STOP BEFORE IT STARTS: REGULATING EMPLOYEE MICROCHIPPING IN THE COVID-19 ERA

Jarod S. Gonzalez[*]

[*] Jarod S. Gonzalez, J. Hadley Edgar Professor of Law, Texas Tech University School of Law, B.B.A., summa cum laude, University of Oklahoma, 1997, J.D., with highest honors, University of Oklahoma College of Law, 2000.

INTRODUCTION

Employment and employment law in the United States has changed dramatically since the World Health Organization declared COVID-19 to be a global pandemic on March 11, 2020.[1] After the declaration, many employers required employees to shift to remote work due to the health and safety risks of the coronavirus, and that trend will continue even after the pandemic subsides.[2] State and local governments issued a variety of shelter-in-place and stay-at-home orders that impacted both employers and employees.[3] "Essential" workers were required to work in the public and face the health and safety risks as new safety regimes evolved.[4] As state governments reopened their economies, more and more employees returned to work and experienced novel health and safety procedures and protocols to address the COVID-19 risks. Social distancing, mask requirements, temperature checks, and COVID-19 testing became the new normal in the workplace.[5] With all these changes, it may seem that employee privacy rights in the workplace are at a very low point.[6]

---

[1] *WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 - 11 March 2020*, WORLD HEALTH ORG. (Mar. 11, 2020), https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 [https://perma.cc/CB78-8SW5].

[2] Anne Fisher, *As Work From Home Becomes the Norm, Companies Get More Comfortable Hiring Fully Remote Employees*, FORTUNE (Apr. 7, 2020, 4:00 PM), https://fortune.com/2020/04/07/remote-work-from-home-jobs-hiring-coronavirus/ [https://perma.cc/XTD7-UFKG].

[3] *See generally* Cal. Exec. Order No. N-33-20 (Mar. 19, 2020); Fla. Exec. Order No. 20-91 (Apr. 1, 2020); N.Y. Exec. Order No. 202.8 (Mar. 20, 2020); Tex. Exec. Order No. GA-14 (Mar. 31, 2020).

[4] *See NSC Calls for Protection of Essential Workers*, OCCUPATIONAL HEALTH & SAFETY (Apr. 7, 2020), https://ohsonline.com/articles/2020/04/07/nsc-calls-for-protection-of-essential-workers.aspx (explaining the importance of essential workers' health during COVID-19) [https://perma.cc/S9Y9-8KRH].

[5] *See* Littler Mendelson, *Facing Your Face Mask Duties – A List of Statewide Orders*, LITTLER, https://www.littler.com/publication-press/publication/facing-your-face-mask-duties-list-statewide-orders [https://perma.cc/2FQ5-QWXA] (last visited Sept. 8, 2020).

[6] *See* Seyfarth Shaw, *COVID-19 and Workplace Privacy: Employers Beware*, EMP'T L. LOOKOUT: INSIGHTS FOR MGMT. (Apr. 14, 2020), https://www.laborandemploymentlawcounsel.com/2020/04/covid-19-and-workplace-privacy-employers-beware/ [https://perma.cc/Y2Z8-QB5K] ("It might strike some people that employees have diminished privacy rights during the current global health emergency caused by the coronavirus. However, this is not true. Employee privacy

In some ways, the coronavirus pandemic fear has flipped employee privacy laws on its head. Take the Americans with Disabilities Act ("ADA") provision on medical examinations of current employees as a prime example. The ADA provides that an employer may require an employee to submit to a medical examination as long as the examination is "job related and consistent with business necessity."[7] Pre-COVID-19, this generally meant that in order to require a medical examination of a current employee, the employer must have an individualized, reasonable belief that an employee's medical condition impairs the ability to perform essential job functions or that the employee poses a direct threat due to their health condition.[8] The individualized reasonable belief had to be based on evidence of current performance problems or observable objective medical evidence that an employee posed a danger to require a medical exam.[9]

Post-COVID-19, ADA law has done away with the individualized analysis needed prior to requiring medical examinations of employees as related to the coronavirus. On March 21, 2020, the U.S. Equal Employment Opportunity Commission ("EEOC") updated its guidance on interpreting the ADA in a pandemic to address the coronavirus disease.[10] Based on a guidance released in March 2020 from the Centers for Disease Control and Prevention ("CDC") and public health authorities, the

---

rights are still alive and well, but the circumstances in which employers – and the world – find themselves have changed.").

[7] 42 U.S.C. § 12112(d)(4)(A) (2020).

[8] U.S. EQUAL EMP'T OPPORTUNITY COMM'N, EEOC-NVTA-2000-1, QUESTIONS AND ANSWERS: ENFORCEMENT GUIDANCE ON DISABILITY RELATED INQUIRIES AND MEDICAL EXAMINATIONS UNDER THE AMERICANS WITH DISABILITIES ACT (July 27, 2000), https://www.eeoc.gov/laws/guidance/questions-and-answers-enforcement-guidance-disability-related-inquiries-and-medical [https://perma.cc/34J9-7U7L].

[9] *Id.* ("Generally, an employer may only seek information about an employee's medical condition when it is *job related and consistent with business necessity*. This means that the employer must have a reasonable belief based on objective evidence that: an employee will be unable to perform the essential functions of his or her job because of a medical condition; or, the employee will pose a direct threat because of a medical condition." (emphasis added)).

[10] *See* EQUAL EMP'T OPPORTUNITY COMM'N, EEOC-NVTA-2009-3, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT (Mar. 21, 2020), https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act [https://perma.cc/94CN-ZXLY] (noting the update was a direct result of COVID-19).

EEOC declared that the COVID-19 pandemic met the "direct threat" standard because the medical facts supported a finding that a significant risk of substantial harm would be posed by having someone with COVID-19, or symptoms of it, present in the workplace.[11] This declaration led to the EEOC's determination that employers may take employees' temperatures to determine whether they have a fever, administer viral COVID-19 tests to employees before permitting employees to enter the workplace, and ask employees about the presence of COVID-19 symptoms before entrance into the workplace.[12] None of these employer-required tests are based on an employer's individualized reasonable suspicion that the employees actually have COVID-19.[13] Thus, mandatory testing of all employees without individualized cause is viewed as necessary to further public health and safety goals.

COVID-19 also raises additional employment-related privacy concerns related to antibody testing and vaccinations of employees. As for antibody testing, medical professionals and legal commentators have opined on the potential use of antibody testing to screen employees as a helpful way to safely get employees back

---

[11] *See id.* Part II.B. of the EEOC's March 2020 update, Pandemic Preparedness Guidance states:

> Based on guidance of the CDC and public health authorities as of March 2020, the COVID-19 pandemic meets the direct threat standard. The CDC and public health authorities have acknowledged community spread of COVID-19 in the United States and have issued precautions to slow the spread, such as significant restrictions on public gatherings. In addition, numerous state and local authorities have issued closure orders for businesses, entertainment and sport venues, and schools in order to avoid bringing people together in close quarters due to the risk of contagion. These facts manifestly support a finding that a significant risk of substantial harm would be posed by having someone with COVID-19, or symptoms of it, present in the workplace at the current time. *Id.*

See also Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act, 29 C.F.R § 1630.2(r) (2012) (defining "direct threat" under the ADA as "a significant risk of substantial harm to the health or safety of the individual or others that cannot be eliminated or reduced by reasonable accommodation.").

[12] *See What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws [https://perma.cc/97KA-K6PJ] (last updated Sept. 8, 2020).

[13] *See generally id.*

to work quicker; however, the tests' accuracy is problematic and it is unclear how much exposure to the virus actually impacts one's immunity.[14] Favoring employees with immunity to the contagious disease over those with lack of immunity would be discriminatory and, presumably, such policies would have to be evaluated under a Bona Fide Occupational Qualification ("BFOQ") standard or direct threat standard.[15] The antibody testing does not test for a current COVID-19 infection; therefore, a positive antibody test does not discern whether the employee is a direct threat to others.[16] And a negative antibody test does not identify whether that employee is threatened by anyone else.[17] The EEOC's current position is that antibody tests are a "medical examination" under the ADA and do not meet the Act's "job related and consistent with business necessity" standard.[18] Therefore, consistent with CDC guidance, an employer cannot currently require that an employee submit to antibody testing before re-entering the workplace.[19]

---

[14] *See* Apoorva Mandavilli, *Coronavirus Antibody Tests: Can You Trust the Results?*, N.Y. TIMES (Apr. 24, 2020), https://www.nytimes.com/2020/04/24/health/coronavirus-antibody-tests.html [https://perma.cc/Y2YQ-F9DZ].

