issue is not the types of information being collected *per se*, but the ease by which that data is processed. The Supreme Court of the United States has found the scalability of surveillance to provoke altered legal reactions from their original form, where a more easily applied system of surveillance is more likely to interfere with individuals' rights than a method requiring more manual input.[48] A police officer following a single car from one location to another is acceptable. However, society does not allow the police to remotely track, twenty-four hours a day, seven days a week, an entire city's worth of cars.[49] The reasoning as described in Justice Sotomayor's concurrence in *United States v. Jones* is clear: when the cost of surveillance is the man-hours of a police department with limited resources, surveillance will only be done when needed.[50]

46. *The Rise of Workplace Spying*, THE WEEK (July 5, 2015), http://theweek.com/articles/564263/rise-workplace-spying.

47. *See*, *e.g.*, Ifeoma Ajunwa, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735 (2017).

48. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (finding that the low cost of GPS monitoring alters the relationship between the citizen and the government).

49. *Id.*

50. *Id.*

When the cost of surveillance instead is merely using an automated service, surveillance will be done limitlessly. Microchipping an employee fulfills the latter. Take, for example, a standard company that employs 200 employees. Each day, employees swipe in for the morning, buy lunch in the café, then swipe out for the day. In this excessively simplified example with no bathroom breaks, break room visits, or any other non-work activities, the employer would collect 180,000 data points over the course of a year of work.[51]

As more employees are chipped, the number of data points increases. The more data points an employer collects, the more capable they will be of quickly detecting trends. Adding in each instance where the employee unlocks his or her computer (which would happen only twice a day in the example above)[52], an employer would have collected approximately 300,000 data points over the same time period. More complete data means an employer can paint a clearer picture about how much time an employee spends on specific tasks and activities and determine their level of productivity without requiring direct managerial oversight. This, in turn, can be used to implement company policies to restrict activities or tasks that consume more time than generate revenue, which could be a positive result if we ignore the human ramifications.

Many American corporations can already track an employee's time using timecards, computer monitoring, and keycards. Thus, in defending the microchip, the question must be posed: what makes the RFID microchip any more invasive than the already-in-place means of surveilling employees? Aside from the procedure of implanting the chip, the answer at this point in time appears to be purely the convenience of the corporation. Instead of pairing the data from the keycard to the data from the computer to the data from the cafeteria about the employee's meal, a microchip allows a singular source of information to compile all three. A company can use this data to increase efficiency and measure trends to make changes to its systems. There may be a specific food in the cafeteria causing a post-lunch slowdown, and a microchip-activated coffee machine could be used to determine the optimal caffeine intake for employees.

A diligent manager can determine this by relying on standard office surveillance, but would lack the capacity to create and manage such an exhaustive data set independently. Moreover, were this information gathered and compiled manually, its cost would likely outweigh its benefits. Such a use of the microchip might feel excessive but would likely be acceptable. If the data being processed were sufficiently anonymized

51. Assuming, for the sake of this calculation, an estimated 300-day work year.

52. Ignoring breaks or other reasons to step away, an employee might unlock their terminal upon arrival, lock for lunch, unlock upon returning from lunch, and finally lock once again at the end of the day.

and used in a manner consistent with such anonymization (specifically, used in such a way where the employer neither would nor could pair the data to a specific employee), there would be no privacy issue under even the more intensive scrutiny of the GDPR.

However, as the uses and abilities of the microchips continue to grow, so too do the implications for their ability to process data and provide information to employers. Microchips also pose grave security risks to employers who rely on them. Devices like "BLEkey," a cheap low energy signal mimicker that preys on weaknesses in the Wiegand protocol,[53] can mimic legitimate RFID signals that such devices have silently copied.[54] Having a single point of failure exist inside one's body, especially one where any patching must be done by removing the chip and installing a new one, poses fundamental physical security issues. Once in, a bad actor utilizing a false signal now has access to doors, computer, and common workspace areas. However, this problem is not unique to the microchip.

Current keycards have the same problem from the door, and password access is bypass-able where no two-factor authentication exists. Yet, putting all the information on a singular device—one that a user cannot secure aside from wearing a glove that would block the signal—poses a fundamental security concern that security analysts are far better equipped to address. Again, this is a situation that technological solutions can address. A decade ago, Dr. Elaine Ramesh wrote that the procedure of installing RFID chips into teeth was a work in progress,[55] a change that would ostensibly make it harder to garner someone's passkeys from a simple handshake. Rather than argue that the technology is not yet ready, this Note argues that as the technology progresses, a legal answer is increasingly necessary because of the risks posed to employees who lack the capacity to turn down the microchipping, even if presented in a voluntary fashion.