[15] *See* Debbie Kaminer, *Discrimination Against Employees Without COVID-19 Antibodies*, N.Y.L. J. (May 4, 2020, 10:00 AM), https://www.law.com/newyorklawjournal/2020/05/04/discrimination-against-employees-without-covid-19-antibodies/ [https://perma.cc/K5G3-K6T9] ("[A] requirement of COVID-19 immunity might not be justifiable in all workplaces and perhaps should be justified by some version or type of BFOQ.").

[16] *To Test or Not to Test: Taking Temperatures, Virus Testing, and Antibody Testing for COVID-19*, GREENWALD DOHERTY, https://greenwaldllp.com/to-test-or-not-to-test-covid-19/ [https://perma.cc/3TRM-ECKS] (last visited Sept. 10, 2020).

[17] *Id. See also* Catherine T. Barbieri & Liku T. Madoshi, *To Test or Not to Test? An Employer's Guide to COVID-19 Testing*, FOX ROTHSCHILD, LLP (May 11, 2020), https://www.foxrothschild.com/publications/to-test-or-not-to-test-an-employers-guide-to-covid-19-testing/ [https://perma.cc/GV5W-FY63].

[18] *See* EQUAL EMPLOYMENT OPPORTUNITY COMMISSION, *supra* note 12.

[19] *Id.* The EEOC responded to a question about whether the ADA allows an employer to require antibody testing before permitting an employee to return to work by stating:

> No. An antibody test constitutes a medical examination under the ADA. In light of CDC's Interim Guidelines that antibody test results 'should not be used to make decisions about returning persons to the workplace,' an antibody test at this time does not meet the ADA's 'job related and consistent with business necessity' standard for medical examinations or inquiries for current employees. Therefore, requiring antibody testing before allowing employees to re-enter the workplace is not allowed under the ADA. Please

The speed with which various vaccine trials for COVID-19 are proceeding means that the vaccination issue should likely end up overtaking the antibody testing issue as the more pressing employee privacy issue.[20] Now that the FDA has approved a vaccine, will state governments require all their residents to submit to mandatory COVID-19 vaccinations backed by criminal penalties for noncompliance?[21] Regardless of what state governments say, will employers be required, or permitted to require, that all employees prove they have received the COVID-19 vaccination as a condition of employment?[22] Employer-required mandatory vaccinations for the flu have been prevalent in the health care industry for a number of years, but the law has not previously blessed widespread vaccination requirements for employees outside the health care context.[23]

---

note that an antibody test is different from a test to determine if someone has an active case of COVID-19 (i.e., a viral test). The EEOC has already stated that COVID-19 viral tests are permissible under the ADA. *Id.*

[20] As of Dec. 21, 2020, the FDA approved COVID-19 vaccines by both Pfizer and Moderna, and distribution began immediately. *See* Dakin Andone, *US Sees Record Covid-19 Cases as CDC Advisory Group Votes to Recommend Moderna Vaccine*, CABLE NEWS NETWORK (last updated Dec. 19, 2020, 8:32 PM), https://www.cnn.com/2020/12/19/health/us-coronavirus-saturday/index.html [https://perma.cc/74RE-NDKB].

[21] In *Jacobson v. Massachusetts*, 197 U.S. 11, 11-12 (1905), the United States Supreme Court held that it was within the police power and authority of state governments to enact and enforce compulsory vaccination laws that criminalize refusal to comply with such mandates.

[22] In 2009, the EEOC opined in its Pandemic Preparedness Guidance within the context of an influenza vaccine that an employer's blanket policy requiring all employees to be vaccinated would violate the ADA and Title VII because of lack of exemptions for ADA-covered disability conditions and religious beliefs under Title VII where reasonable accommodation obligation exists. *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, EEOC-NVTA-2009-3, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT (Oct. 9, 2009), https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act [https://perma.cc/PH72-UBF5].

[23] Several states including Tennessee, Rhode Island, New York, New Hampshire, Nebraska, Massachusetts, California, and Colorado require hospitals to ensure their health care workers get the flu shot. John Murphy, *Can Your Hospital Fire You for Exercising Your Rights?*, MDLINX (Dec. 10, 2018), https://www.mdlinx.com/article/can-your-hospital-fire-you-for-exercising-your-rights/lfc-3148 [https://perma.cc/8QLR-KHRZ]. Even if not mandated by state law, some health care employers require their health care workers to get a flu shot as a condition of employment. *Id.*

Employer policies that mandate vaccination for employees relate to the Occupational Safety and Health Act's requirement that employers have a general duty to maintain a safe workplace for all employees.[24] Such policies also implicate federal and state employment discrimination laws because they affect the accommodation rights of disabled workers under the ADA and Title VII rights for employees who have religious beliefs that preclude vaccination.[25] If and when a safe and reliable FDA-approved COVID-19 vaccine is available, the legal questions surrounding conditioning employment on vaccination will demand an answer. The New York State Bar Health Law Section is one of the initial groups to stake out its position that "mandatory vaccinations for COVID-19 should be required in the United States" when the vaccine becomes available.[26] The group notes that a House Resolution introduced in 2019 would provide a limited exemption for individuals who have health issues that make it more dangerous than others to take the vaccine and are exempted by their doctors, but the group notably rejects any sort of religious exemption.[27] All the while, a May 2020 poll indicated a significant number of Americans will refuse a COVID-19 vaccine if it becomes available.[28]

Privacy issues in the workplace related to medical examinations and vaccinations for COVID-19 are expected to dominate employment law in the next few years. While it is unclear how all of those issues will play out, it is likely that employers will, at the very least, have flexibility to condition

---

[24] *See* 29 U.S.C. § 654(a)(1) (2020).

[25] *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, EEOC-NVTA-2009-3, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT (Oct. 9, 2009), https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act [https://perma.cc/93FB-TRKA].

[26] *Report of the New York State Bar Association's Health Law Section Task Force on COVID-19*, N.Y. ST. B. ASS'N, 60 (May 13, 2020), https://nysba.org/app/uploads/2020/05/HealthLawSectionTaskForceCOVID-19Report_5.13.20-1.pdf. [https://perma.cc/9FNQ-SQ6S].

[27] *See id.* at 60-62 (citing Vaccinate All Children Act of 2019, H.R. 2527, 116th Cong, (as introduced by Rep. Frederica Wilson, May 3, 2019)).

[28] *See* Lauren Frias, *A New Poll Found One in 5 Americans Said They'd Refuse a COVID-19 Vaccine, Which Companies are Racing to Create*, BUS. INSIDER (May 28, 2020, 1:31 AM), https://www.businessinsider.com/poll-some-americans-would-refuse-covid-19-coronavirus-vaccine-2020-5 [https://perma.cc/CJG9-DSY7].

employment on COVID-19 vaccination and that advocates will have to make persuasive arguments to hold on to the medical and religious exemptions to those vaccination requirements. At least with respect to balancing the right to work with public health and safety, governmental responses to COVID-19 indicate that public health and safety will likely largely win out over individual decision-making and employee privacy. If safety trumps privacy related to invading an employee's body, will convenience and efficiency trump privacy with respect to other invasions of an employee's body? One would hope not. The next generation privacy question concerns human microchipping of employees in the workplace.

The focus of this article is on regulating employee microchipping. The important points of this article are as follows. First, the law must prohibit employee microchipping as a condition of employment, penalizing any employee for refusing to be microchipped, or allowing an employer to access data from an employee microchip without the employee's permission. State legislatures should stop this upcoming problem of employers requiring their employees to be chipped as a condition of employment. Second, the "voluntary" use in the workplace of an employee's microchip implant, if even allowed at all, must be heavily regulated to protect employee privacy rights. States should enact their own employee microchipping statutes because the common law of employee invasion of privacy is too ambiguous to provide the certainty and clarity in the law that is necessary to protect employee privacy on this matter. Third, federal and state employment discrimination laws that provide accommodation rights for disabled and religious employees must be adhered to when employee microchipping issues arise in the workplace for protected individuals.

This article is divided into five parts. First, the introductory portion of this article will explain the human microchipping technology as it currently exists and how it may possibly be used in the future—especially by employers. Second, the article will examine how employee microchipping issues would be evaluated under the common law of employee invasion of privacy. Third, the article will explain how Title VII antidiscrimination accommodation principles are relevant to evaluating employee

microchipping issues in different contexts. Fourth, the article concludes that current common law and statutory protections related to employee microchipping are insufficient. Thus, state legislative responses for increased state statutory regulation of employee microchipping are required as a means of stopping the problem before it starts. Specifically, the article will highlight key aspects of well-drafted state anti-employee chipping statutes. Finally, this article will conclude with a summary of the main points of the article.

I. HUMAN MICROCHIPPING

In 1998, Kevin Warwick, a British scientist, became the first human being to receive a Radio Frequency Identification Technology ("RFID") microchip implant.[29] Since that time, numerous human beings have had the small RFID implants inserted into their bodies; the chip is typically inserted under the skin of the human hand.[30] The entire process of using a needle to place a microchip under a person's skin only takes a few minutes.[31] Human "[m]icrochip implants are essentially cylindrical bar codes that, when scanned, transmit a unique signal through a layer of skin."[32] The RFID/Near Field Communication ("NFC") technology on which the chip operates has been in existence for decades.[33] For example, the RFID technology has been used in the agricultural industry.[34] RFID tags have also been implanted into cattle to track and distinguish between different

---

[29] Haley Weiss, *Why You're Probably Getting a Microchip Implant Someday*, THE ATLANTIC (Sept. 21, 2018), https://www.theatlantic.com/technology/archive/2018/09/how-i-learned-to-stop-worrying-and-love-the-microchip/570946/ [https://perma.cc/6FZ6-QX55].

[30] Maddy Savage, *Thousands of Swedes Are Inserting Microchips Under Their Skin*, NAT'L PUB. RADIO (Oct. 22, 2018, 10:48 AM), https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin [https://perma.cc/72XU-UKGG].

[31] *See id.*

[32] Oscar Schwartz, *The Rise of Microchipping: Are We Ready for Technology to Get Under the Skin?*, THE GUARDIAN (Nov. 8, 2019, 5:00 A.M.), https://www.theguardian.com/technology/2019/nov/08/the-rise-of-microchipping-are-we-ready-for-technology-to-get-under-the-skin [https://perma.cc/CV39-PF67].

[33] *See* Charles Smith, *Human Microchip Implantation*, 3 J. TECH. MGMT. & INNOVATION 151 (2008) ("RFID technology began in WorldWar [sic] II . . . .").

[34] *Id.*

cattle brands and to prevent overfeeding.[35] The tags are also used to track consumer products in retail merchandise, track vehicles, airline luggage, and pet recoveries.[36] RFID chips have even been utilized in credit cards.[37]

It is estimated that in Sweden more than 6,000 people have had these small human microchips, around the size of a grain of rice, inserted into their hands.[38] Although human microchipping has occurred in various countries throughout the world, Sweden is the leader of the movement with top pioneers working to export human microchipping to other parts of Europe and throughout the world.[39] Proponents of human microchipping believe that over time millions of people will choose to be chipped because of the convenience and benefits that they argue it provides.[40]

Advocates for human microchipping point out various alleged benefits of this practice that largely focus on convenience. The human chips may be used to unlock doors and pay for consumer goods. Employees could immediately access employer facilities without a key, fob, or other similar device, and employers could immediately access pertinent employee information related to employment.[41] Human chips may store medical information of an employee that could be particularly important to access in a

---

[35] *Id.*

[36] *See* Kevin Bonsor & Wesley Fenlon, *How RFID Works*, HOWSTUFFWORKS, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm [https://perma.cc/Z2DL-5YSA] (last visited Sept. 10, 2020).

[37] *See* Weiss, *supra* note 29.

[38] *See* Stacey Naggiar, *People Are Getting Microchipped in Sweden, and It's Pretty Normal*, VICE NEWS (May 3, 2020, 7:59 AM), https://www.vice.com/en_us/article/y3madg/people-are-getting-microchipped-in-sweden-and-its-pretty-normal [https://perma.cc/3KEX-CLB2].

[39] Sweden has a history of being open to new technologies and is one of the most digitized countries in the world. "Ninety-seven percent of the [financial] transactions are done without bills." *Id.* The country has a stated goal of being a cashless society and the human chips would help to make cash and credit cards redundant. *See* Tony Winterburn, *Swedes Get Futuristic High Tech Implants in Their Hands to Replace Cash and Credit Car[d]s, Eliminating Coronavirus Contact*, EUROWEEKLY NEWS (Apr. 10, 2020), https://www.euroweeklynews.com/2020/04/10/swedes-get-futuristic-high-tech-implants-in-their-hands-to-replace-cash-and-credit-cars-eliminating-coronavirus-contact/ [https://perma.cc/9KA4-RV3P].

[40] *See id.*

[41] *See* Robert Connor, *Microchipping Humans — Pro's and Con's*, NOW FUTURE TECH, https://nowfuturetech.com/microchipping-humans-pros-and-cons/ [https://perma.cc/667R-3VSU] (last visited Sept. 10, 2020).

medical emergency.[42] It has been contended that the use of this technology could particularly assist employees with certain disabilities.

The RFID/NFC technology that supports the human microchipping movement presents plenty of privacy problems for employees who are chipped. The downsides of this technology are substantial, which include violations of personal privacy, theft and misuse of personal data, governmental and corporate surveillance, and infringement on religious liberties.[43] Proponents of human microchipping argue that the chipped individual is in control of their own data stored on the chip. The RFID microchip technology allows the individual to control who has access to the information in the chip.[44] Still, there is a risk of the information on the chip being stolen or hacked.[45] Moreover, the more-sophisticated microchips are now being "powered by human … heat and include[] GPS tracking capabilities and voice activation[,]" which raises the potential of employer tracking of employee movements.[46]

---

[42] RFID implants are being developed to continually monitor an individual's vital signs, which could allow "patients and doctors to access highly accurate real-time information." *See* Weiss, *supra* note 29.

[43] *See* Connor, *supra* note 41. As explained later in the article, the technology implicates religious rights of certain Christians who view human microchipping as indicating the "Mark of the Beast" from Revelations.

[44] *See* Hope Reese, *Microchip Implants Help Employees Access Data; Experts Worry About 'Slippery Slope' for Privacy*, TECH REPUBLIC (Apr. 14, 2017, 4:00 AM), https://www.techrepublic.com/article/microchip-implants-help-employees-access-data-experts-worry-about-slippery-slope-for-privacy/ [https://perma.cc/E9C8-93GT] (noting RFID microchips are "passive" and cannot "send signals about location-based data" and the power and transfer of data has to come from a device that is in "close contact with the chip").

[45] *See* Shainaz Firfiray, *Microchip Implants are Threatening Workers' Rights*, THE CONVERSATION (Nov. 22, 2018, 6:20 AM), https://theconversation.com/microchip-implants-are-threatening-workers-rights-107221 [https://perma.cc/2FS8-MWSZ] ("Some research also suggests that implanted chips are susceptible to security risks and increase the potential for identify theft given that it is relatively easy to hack a microchip implant. So employees could be subjected to something that actually threatens their personal security.").

[46] Peter Holley, *This Firm Already Microchips Employees. Could Your Ailing Relative be Next?*, WASH. POST (Aug. 23, 2018, 3:48 PM), https://www.washingtonpost.com/technology/2018/08/23/this-firm-already-microchips-employees-could-your-ailing-relative-be-next/ [https://perma.cc/37JG-AXJE].

The COVID-19 pandemic is demonstrating how GPS technology, as applied to contact tracing, presents realistic privacy concerns. Governments and corporate actors are promoting the use of invasive digital contact tracing apps on cell phones that monitor an individual's movements so that people who are more likely to be exposed to the coronavirus will self-isolate and prevent the spread of the virus.[47] Critics argue that these surveillance tools are unjustified and wrongfully interfere with individual privacy rights.[48] These same digital tracing and movement tracking techniques could be undertaken by employers via an employee's microchip in the future. History suggests that when employers are legally permitted to use technology to further efficiency and convenience, they will use it. Absent appropriate regulation, current and future technological developments present very real risks that employees with implanted microchips will turn over autonomy of their movements and personal information to corporate and governmental actors in an unprecedented and problematic way. The following explains how the common law of employee privacy provides some privacy protections for the use of employee microchips in the workplace but is nonetheless insufficient.

II. HUMAN MICROCHIPPING AND COMMON LAW EMPLOYEE PRIVACY RIGHTS

An employer who requires that an employee submit to an invasive microchipping procedure and that certain employment-related information be stored on the chip and be accessible to the

---

[47] *See* Jason Horowitz & Adam Satariano, *Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation*, N.Y. TIMES (June 16, 2020), https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html [https://perma.cc/984H-67T2]; Kelly Servick, *COVID-19 Contact Tracing Apps are Coming to a Phone Near You. How Will We Know Whether They Work?*, SCIENCE (May 21, 2020, 5:10 PM), https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how [https://perma.cc/3H7R-7FTB].