---

53. Francis Brown, *RFIDiggity, Pentest Guide to Hacking HF/NFC and UHF RFID*, BISHOP FOX (Apr. 5, 2016), http://www.bishopfox.com/files/slides/2016/InfoSec_World_2016-RFIDiggity-Brown-05Apr2016.pdf. While this Note will not investigate the specifics of the well-covered cybersecurity risks of the Wiegand protocol, it is important and relevant to note that even new devices allow for backwards compatibility with Wiegand protocol compliant RFID devices—meaning many businesses can still fall victim to this issue.

54. Swati Khandelwal, *This $10 Device Can Clone RFID-equipped Access Cards Easily*, THE HACKER NEWS, (July 28, 2015), https://thehackernews.com/2015/07/hacking-rfid-access-card.html. Undoubtedly, a lot of security gaps on this front can be overcome with additional research and development but the current schema for RFID usage relies, at least in part, on security by obscurity.

55. Elaine Ramesh, *Time Enough—Consequences of Microchip Implantation*, 8 RISK: HEALTH, SAFETY, & ENVIR. 373–407 (1997), http://scholars.unh.edu/cgi/viewcontent.cgi?article=1344&context=risk

IV. RFID MICROCHIPPING IN LIGHT OF PRIVACY CONCERNS

Upon collection and processing of the information obtained by RFID microchipping, employers will have to deal with safely maintaining the integrity of this data. As the Federal Trade Commission ("FTC") noted in its "RFID Applications and Implications" report, experts are concerned about the manner in which the data is stored after it is collected.[56] In the event of a data breach, hackers might only receive pseudonymized identification numbers and the access time or, ideally, a completely encrypted data set that is of no use to them. However, such information can still be personally identifiable simply by pairing up arrival time or days off. Access to current information (as opposed to just past information) would allow a bad actor to merely keep track of door entries and line up one or two days of data to determine which employee bore which identification number. As the employer collects and processes more data, the danger of a potential breach increases. Nonetheless, where the FTC brings the federal actions for privacy protection, no such action has been brought solely in regards to the information pertaining only to the employees of a company. This is a result of the purpose of the FTC's consumer protection initiative, under which fair employment practices do not fall. Such protection would fall under the purview of the National Labor Relation Board ("NLRB") whose actions indicate a willingness to protect private-sector employees.[57] Nonetheless, because there has not been a breach of this technology to date (namely, because so few employees in America are currently microchipped), it is unclear which actions the NLRB will take in its efforts to protect employees, should such a breach occur.

Fundamentally, the protections available for at-will employees against being compelled to receive a microchip in states other than California and Maryland are mechanically akin to those bringing Title VII claims against their employers. The current scheme of protection grants employers ample leeway in their ability to terminate an at-will employee for most reasons. Provided the employer does not have a policy or a clear pattern of terminating–in the case of Title VII–members of a protected class, it can be difficult for Title VII claims to succeed.[58] Similar factors can therefore be used to discover instances of firing or failure to promote, as illustrated in *McDonnell Douglas Corp. v. Green*.[59]

---

56. FED. TRADE COMM'N, *supra* note 11.

57. *See, e.g.*, NLRB's recent order barring AT&T Mobility LLC from disallowing employees from filming co-workers as an example of their directive.

58. *See, e.g.*, Univ. of Tex. Sw. Med. Ctr. v. Nassar, 570 U.S. 338, 360 (2013) (requiring proof that the prohibited criterion was the but-for cause of the termination).

59. McDonnell Douglas Corp. v. Green, 411 U.S. 792 (1973).

The existing privacy laws do little to protect employees from overreaching privacy interferences from employers. One of the most rudimentary issues here is consent. Consent in the U.S. is often viewed at a more "macro" level, as compared to European privacy laws. Where European laws allow more user level controls and require an opt-in process for more traditionally invasive behaviors, American law is almost entirely the inverse. The macro level view can be summarized as such: either consent or choose not to work here. Assuming, therefore, that an employee chose to continue to work somewhere, receiving the microchip instead of losing his or her job, this might manifest consent. Once the user has consented, the data collection can be used for the purposes outlined upfront. Failure to uphold this portion of the arrangement is more akin to a contract law violation than a privacy law violation. While the FTC has authority over unfair trade practices, which involve changing the scope of a consented-to arrangement without providing notice, this is outside of the FTC's typical authority to take such an action where it is not affecting the public at large, but rather, "consenting" employees at a specific corporation.[60]