[48] *See, e.g.*, *Bahrain, Kuwait and Norway Contact Tracing Apps Among Most Dangerous for Privacy*, AMNESTY INT'L (June 16, 2020, 6:40 AM), https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ [https://perma.cc/FY49-QW7D] ("Bahrain, Kuwait and Norway have run roughshod over people's privacy, with highly invasive surveillance tools which go far beyond what is justified in efforts to tackle COVID-19.").

employer should violate the employee's common law privacy rights. However, it is arguable whether an employee's common law privacy rights are violated if the employee has voluntarily agreed to be chipped and agreed that the employer may access various information that is stored on the chip. To the extent that accessing an employee's microchip in the workplace could be viewed as legal, legality would turn on whether society is willing to accept the employee's "consent" to the employer swiping their chip and accessing their information as informed, voluntary, and valid, which overrides the employee's reasonable expectation of privacy in their physical person.

The classic formulation of common law privacy rights focuses on four distinct types of invasions: "(1) intrusion upon seclusion, (2) public disclosure of private facts, (3) publicity placing a person in a false light, and (4) misappropriation of a person's name or likeness."[49] "Of the[se] four privacy torts, the first three are [the] most relevant in the employment [law] context[,]"[50] and the intrusion upon seclusion tort is the one that appears to be most relevant to the use of the human microchip in the workplace.[51]

Many jurisdictions recognize the availability of a common law invasion of privacy claim for intrusion upon seclusion in the employment context.[52] In general, it is unlawful for an employer to intentionally intrude, physically or otherwise, on the seclusion or solitude of an employee "if the intrusion would be highly offensive to a reasonable person."[53] In the employment context, an employee "has a reasonable expectation of privacy" in aspects relating to the employee's physical person and the employee's physical or

---

[49] RESTATEMENT OF EMP'T LAW § 7.01 cmt. a (AM. LAW INST. 2015); *see also* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (AM. LAW INST. 1977).

[50] RESTATEMENT OF EMP'T LAW § 7.01 cmt. a (AM. LAW INST. 2015).

[51] The Restatement of Employment Law is a useful tool through which to view invasion of privacy in the employment context because it presents a compilation of generalized principles of employee privacy law and will provide a good background for considering the employee privacy rights related to mandatory vaccinations and employee microchipping in this article.

[52] *See, e.g.*, Muick v. Glenayre Elecs., 280 F.3d 741, 743-744 (7th Cir. 2002); Frye v. IBP, Inc., 15 F. Supp. 2d 1032, 1040 (D. Kan. 1998); Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1133 (Alaska 1989); Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 383 (Mich. Ct. App. 1989); Farrington v. Sysco Food Servs., Inc., 865 S.W.2d 247, 253 (Tex. Ct. App. 1993).

[53] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

electronic location.[54] Moreover, the employee has an interest in not disclosing to the employer "information of a personal nature."[55]

A. Physical Intrusion

An employee has a protected privacy interest in their physical person, which includes the employee's body.[56] An employer's requirement that an employee be microchipped as a condition of employment physically intrudes upon the employee because the employee must submit to an invasion of the employee's body when the employee's hand is cut open and the chip placed inside. This chipping invasion of the body is somewhat analogous to the intrusion that occurs when an employer requires an employee to submit to vaccination as a condition of employment—although human microchipping is arguably more invasive. Both vaccination and human microchipping require penetration of the human skin. It has been recognized that less invasive intrusions, such as providing urine samples to test for unlawful drug use as a job requirement, intrude upon an employee's protected privacy interest.[57] Moreover, every time the employer scans the chip to access the employee's pertinent information, it is engaging in an intrusive "search" of the employee's physical body.[58]

---

[54] RESTATEMENT OF EMP'T LAW § 7.02(a) (AM. LAW INST. 2015).

[55] *Id.* § 7.02(b).

[56] *Id.* § 7.03(a)(1) ("An employee has a protected privacy interest against employer intrusion into [] the employee's physical person, bodily functions, and personal possessions[.]"); *see also id.* § 7.03 cmt. b (noting protected privacy interest in the employee's physical person includes the employee's body).

[57] *See id.* § 7.03 cmt. b ("An employer's job requirement that an employee provide a urine sample as part of a test for unlawful drug use is an intrusion into a protected privacy interest."). *But see*, Rushing v. Hershey Chocolate- Memphis, No. 99-5802, 2000 U.S App. LEXIS 27392, at *6-9 (6th Cir. Oct. 19, 2000) (rejecting invasion of privacy claim because there was no explanation as to how the employee's refusal to take a drug test was an unlawful intrusion).

[58] An employer's search of an employee's personal possessions like a purse or wallet has been viewed as an intrusion upon an employee's protected privacy interests. *See* RESTATEMENT OF EMP'T LAW § 7.03 cmt. b (AM. LAW INST. 2015). A search of an employee's personal possession, such as microchip within the body, is arguably even more of an intrusion than a search of an employee's personal possession worn outside the body.

B. Electronic Intrusion

To the extent that the employer is improperly accessing information from the employee's microchip, there is an electronic intrusion merely because private data is being improperly accessed electronically. Under the Restatement of Employment Law, "locations" are defined very broadly to include "particular places or sites that can be accessed physically or electronically."[59] So, whether an employee's data is stored on a laptop computer, cell phone, within a cloud computing system, or on a human microchip, the key point is that the improper accessing of data stored on that system is an intrusion.[60]

C. Highly Offensive to a Reasonable Person

In general, "[a]n employer is subject to liability for a wrongful intrusion upon an employee's protected privacy interest" only if the violation of that privacy interest "would be highly offensive to a reasonable person under the circumstances."[61] This inquiry considers the "nature, manner, and scope of the intrusion" and balances the intrusion against the "employer's legitimate business interests or the public's interests in intruding."[62] Legitimate business interests of the employer include the employer's ability to manage the employee's ongoing job performance, effectively conduct its business, maintain its reputational interest in the marketplace, and adhere to its legal rights and responsibilities.[63]

---

[59] *Id.* § 7.03 cmt. c (noting an intrusion is accomplished whether or not a physical space is associated with an electronic location by accessing data electronically from that location).

[60] *See id.* § 7.03 cmt. d. The privacy protection for an employee should be the same regardless of whether or not a human microchip is viewed as a workplace or nonworkplace physical or electronic location.

[61] *Id.* § 7.06(a). The employee generally has the burden of persuasion to prove that the employer has intruded upon a protected privacy interest and that the intrusion is highly offensive. *See* Mauri v. Smith, 929 P.2d 307, 311-12 (Or. 1996).

[62] RESTATEMENT OF EMP'T LAW § 7.06(b) (AM. LAW INST. 2015).

[63] *Id.* § 7.06 cmt. c (explaining "legitimate business interests," the Restatement provides: "Courts look to the justifications for the intrusion in evaluating its offensiveness. Those justifications can be broken down into two categories: (1) the employer's business interests; and (2) third-party or public interests. Legitimate business interests in the first category are those that affect the employer's ability to conduct its business effectively. These interests relate not only to the employee's

Public interests beyond the employer's interest include safety of third-parties and the overall public, transparent institutional or governmental processes, the necessity to obtain information related to a lawsuit or some other public proceeding, and the interest in securing enforcement and compliance with the law.[64] In some cases, the employer's actions in intruding upon the employee's privacy are so extreme and unwarranted that there is a violation of the privacy right.[65] In other cases, the employer's legitimate interests are so compelling and obvious that there is no invasion of privacy violation.[66] Then there are the more difficult cases that are in the middle.[67]

An employer that compels employees to submit to a mandatory COVID-19 vaccination as a condition of employment is severely intruding upon the seclusion of an employee, but the employer has a substantial interest in maintaining a safe workplace for all of its employees, customers, and other third parties and in avoiding litigation related to individuals who are exposed to COVID-19 in the workplace. There is also a public interest in maintaining the health and safety of employees and the public, which required employee vaccinations would further. For these reasons, the employer's interest and public's interest in health and safety may outweigh the employee's privacy interests in preventing a mandatory COVID-19 vaccination if such vaccination is proven to be safe and reliable.

The human microchipping case is a much different story. Compelling employee microchipping and then conducting

---

ongoing performance, but also to the employer's reputation in the marketplace and legal rights and responsibilities.").

[64] *Id.* § 7.06 cmt. d ("Public interests extend beyond a particular employer's interests. For employees in safety-sensitive positions, for example, courts have ruled that workplace testing for illegal drug use furthers not only the employer's business interests but also the public's interest in the reliable, safe delivery of services. Other public-policy interests that an intrusion may serve include the transparency of governmental or institutional processes; the need to obtain information relevant to a lawsuit or other public proceeding; and the interest in securing compliance with and enforcing the law.").

[65] *Id.* § 7.06 cmt. b ("In some cases, the employer's conduct is so extreme or the scope or manner of the intrusion so patently improper that the employer must make a compelling showing of business justification to avoid liability.").

[66] *Id.* (noting the public interest or business purpose can be "so clear as to be decisive.").

[67] *See id.*

"searches" of the information in the chip is beyond the pale of what is acceptable in society and would likely be, *per se,* highly offensive to a reasonable person. The nature and manner of the intrusion concerns a physical opening of the skin, a foreign object being placed underneath the skin, and then a scanning of that device by invading the human body and accessing personal information. In today's society, individuals are accustomed in certain settings to present their fingerprint for purposes of a scan to verify identity or to invasive scans and searches of their body at airports. Individuals also make personal choices to implant certain devices like pacemakers into their body for medical or other reasons, but this is much different than a required cutting open of the body to place an electronic device that must then be maintained in the body and that the employer may then access data on. The employer's business interests in requiring chipping have to do with convenience and efficiency and they fall well short of the public health and safety concerns that may justify the employer's ability to compel employee vaccinations for COVID-19. The information that the employer is accessing from the employee's microchip would seem to be available from other noninvasive sources.

D. Consent

In 2017, Three Square Market, a River Falls, Wisconsin company that provides self-service mini-markets to hospitals, hotels, and company break rooms, held a big event where approximately fifty employees were *voluntarily* microchipped.[68] These "chipped" employees use the chip regularly at work for activities like entering the office, logging on to computers, buying food and drinks in the company cafeteria, and storing basic identifying and medical information about themselves.[69] By 2018,

---

[68] *See* Jeff Baenen, *Aug. 2, 2017: Wisconsin Company Holds 'Chip Party' to Microchip Workers*, CHI. TRIB. (Aug. 2, 2017, 7:32 AM), https://www.chicagotribune.com/business/blue-sky/ct-wisconsin-company-microchips-workers-20170801-story.html [https://perma.cc/5BKW-VW57].

[69] *See* Rachel Metz, *This Company Embeds Microchips in Its Employees, and They Love It*, MIT TECH. REV. (Aug. 17, 2018), https://www.technologyreview.com/2018/08/17/140994/this-company-embeds-microchips-in-its-employees-and-they-love-it/ [https://perma.cc/6VZQ-Q4YR].

an additional thirty employees were voluntarily chipped; at that point, approximately a third of the company's workforce were "cyborgs."[70]

The company's position is that all chipped employees voluntarily agreed to the chipping and so effectively consented.[71] However, the mere fact that an American company is promoting a chipping program for its employees raises questions about what effective legal consent should really look like for such conduct under this country's employee privacy laws. If an employee truly desires the insertion of a chip and wants to use the chip in the workplace for convenience and other purposes, in one sense, what is the harm? The problem is it may be difficult to ascertain in certain circumstances whether consent is really voluntary. And it is important to consider whether chipping in the workplace could ever be truly, legally voluntary for purposes of avoiding an invasion of privacy claim. The following portion of the article presents various circumstances regarding employee microchipping and presents arguments as to whether the law should conclude that effective consent to the microchipping exists.[72]

Consent is defined in Section 892 of the Restatement (Second) of Torts as "willingness in fact for conduct to occur. It may be manifested by action or inaction and need not be communicated to the actor."[73] The general principle is that effective consent is a complete defense to an intentional tort. Consent precludes recovery in tort for the conduct or harm resulting from the conduct that was consented to.[74]

---

[70] *Id.* (noting approximately 80 of the 250 employees had chips).

[71] *See id.*

[72] Once again, the Restatement of Employment Law on employee invasion of privacy is instructive for this analysis and will be utilized. For public employees, a similar Fourth Amendment analysis would apply.

[73] RESTATEMENT (SECOND) OF TORTS § 892(1) (AM. LAW INST. 1977).

[74] *Id.* § 892A(1) ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it."). *See also,* RESTATEMENT OF EMP'T LAW § 706 cmt. h (AM. LAW INST. 2015).

1. Employee Consent for Microchipping Obtained as a Condition of Retaining Current Employment

In an at-will rule world, there are examples of terms and conditions of employment that an employer imposes on an employee on a "take it or leave it" basis, and courts enforce the "agreement" to the conditions.[75] This is the idea that consent in any form is effective regardless of the risk of unemployment.[76] But the better view for such a significant intrusion as employee microchipping is that consent based on the threat of termination of employment is ineffective. To be valid, consent must be freely and voluntarily given; taking an employee's job away for refusing to be chipped is not a voluntary consent but actually looks more like duress.[77]

2. Employee Consent for Microchipping Obtained as a Condition of Initial Employment

Consent obtained as a condition of initial employment yields the same result as the prior employee situation. Courts sometimes see the equities as favoring the employer when consent is obtained as a condition of initial employment on the basis that applicants who accept the job know what they are getting into, and if they did not like the condition, applicants could just walk away.[78] The

---

[75] *See* In re Halliburton Co., 80 S.W.3d 566, 568-73 (Tex. 2002) (enforcing employer's mandatory arbitration program imposed on the at-will employee on a "take it or leave it" basis as a condition of employment).

[76] *See* Jennings v. Minco Tech. Labs, Inc., 765 S.W.2d 497, 502 (Tex. Ct. App. 1989) (finding employee's consent to a drug test waived any privacy claim even though consent was provided by employee only to keep her job).

[77] *See* RESTATEMENT OF EMP'T LAW § 706 reporter's note to cmt. h (AM. LAW INST. 2015) ("The general rule should be that an employee does not voluntarily consent if the alternative is termination."); Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia, 812 F.2d 105, 111 (3d Cir. 1987) (under Pennsylvania's privacy laws, "[t]ests applied as a prerequisite for continued employment are hardly to be considered voluntary.").

[78] *See* RESTATEMENT OF EMP'T LAW § 706 reporter's note to cmt. h ("Consent obtained as a condition of initial employment is more favorably received by the courts [than consent obtained by imposing a new condition on a current employee] on the ground that the employee knew what she was getting into when she took the position."); Feminist Women's Health Ctr. v. Superior Court, 61 Cal. Rptr. 2d 187, 195 (Cal. Ct. App. 1997) (rejecting privacy claim, in part, because the employee had agreed to perform certain job duties at the outset of her employment).

idea is that it is easier for the applicant with the job offer to walk away from the job than it would be for a current employee. But, once again, the nature of the employee microchipping intrusion is so substantial, and the applicant's need for the job may be so strong that there is inherent coercion here and not really voluntary consent.

3. Employee Consent for Microchipping Where the Chipped Employee Receives No Benefit or Detriment for the Consent, and Unchipped Employees are Not Penalized for the Lack of a Chip

The best-case scenario for effective consent is when there is an absence of any penalty or incentive for an employee to be chipped. The employee who decides to be chipped and allow the employer to access information in the chip is treated no worse or better than the employee who declines to be chipped. One of the foreseen problems with this no "tangible advantage" approach is that as more employees adopt the chips over time, there will be more pressure for holdouts to acquiesce and agree to the chip and at some point, the chipping of employees is the only practical option.[79] Furthermore, thorny issues regarding consent would have to be worked out. Perhaps informed consent concepts should require the employer to specify to the employee all the known risks of the chips and a mechanism by which the employee could easily revoke the employer's right to access information in the chip is established.[80] Perhaps effective consent for access of an

---

[79] *See* Mary Colleen Charlotte Fowler, *Chipping Away Employee Privacy: Legal Implications of RFID Microchip Implants for Employees*, NAT'L L. REV. (Oct. 10, 2019), https://www.natlawreview.com/article/chipping-away-employee-privacy-legal-implications-rfid-microchip-implants-employees [https://perma.cc/RR9D-ZFB5] ("Employers asking employees to implant microchips may become so standard that even if an employee has the opportunity to refuse implantation, it would still be to their detriment.").

[80] *See id.* ("States should incorporate informed consent into their [own] statutes. . . . In addition to informed consent, legislators should include provisions allowing for an individual to easily revoke consent, so employees could have it removed without fear of retaliation from their employer.").

employee's microchip in the workplace should not be permitted at all.[81]

The common law of employee invasion of privacy would likely be consistently applied by jurisdictions to deny the employer the right to condition employment on the employee agreeing to an implant and the accessing of data from the microchip. But beyond that, courts that look to interpret or develop common law employee invasion of privacy principles as applied to *voluntary* employee microchipping would struggle to deal with the consent issue. The common law alone probably allows for too much ambiguity on whether employee privacy rights are protected in many employee microchipping contexts. These difficult employee microchipping issues call for a nuanced approach that is better addressed through targeted legislation enacted by our representatives and not through common law development by judges. As explained later in this article, the need for detailed and focused statutory regulation on employee microchipping is significant.

III. ACCOMMODATION LAW

In addition to common law employee privacy law, both ADA accommodation law and Title VII religious accommodation law will affect the rights of employees on the microchipping issue. ADA accommodation laws may otherwise compel the use of employee microchips in the workplace for certain disabled employees even if an employer was not inclined to permit such use or if state law prohibited such action. On the flip side, in an imagined world where someday employee microchipping may be the norm and required by employers, employers will need to accommodate employees under Title VII who do not want to be microchipped for religious reasons.