Other statutory provisions designed to protect the public from overly aggressive privacy invasions also fail to protect employees from predatory pressures involved in microchipping. While the technology looks akin to the protections enabled by the Electronic Communications Privacy Act ("ECPA"), ECPA provides employers with the legal right to monitor work e-mail, web activity, and other electronic activity, which would include the electric signal received by the RFID transmitters installed around the office.[61]

Additionally, the employers own the RFID receivers that they install around the office, meaning the data is theirs to collect. Accordingly, the data they collect via electronic means rightfully belongs to them under any statutory scheme that is currently available. In order to secure the privacy for employees who seek to limit the amount of information that their employers can collect and process about their workplace activity, the legislation must therefore address the privacy concerns prior to the employee passing an installed RFID receiver, or directly limit the usage of the data.

Limiting the usage of the data collected by the employer through legislation, however, is legally problematic. In *Sorrell v. IMS Health*, the government sought to protect a specific type of data from a specific

60. FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

61. V. John Ella*, Employee Monitoring and Workplace Privacy Law*, AM. BAR ASS'N (2016).

usage.[62] Specifically, the government sought to limit pharmacists from selling data to pharmaceutical companies that the pharmaceutical companies would use for the purpose of "detailing" doctors, or using the data to help them encourage doctors to sell more of their products. The Supreme Court, in a 5-4 split, found that the law effectuated content and speaker-based discrimination and was therefore unconstitutional under the First Amendment. The limitation on the "speech" of processing employee data is arguably less pronounced than that of *Sorrell*, but the fact remains that such a law can be excessively burdensome on the First Amendment-protected speech of the corporation. Where the law seeks only to prohibit the usage of this data for corporations, but allows it for, say, Alzheimer's patients or prisoners, it inherently is selecting a valid viewpoint or speaker while denying another. While the State of Vermont attempted to argue that the law was merely commercial regulation, this was insufficient because the law was found to impose "more than an incidental burden on protected expression."[63]

Because of the constitutional dangers of restricting the means through which the data is used, it is clearer that protections against the actual mandatory chipping are superior. The federal government undoubtedly has the authority to issue such a regulation, which closely mirrors other federal labor laws.[64] Given the lack of legislative force on privacy in the workplace, a law like this would more closely echo laws that protect worker rights. This conceptually removes the necessity for implementing stronger privacy rights for workers than already exists, but allows for a specifically targeted law that might relieve workers of a particular issue. An employer will still be able to obtain the bulk of the same information through smart badges, but will do so without interfering with an employee's anatomical autonomy without the employee willingly consenting to such a technological intrusion.

V. TRANSHUMANISM AND MICROCHIPPING

Some transhumanists have adopted a form of utilitarianism. Of particular note is philosopher and co-founder of Humanity+, an international organization that advocates for ethical techno-utopianism, David Pearce, who proposed the "hedonistic imperative."[65] Seeking eradication of sentient suffering, Pearce proposes an ethical utilitarian view of expansion and progression in technology. By focusing on

62. Sorrell v. IMS Health, 564 U.S. 552 (2011).

63. *Id*. at 556.

64. *See, e.g.*, Fair Labor Standards Act, 29 U.S.C. § 201 (1938) (A law with a similar purpose of work protection at a federal level.

65. David Pearce, *The Hedonistic Imperative*, (1995), https://www.hedweb.com/.

maximizing positive value and eliminating negative value from the technology, Pearce argues that a purist hedonism ought to be the passage to an ideal future without suffering.[66] This philosophy might entice transhumanists, but denies the necessity for progress that More so elegantly reflects in the Proactionary Principle. To become the post-human hedonistic model Pearce sought, humanity must first develop the technologies to displace itself from the workplace, which must become the primary objective. Philosophically, this must be disassociated from idealism that embodies the bulk of the transhumanist movement. Where Transhumanism already angles itself towards inevitability of enhancements Michael Shapiro discussed,[67] it becomes entangled in its own ideals.

Thus, to align the concepts of microchipping with the traditional non-More theorists in the transhumanist school imputes a strong distaste for the concept. An enhancement should not forfeit a fundamental freedom to an employer where instead technology ought to be used in a Piercian hedonistic society. However, without the weary progress that fails to align with the ethical utilitarianism, there can be no ascension beyond "the life-impoverishing hang-ups of humanity's biological past."[68] As More points out, the bulk of the transhumanist philosophers can agree that major scientific and technological progress is "both possible and desirable."[69] Beyond that, More writes, the agreement ends.[70] Nonetheless, there exists a counterpoint to transhumanism upon which the philosophers agree: the weariness of "bioconservatives," namely, those who are unwilling to affect a technological change in themselves, regardless of its objective positive effect.