A. ADA Disability Accommodation

If an employer has a general rule or policy that precludes it from accessing information on an employee with a microchip (or a state statute prohibits such action), an employee with a disability

[81] *Id.* (opining that states could consider an outright ban on employee microchip use in the workplace).

may contend that it needs to use the chip in the workplace to perform job functions.[82] For example, an employee unable to use their arms may have difficulty utilizing keys or fobs or logging into a computer, and the employee's microchip would facilitate the accomplishment of those tasks.[83] In this situation, an employer may have a duty to allow the employee to use the human microchip in the workplace in order to fulfill its accommodation obligations under the ADA.[84] As the human microchipping technology develops, and as technology affects how employees do their work, there will likely be an even greater need for employees with certain disabilities to use their human microchips to have equal employment opportunities in the workplace.

B. Title VII Religious Accommodation

Some Christians have opposed or expressed concern for human microchipping on religious grounds.[85] The religious belief is that an implanted chip may be the "Mark of the Beast" from the Biblical New Testament's Book of Revelation.[86] In the scriptural passages, believers are warned to avoid the "Mark of the Beast" as it signals the worshiping of the Antichrist and manipulation of the believer.[87] If employers are ever permitted by law to require employees to have a microchip implantation, employees who have

---

[82] Under the ADA, a disability is defined as "a physical or mental impairment that substantially limits one or more major life activities of such individual[.]" 42 U.S.C. § 12102(1)(A) (2020).

[83] *See Microchips in Humans: Great Promise, Greater Risk?*, PBS NEWSHOUR (Jan. 31, 2019), https://www.pbs.org/video/microchipping-1548896453/ [https://perma.cc/KXS2-2B6R] (describing how an individual who suffers from a condition where he has no arms uses the microchip to access doors, computers, and store important medical information).

[84] Under the ADA, a "qualified individual" with a disability is an "individual who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires." 42 U.S.C. § 12111(8) (2020). "Reasonable accommodation" may include "making existing facilities used by employees readily accessible to and usable by individuals with disabilities." *Id.* at § 12111 (9)(A).

[85] *See* Holly Meyer, *'Mark of the Beast?' Microchipping Employees Raises Apocalyptic Questions*, THE TENNESSEAN, (Aug. 4, 2017, 5:47 PM), https://www.tennessean.com/story/news/2017/08/04/mark-beast-microchipping-employees-raises-apocalyptic-questions/538162001/ [https://perma.cc/CC75-SSX9].

[86] *Id.*

[87] *See Revelation* 13:16-18, 14:9-11 (New King James).

a religious belief that precludes them from being chipped should be excused from that requirement as a religious accommodation.

Although not a microchip case, the Fourth Circuit Court of Appeal's decision in *EEOC v. Consol Energy, Inc.* is instructive on how employer-required technology use may infringe upon the religious beliefs of employees and require accommodation.[88] In *Consol Energy*, the employer utilized a biometric hand-scanner system in order to track its employees.[89] The hand-scanning system helped the employer "to better monitor the attendance and work hours of its employees."[90] One employee, an Evangelical Christian, refused to use the system because of his religious beliefs.[91] The employee sincerely believed in the Antichrist and that "the Antichrist"s followers are condemned to everlasting punishment."[92] The employee believed from the Book of Revelation that the Mark of the Beast brands one as a follower of the Antichrist, which allows the Antichrist to manipulate that individual.[93] The employee feared that his use of the employer's hand-scanning system "would result in being so 'marked,' for even without any physical or visible sign, his willingness to undergo the scan" with either of his hands "could lead to his identification with the Antichrist."[94]

The employee requested to be excused from the hand-scanning requirement as a religious accommodation, which the employer denied.[95] The case went to trial and the jury returned a verdict in favor of the employee.[96] The appellate court affirmed the judgment in favor of the employee.[97] Trial testimony revealed that the employer excused other employees with hand injuries from the scanning requirement and allowed those individuals to enter their

---

88 860 F.3d 131 (4th Cir. 2017).
89 *Id.* at 136.
90 *Id.* at 137.
91 *Id.* at 136-37.
92 *Id.* at 137.
93 *Id.*at 137-38.
94 *Id.* at 138.
95 *Id.* at 138-39.
96 *Id.* at 140.
97 *Id.* at 143.

personnel numbers on a keypad attached to the system, but the religious objector was denied that same right.[98]

The employer primarily tried to defend its actions by arguing that the employee had misinterpreted the relevant passages from the Book of Revelation regarding the Mark of the Beast, but the appellate court rejected the argument.[99] What mattered was that the employee's belief was a sincerely held religious belief and the jury had so found. It was therefore irrelevant how the employer interpreted Revelation, or even that the employee's pastor may have disagreed with the employee's interpretation of the scripture passage.[100] At that point, the case was a relatively easy decision for the appellate court because the reasonable accommodation/undue hardship defenses for a Title VII religious accommodation claim were not defensible.[101] The employer admitted that allowing the religious employee to bypass the scanner and enter his personnel number would have imposed no additional costs or burdens on the company.[102] And this was backed up by the fact that in the same communication that the employer denied the accommodation from hand-scanning for the religious employee, it granted the same accommodation to two similarly-situated employees with hand injuries.[103]

Consol Energy was correctly decided and there are lessons to be learned from the Fourth Circuit's opinion as applied to a potential employer requirement that an employee be microchipped and have information on their chip scanned by the employer. First, putting all other possible employment regulations to the side on this issue and looking at the issue solely under Title VII, an employee who has a sincere religious belief that conflicts with

---

[98] *See id.* at 138-39.

[99] *Id.* at 142-43.

[100] *Id.*

[101] *See id.* at 143.

[102] *See id.* at 138-39. Under Title VII, "[t]he term 'religion' includes all aspects of religious observance and practice, as well as belief, unless an employer demonstrates that he is unable to reasonably accommodate to an employee's or prospective employee's religious observance or practice without undue hardship on the conduct of the employer's business." 42 U.S.C. § 2000e(j) (2020). In *Trans World Airlines, Inc. v. Hardison*, 432 U.S. 63, 84 (1977), the U.S. Supreme Court held that requiring the employer to bear anything more than a de minimis cost in meeting its reasonable accommodation obligations under Title VII is an undue hardship.

[103] *See Consol Energy, Inc.*, 860 F.3d at 143.

the employer's microchipping requirement is entitled to the consideration of excuse from the requirement. It is no matter that the employer would disagree with the religious view. Second, whether an employer could prove that no reasonable accommodation exists or there is undue hardship in accommodating the religious employee from a microchip requirement will depend on the additional cost and burden the employer bears in providing such accommodation. In *Consol Energy*, it was easy to see that there was very little to no additional burden on the employer to allow the accommodation.[104] In a microchip situation, allowing religious employees an alternative mechanism to meet employer requirements that do not involve the insertion of a microchip into the employee and the accessing of that information should not be too burdensome on the employer. There should be a societal expectation that employers provide such religious accommodations as a matter of course to employees who refuse to be chipped, even though the undue hardship standard for employers is relatively low. Finally, a more basic principle of equal treatment of employees with sincerely held religious beliefs: an employer cannot fail to provide accommodations to a religious employee if it willingly provides those same accommodations to a similarly-situated non-religious employee.

IV. LEGISLATIVE RESPONSES

Over the last few years, a small but growing number of state legislatures have taken action to regulate human microchipping. Several states have enacted general human microchipping bans that typically make it a crime or a civil violation for an individual to be forced to have an implanted microchip inserted into his or her body.[105] Five states—Arkansas, Indiana, Missouri, Montana,

---

[104] *See id.* at 138-39.

[105] The states are California, Maryland, North Dakota, Oklahoma, and Wisconsin. *See* CAL. CIV. CODE § 52.7(a) (West 2020) ("Except as provided in subdivision (g), a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device."); *Id.* § 52.7(b)(1) ("Any person who violates subdivision (a) may be assessed an initial civil penalty of no more than ten thousand dollars ($10,000), and no more than one thousand dollars ($1,000) for each day the violation continues until the deficiency is corrected."); MD. CODE ANN. HEALTH-GEN. § 20-1902(a) (West 2020) ("A person or an agent, a representative, or a designee of

and Nevada—have enacted statutes that are specifically targeted at regulating employee microchipping in some way, presumably with the idea that the common law of employee privacy is insufficient to address the problem.[106] Similar bills banning employee microchipping are pending in the Iowa and Tennessee Legislatures.[107] Thus, the issue is starting to gather the attention of more politicians, policy makers, and the public.

Some critics of the legislative actions on employee microchipping say that these actions are unnecessary as they are merely a solution in search of a problem.[108] In contrast with Europe, there has been relatively little voluntary microchipping of employees by employers in the United States, and no known reports of employers forcing employees to be chipped.[109] Critics

---

the State or a local government may not require, coerce, or compel an individual to undergo the subcutaneous implanting of an identification device."); N.D. CENT. CODE ANN. § 12.1-15-06 (West 2019) ("A person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device. A violation of this section is a class A misdemeanor."); OKLA. STAT. ANN. tit. 63, § 1-1430(A) (West 2020) ("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."); *Id.* § 1-1430(B) ("The State Department of Health may impose a fine not to exceed Ten Thousand Dollars ($10,000.00) on any person who violates this act. Each day of continued violation shall constitute a separate offense."); WIS. STAT. ANN. § 146.25(1) (West 2020) ("No person may require an individual to undergo the implanting of a microchip."); *Id.* § 146.25(2) ("Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense.").

[106] *See* ARK. CODE ANN. § 11-5-501 (West 2020); IND. CODE ANN. §§ 22-5-8-1 to 22-5-8-4 (West 2020); MO. ANN. STAT. § 285.035 (West 2020); MONT. CODE ANN. §§ 39-2-1501 to 39-2-1503 (West 2019); NEV. REV. STAT. ANN. § 200.870(1)(b) (West 2020).

[107] The Iowa Judiciary Committee unanimously advanced H.F. 580, a bill banning employee microchipping, in February 2020 through Iowa's legislative process. *See* Shane Vander Hart, *Iowa House Bill Prohibiting Mandatory Microchipping of Employees Advances*, CAFFEINATED THOUGHTS (Feb. 14, 2020), https://caffeinatedthoughts.com/2020/02/iowa-house-bill-prohibiting-mandatory-microchipping-of-employees-advances/ [https://perma.cc/HDF5-AMVE]. Similarly, a general bill banning mandatory human microchipping is pending in Tennessee. *See* H.B. 1418, Gen. Assemb., 111th Sess. (Tenn. 2019).

[108] *See* Dave Royse, *States Just Saying No to Employee Microchipping*, ST. NET CAP. J., LEXISNEXIS, https://www.lexisnexis.com/en-us/products/state-net/news/2020/03/13/states-just-saying-no.page [https://perma.cc/G5UZ-MYU6] (noting Indiana Legislature's Nonpartisan Legislative Services Agency indicated that employee microchipping has not been a problem in Indiana or anywhere else in the country yet).

[109] *See* IND. OFFICE OF FISCAL & MGMT. ANALYSIS, FISCAL IMPACT STATEMENT: H.B. 1143 (Feb. 24, 2020), http://iga.in.gov/legislative/2020/bills/house/1143#document-

may question the need for legislation right now if no practical problem currently exists.

While there may be cases where legislatures act too quickly to regulate new technologies in society and end up doing more harm than good, that would not be the situation with employee microchipping. It makes sense to get in front of the implant issue. The states that have already acted with legislation and those that act in the near future are preemptively trying to get ahead of the curve as legislators understand the inherent dangers to privacy and religious liberty that the use of this technology has the potential to impose.[110] While general societal preferences right now disfavor human microchipping, views on the use of chipping technology in the human body for general or employment-related purposes may change relatively quickly. Moreover, employers are constantly searching for efficiencies in the use of technology. With these pressures in place, the employee microchipping issue will have a much more prominent role in the law of the workplace over time. The use of technology to battle COVID-19 through vaccination and the perceived minimizing of employee privacy rights in this era will only accelerate the speed with which employee microchipping becomes a more practical issue. It makes sense for legislatures to make strong statements right now that protect the privacy rights of employees and set appropriate limits on the use of microchip technology in the workplace. Mandatory employee microchipping is wrong. It is better to address the matter now instead of kicking the can down the road to consider the matter in the future.

The states that have enacted these statutes have seen strong bipartisan support (sometimes unanimous support) for the legislation.[111] Moreover, acting now allows states to experiment

---

22ee85b7 [https://perma.cc/E92V-P8BZ] ("There are currently no known employers in the U.S. that require employees to have any device implanted or otherwise incorporated into their body as a condition of employment. There are a few companies offering microchipping as a voluntary option to employees.").

[110] *See* Chris Marr, *Forced Worker Microchipping Faces Growing Preemptive Strike*, BLOOMBERG LAW (Mar. 19, 2020), https://news.bloomberglaw.com/daily-labor-report/forced-worker-microchipping-faces-growing-preemptive-strike [https://perma.cc/HMF4-8UCD].

[111] Andrew Keshner, *States are Cracking Down on Companies Microchipping Their Employees—How Common Is It?*, MARKETWATCH (Feb. 4, 2020, 9:33 AM),

with different approaches to their employee microchipping statutes and over time this will help to figure out the appropriate balances on the use of this technology and privacy rights. Uniformity is not needed at this point. States should act right now and follow the early adopters who have begun to regulate employee microchipping in the workplace. The uncertainties of the common law of employee privacy should spur the action. A statutory approach allows the legislature to craft nuanced "consent" rules should do a better job than the common law in protecting employee choice and privacy in this area. The remainder of this article focuses on how states can best regulate employee microchipping through legislation. Analysis of the statutes that have already been enacted in a handful of states help inform this analysis.

There are three main ways to approach statutory regulation. One is to have a short statement banning mandatory employee microchipping without much additional explanation. Missouri, which has a very short statute banning mandatory employee microchipping, is an example.[112] A second approach is to ban mandatory employee microchipping, allow for the use of the technology in the workplace by consent, and then specify very specific protective rules as to what constitutes consent so that employees who decide to be chipped and have their data accessed are really making a meaningful choice. Under this approach, it is made clear that employees will not be discriminated against for refusing to use a chip and there are no incentives or benefits for using a chip or not using a chip in the employment context. This approach is taken by Arkansas and Montana.[113] Another approach

---

https://www.marketwatch.com/story/states-are-cracking-down-on-companies-microchipping-their-employees-how-common-is-it-and-why-does-it-happen-2020-02-03 [https://perma.cc/9F4Z-F8G5] (noting the Indiana Legislature's vote on their employee microchipping bill was 96-0.)

[112] MO. ANN. STAT. § 285.035(1) (West 2020) ("No employer shall require an employee to have personal identification microchip technology implanted into an employee for any reason.").

[113] *See* ARK. CODE ANN. § 11-5-501 (West 2020) (providing detailed rules concerning consent, removal, and reasonable accommodation for employees who do not choose to use a microchip as well as what constitutes coercive behavior to try and get an employee to implant a microchip and unlawful discrimination); MONT. CODE ANN. § 39-2-1502 (West 2019) (providing detailed disclosure, consent, and removal rules for employment use of the microchip).

that states should consider is to simply ban both mandatory and voluntary employee microchipping. In other words, it is illegal for employers to access employee information through an employee's implanted microchip, even if the employer and employee would agree and the employee has been voluntarily chipped. No state has currently taken this approach as of yet but it should not be dismissed out of hand.[114]

States who want to be as protective as possible should seriously consider the possibility of banning even voluntary employee microchipping. This action would help to stop any use of employee microchipping and would be most protective of privacy rights. This action finds support in areas of employment law where the right in existence is so fundamental and important that the law precludes employees from voluntarily waiving their statutory rights. For example, the Fair Labor Standards Act's minimum wage and overtime rights are not generally permitted to be waived by employees because these core wage rights are so fundamental to the underlying purpose of the wage and hour statute.[115] The right to be free from an implanted chip could be analogously viewed as a similar core employee privacy right that is simply not capable of waiver or voluntary agreement. The downside to such action would be that it might take longer to determine the practical benefits, if any, of the use of implants in the workplace. Thus, a complete ban on voluntary employee microchipping may be unrealistic and unwise.

Assuming most states will not go so far as to completely ban all employee microchipping, states that desire to regulate in this area should, at the very least, completely ban forced employee microchipping and strictly regulate voluntary employee microchipping. A successful employee microchipping statute should contain several key provisions, which are as follows.

First, the statute should broadly define "employment" to cover both employees and independent contractors so the

---

[114] Fowler, *supra* note 79. ("One option to overcome this question of consent would be an outright ban of employment microchip use regardless of consent for employment-related purposes. No state has taken this approach.").