Nick Bostrom, a Swedish transhumanist philosopher, sets forth four levels of objections to post-humanity, which is the prime objective of the movement.[71] These objections closely mirror potential objections to microchipping technology. Level 0, he contends, is that "it can't be done." This can be easily dispatched in the present case: it has already been done. Level 1 provides a more practical response: it is too difficult or costly.

66. *Id*. at 93.

67. Michael Shapiro, *Performance Enhancement and Legal Theory*, *in* TRANSHUMANIST READER: CLASSICAL AND CONTEMPORARY ESSAYS ON THE SCIENCE, TECHNOLOGY, AND PHILOSOPHY OF THE HUMAN FUTURE 283 (Max More & Natasha Vita-More eds., 2013).

68. Pearce, *supra* note 65.

69. Max More, *The Philosophy of Transhumanism*, *in* TRANSHUMANIST READER: CLASSICAL AND CONTEMPORARY ESSAYS ON THE SCIENCE, TECHNOLOGY, AND PHILOSOPHY OF THE HUMAN FUTURE 14 (Max More & Natasha Vita-More eds., 2013).

70. *Id.*

71. Nick Bostrom, *Why I Want to be a Posthuman When I Grow Up*, *in* TRANSHUMANIST READER: CLASSICAL AND CONTEMPORARY ESSAYS ON THE SCIENCE, TECHNOLOGY, AND PHILOSOPHY OF THE HUMAN FUTURE 20 (Max More & Natasha Vita-More eds., 2013).

Here, however, the cost of the chips is low for each individual employee and the benefit from the information provided by the chips likely outweighs the modest cost per chip.[72] Bostrom lumps medical concerns into this category as well, some of which have been posited against microchipping although never proven.[73] Level 2 is that it would be bad for society. This summons the Proactionary Principle—determining the positive effect on society as a whole. Clearly, if efficiency were to increase without any human cost, this would resolve the Level 2 criticism. Level 3 criticism of post-humanity–and, in this context, the step towards it that might be microchipping–is the claim that lives would be worse. Thus, at Level 3, one can bring in the proposal that an excess increase in efficiency might fundamentally harm or damage the employee's psyche or ability to cognitively perform at a high level, even where there exists a high level of efficiency. Here, one can add in the danger of such a policy giving rise to gamesmanship and forcing employees to actively circumvent the safety measures that employers put into place. Finally, Bostrom's Level 4 is that "we couldn't benefit." This, ultimately, is the sticking point of RFID microchipping.

Transhumanism as a whole can therefore be used to view the technology in two different ways: (1) that RFID microchipping is inherently a benefit to humans on the path to post-humanity, given its propensity for increasing market efficiencies and furthering the likelihood of human displacement from the market, or (2) that the minor benefits of convenience to the human are drastically outdone by the inconvenience, risks, and pressure placed upon them, thus providing a small benefit at a high cost. Given the idealistic nature of transhumanists like More and Pearce, it is not a stretch to say that they would not recognize the technological advancement sufficient to warrant inquiry and find that the costs to the human are too great to warrant such an intrusion, not physically but mentally. This mirrors Pearce's ethical utilitarianism. Like Bentham's Principle of Utility, the incursion into the mental space of the employee brings more pain than pleasure to the employee.[74] Bentham's means of quantification of the two involves weighing this pain (the pressure, stress, and so forth) with the pleasure (the convenience garnered from the chip).

Unlike Transhumanism, Bentham's utilitarianism demands a quantifiable measurement for the trade-off between the pain and the

72. Gillies, *supra* note 2.

73. In fact, the FDA has explicitly cleared microchip implanting for humans. *See* Associated Press, *FDA Approves Computer Chip for Humans*, NBC NEWS (Oct. 13, 2004), http://www.nbcnews.com/id/6237364/ns/health-health_care/t/fda-approves-computer-chip-humans/.

74. JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION (1780).

pleasure. To quantify the balance, one must take a similar approach, as this Note does, to the sixth tenet of the Proactionary Principle, that of weighing the probable risks with the probable benefits. However, the speculative effect on the economy cannot be considered as an overall wellbeing of the economy and cannot be strictly construed to equal the pleasure of the employee. In fact, various studies have indicated that an increase in the American economy has not been tied to an increase in the general American happiness.[75] Thus, the only meaningful pleasure that is foreseeable under a Bentham-esque analysis is the satisfaction of fulfilling a company directive. However, such joy is diminished where the fulfilment of the directive is a matter of necessity.[76]

Thus, under utilitarianism, the technological progress inspired by RFID microchip implanting might be otherwise impeded. This is, in a sense, what Transhumanism seeks to avoid. Because microchipping necessarily benefits the corporation rather than the employee, at least in the short term, a utilitarian philosophy dictates that the microchipping should not exist, as it will consistently cause more pain than pleasure for the microchipped individual. For this reason, Bentham's utilitarianism becomes overly restrictive against the potential long-lasting benefits that microchipping can provide to corporations and to the U.S. economy. However, transhumanism does not recklessly advocate for advancements in technology without regard for the subsequent effects on the individuals. While the Proactionary Principle does, in part, limit the consideration of the effect of the technology to those that are reasonable, transhumanism considers the movement of the species towards a sense of technological ascension and to discover new possibilities for ordinary living.[77] While Bentham and other philosophers might seek a more hedonistic result, transhumanism allows a level of "pain" on the individual level in order to achieve greater heights as a species.

However, Bentham's calculus is not entirely converse to the transhumanistic foresight embodied in the Proactionary Principle. Bentham recognized that pain and pleasure could both be measured in their propinquity, or how imminent the two are when performing the calculus.[78] This does not completely square away with transhumanism

75. *See, e.g.*, Ed Diener, *Beyond Money: Toward an Economy of Well-Being*, 5 PSYCHOL. SCI. IN THE PUB. INTEREST 1–31 (2004).

76. It is worth considering that studies are relatively conflicted in regards to whether or not such joy experienced by the employee feeds back into the company as a form of productivity or profit. *Cf., e.g.*, Cynthia D. Fisher, *Happiness at Work*, 12 INT'L J. MGMT. REVS. 384–412 (2010); Rhian Silvestro, *Dispelling the Modern Myth: Employee Satisfaction and Loyalty Drive Service Profitability*, 22 INT'L J. OPERATIONS & PRODUCTION MGMT. 30–49 (2002).

77. *See*, Julian Huxley, *Transhumanism*, 6 ETHICS IN PROGRESS 12–16 (2015).

78. BENTHAM, *supra* note 74.

since transhumanism seeks to create long-term benefits. Only in the final portion of the Proactionary Principle is there such a reference to an idea like propinquity—that imminent threats ought to receive priority over distant threats. Yet, there exists only a modest analogy for the pleasure where the threats are akin to the pain.

The Proactionary Principle values increased determinate pleasure more than increased hypothetical pleasure. This exists parallel to Bentham's concept of propinquity by extrapolation that a distant pleasure is, by its very nature, a more hypothetical pleasure or that it is too distant to matter. Still, the connection between the two on this point is that of divergence and not of convergence. While transhumanism pays heed to the time that it will take for the results to come to fruition and for the risks to fester in the meantime, the philosophy still allows for progression at a cost. This, crucially, is the backbone of transhumanism. Transhumanism does not blindly amble towards technological progress while ignoring the human cost. Nor is transhumanism unwilling to exert some pain in order to achieve a globalized future pleasure.

CONCLUSION

Relying on Max More's Proactionary Principle and Pearce's overtly hedonistic Bentham-esque ethical utilitarianism, RFID microchipping cannot be said to be a drastic or meaningful step towards post-humanism. The technology's risks outweigh the benefits and threats to the condition of the worker, while not actively propelling the human race further towards the ideal condition. Nonetheless, under the guidance of the Proactionary Principle, such a technological advance ought not be halted on the grounds of fearfulness or concerns about the results.

Therefore, consistent with Transhumanism, this Note concludes that law must be reshaped to allow for willing and interested employees to take part in RFID microchipping campaigns, but only where they are capable of withdrawing from the program or unwilling employees are able to reject the program without adverse ramifications. Given the limits of employment law in relation to at-will employees, the law must provide the best protections that it can without overreaching. California and Maryland's statutes preventing compulsion through coercive behavior such as denial of promotions strikes closest at providing a workable remedy that simultaneously allows interested employees the opportunity to test the technological waters, while leaving "bioconservatives," or those hesitant about this specific technology, to remove themselves from the initiative while remaining competitive in the workforce.

Rather than waiting on states to implement serviceable statutes that prevent employers from mandating microchipping or pressuring

employees to accept the microchipping for fear of not getting a promotion or bonus, the federal government should protect the advancement of the technology and employees' welfare by passing legislation that mirrors that of California and Maryland: no mandatory microchipping and no reliance on workplace pressures to ensure that employees consent. Such a law does not impede the flow of technology; rather, it increases workers' rights and legitimizes an interest in implanted privacy.