[115] *See* Brooklyn Sav. Bank v. O'Neil, 324 U.S. 697, 705-07 (1945) (finding employees cannot waive their FLSA statutory rights to wages because such waiver would nullify the purposes of the Act).

independent contractors are also protected from forced microchipping.[116] Second, the statute should clearly define what a "microchip" is for purposes of the statute.[117] Third, the statute should prohibit an employer from requiring an employee to have a microchip implanted in the employee's body (and prohibit an employer from requiring access to that data in the microchip) as a condition of employment.[118] Also, employers should be prohibited from asking prospective employees whether they would agree to a microchip as a condition of employment.[119] The statute should be broadly written to prohibit any sort of employer behavior that

---

[116] Montana's employee microchipping statute defines "employee" to include both traditional employees and independent contractors and the term "employer" to include entities that have both traditional employees and independent contractors as workers. *See* MONT. CODE ANN. § 39-2-1501(1)-(2) (West 2019) (defining employee as "a person who works for another for hire and includes independent contractors[,]" and defining employer as "a person or entity that has one or more employees or independent contractors.").

[117] *See, e.g.*, MO. ANN. STAT. § 285.035(2) (West 2020) ("'[P]ersonal identification microchip technology' means a subcutaneous or surgically implanted microchip technology device or product that contains or is designed to contain a unique identification number and personal information that can be noninvasively retrieved or transmitted with an external scanning device."); MONT. CODE ANN. § 39-2-1501(4) (West 2019) (defining microchip as "technology that: (a) is designed to be surgically implanted in the body of an individual; and (b) contains a unique identification number and personal information that can be noninvasively retrieved or transmitted with an external scanning device."); NEV. REV. STAT. ANN. § 200.870(4)(a) (West 2019) (defining the term "microchip" to mean "a device that is subcutaneously implanted in a person and that is passively or actively capable of transmitting personal information to another device using radio frequency technology.").

[118] *See, e.g.*, ARK. CODE ANN. § 11-5-501(c) (West 2020) ("An employer shall not require an employee to have a microchip implanted in the employee's body as a condition of employment."); IND. CODE ANN. § 22-5-8-2(a)(1) (West 2020) (declaring an employer cannot require any employee to submit to an implant or undergo a procedure to implant a device in the employee's body as a condition of employment); MO. ANN. STAT. § 285.035(1) (West 2020) ("No employer shall require an employee to have personal identification microchip technology implanted into an employee for any reason."); MONT. CODE ANN. § 39-2-1502(1) (WEST 2019) ("An employer is prohibited from requiring an employee to have a microchip implanted in the employee's body as a condition of employment."); NEV. REV. STAT. ANN. § 200.870(1)(b) (West 2020) (stating it is unlawful for an employer to require any person to "undergo the implantation of a microchip . . . as a condition of employment").

[119] *See, e.g.*, ARK. CODE ANN. § 11-5-501(b) (West 2020) (prohibiting employers from asking prospective employees during the application and interview process whether he or she "will consent to having a microchip implanted in his or her body"); IND. CODE ANN. § 22-5-8-2(a) (West 2020) (prohibiting employers from requiring a prospective employee to submit to an implant as a condition of employment).

seeks to coerce an employee into getting an implant or harasses the employee in any way because an employee does not have an implant or does not agree to an implant.[120] Of utmost importance, the statute should make it illegal for the employer to condition any benefit or detriment related to a term, condition, or privilege of employment on implantation of a chip in the employee.[121] Fourth, the statute should provide clear "informed consent" rules that allow for voluntarily microchipping of an employee if written consent is provided and then revocation of that consent at any point when the employee so desires.[122] Finally, the statute should provide an anti-retaliation provision that makes it illegal for an employer to discriminate against an employee who refuses an implant or makes a complaint to the employer or a relevant government agency about any alleged violation of the employee

---

[120] *See, e.g.*, ARK. CODE ANN. § 11-5-501(e)(1)(A)-(E) (West 2020) ("An employer shall not: (A) Coerce an employee into consenting to have a microchip implanted in his or her body; (B) Create a hostile work environment for an employee who does not consent to having a microchip implanted in his or her body; (C) Withhold advancement within the company from an employee who does not consent to having a microchip implanted in his or her body; (D) Withhold a salary or wage increase from an employee who does not consent to having a microchip implanted in his or her body; or (E) Dismiss an employee based on the decision of the employee not to consent to having a microchip implanted in his or her body.").

[121] For example, under Arkansas's employee microchipping statute, unlawful coercion of an employee to consent to an implant includes "[t]he conditioning of a private or public benefit, including without limitation employment, promotion, or another employment benefit, with the purpose of causing a reasonable individual of ordinary susceptibilities to acquiesce when the individual otherwise would not[.]"). *Id.* § 11-5-501(e)(2)(B). *See also* IND. CODE ANN. § 22-5-8-2(a) (West 2020) (declaring employer may not condition an employee's receipt of "additional compensation or other benefits" on an agreement to submit to the implantation of an employee microchip); NEV. REV. STAT. ANN. § 200.870 (West 2020) (permitting voluntary microchipping but only without "an incentive or other inducement").

[122] In Arkansas, employees must consent in writing to the implantation of the chip and may insist on removal at any time. *See* ARK. CODE ANN. § 11-5-501(f) (West 2019). The implant must then be removed within 30 days of the request. *Id.* § 11-5-501(f)(2)(B). The employer must pay for the cost of the implantation and removal and must pay for any medical costs associated with bodily injury arising from the implantation. *Id.* § 11-5-501(g)(1)-(2). Furthermore, the employer must disclose to the employee how data maintained on the microchip will be used by the employer. *Id.* § 11-5-501(h). Montana has enacted similar consent, disclosure, and removal provisions under its employee microchipping statute. *See* MONT. CODE ANN. § 39-2-1502 (West 2019).

microchipping statute.[123] In addition to the substantive provisions of the statute, the statute should contain a section that creates a private right of action (with appropriate remedies such as damages, costs, and attorneys' fees) for an employee to sue an employer for statutory violations.[124]

CONCLUSION

What does the future hold for employees and their privacy with respect to vaccination and microchipping? Will employees in the coming decades be routinely microchipped as part of workplace requirements such that information like mandatory employee vaccination records are immediately accessible to employers through the scan of the implanted human microchip? It may seem far-fetched right now, but the COVID-19 pandemic is demonstrating how quickly privacy rights can disappear when faced with the health and safety concern and employer liability concerns. Over time, the efficiency value of the implanted

---

[123] Anti-retaliation provisions are common in other federal and state employment law statutes and are necessary to protect the underlying substantive rights at issue. *See* 29 U.S.C. § 215(a)(3) (2020) (Fair Labor Standards Act anti-retaliation provision) ("It shall be unlawful for any person . . . to discharge or in any other manner discriminate against any employee because such employee has filed any complaint or instituted or caused to be instituted any proceeding under or related to this chapter, or has testified or is about to testify in any such proceeding, or has served or is about to serve on an industry committee[.]"); 29 U.S.C. § 2615(a)(1)-(2) (2020) (Family and Medical Leave Act anti-retaliation/interference provision) ("(1) It shall be unlawful for any employer to interfere with, restrain, or deny the exercise of or the attempt to exercise, any right provided under this subchapter. (2) It shall be unlawful for any employer to discharge or in any other manner discriminate against any individual for opposing any practice made unlawful by this subchapter."); 42 U.S.C. § 2000e-3(a) (2020) (Title VII anti-retaliation provision) ("It shall be an unlawful employment practice for an employer to discriminate against any of his employees . . . because he has opposed any practice made an unlawful employment practice by this subchapter, or because he has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this subchapter."). An employee microchipping statute needs to have similar anti-retaliation protections. *See, e.g.*, IND. CODE ANN. § 22-5-8-2(b) (West 2020) (declaring it unlawful for an employer to discriminate against an employee with respect to the employee's compensation and benefits or other terms and conditions of employment based on the employee's refusal to submit to an implanted microchip).

[124] The Indiana employee microchipping statute allows employees and prospective employees to bring a civil action against the employer for violating the statute and upon proof of a violation permits the recovery of actual damages, court costs, and reasonable attorneys' fees. *See IND. CODE ANN.* § 22-5-8-3(a)-(b) (West 2020).

employee microchip may place similar pressures on employee privacy rights. Privacy is only as important as we as a collective society desire it to be. And privacy is only protected when there is a sufficient will to make it a priority through both law and everyday behavior. The common law of employee privacy may fall short in addressing the employee microchipping issue. Without well-drafted employee microchipping legislation now, employees may end up paying later in terms of restrictions on their freedom to be free of an implanted chip and access to their personal data. It is not too early for balanced legislation that protects the privacy rights of employees but also allows for the voluntary use of microchipping technology in the workplace, given appropriate protections are in place to ensure that the use is truly voluntary. Accommodation law for individuals with disabilities and employees with religious beliefs will also be crucial in helping to shape the legal rights of employers and employees as related to employee microchipping.