Northwestern Journal of Technology and Intellectual Property

Volume 14 | Issue 2 Article 1

2016

The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables

Timothy L. Fort
Indiana University

Anjanette H. Raymond
Indiana University

Scott J. Shackelford
Indiana University

Volume 14, Number 2 (2016)
Northwestern Journal of Technology and Intellectual Property

The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables

By Timothy L. Fort,[*] Anjanette H. Raymond [**] & Scott J. Shackelford [***]

ABSTRACT

The wearable revolution is upon us. Bulky chest straps and large wristbands are going the way of flip cellphones and floppy disks. In the near future, for example, it may be commonplace for athletes to wear Biostamps or smart T-shirts with embedded sensors during practices, games, and even sleep. And while athletic competitors may have been one of the first movers in the area, health care, the military, and the industrial sector have all begun to use wearables to harness vast treasure troves of information destined to provide highly individualized feedback. The possibilities are almost endless when such personal information is combined with big data analytics in the name of improving large-scale efficiency.

Interestingly, employers were one of the first movers in the wearable revolution. Yet, other than basic tracking of people and goods, there is still a tremendous potential for expansion. What if wearables could be harnessed to assist employees in avoiding conflict of interests? What if wearables could assist employees in identifying ethical dilemmas and could then prompt them to consider alternative courses of action? What if the wearable evolution became an ethical revolution?

But the drawbacks of using wearables in such a manner must also be critically analyzed. This Article takes this step by exploring the use of wearables as personal information gathering devices that feed into larger data sets. It then considers some of the legal and policy implications of the use and aggregation of data in such a manner and ultimately makes suggestions for bottom-up baseline regulation. Ultimately, we argue for the desirability of leveraging this emerging technology, subject to privacy and security safeguards, to help drive an ethical revolution in business cultures.

---

[*] Eveleigh Professor of Business Law and Ethics, Indiana University.

[**] Assistant Professor of Business Law and Ethics, Indiana University; Adjunct Assistant Professor of Law, Maurer School of Law, Indiana University; Visiting Fellow in International Commercial Law, Centre for Commercial Law Studies, Queen Mary, University of London. The authors would like to thank the participants at the research colloquium, "Law and Ethics of Big Data," co-hosted by Indiana University and Virginia Tech, is sponsored by the Center for Business Intelligence and Analytics in the Pamplin College of Business, Virginia Tech, the Kelley School of Business at Indiana University and the Poynter Center for the Study of Ethics and American Institution at Indiana University for their valuable assistance, comments and feedback. All errors are those of the authors.

[***] Assistant Professor of Business Law and Ethics, Indiana University; Senior Fellow, Indiana University Center for Applied Cybersecurity Research; W. Glenn Campbell and Rita Ricardo-Campbell National Fellow, Stanford University Hoover Institution.

TABLE OF CONTENTS

INTRODUCTION 141

I. THE USE OF WEARABLES BY EMPLOYEES 144

A. Technology Helps Shine New Light on Old Knowledge 147
1. Simple Feedback Devices 148
2. Wearables and Behavior 149
3. Wearables and 'The Nudge' 150
4. The Techno-Connected Employee 151

B. Issues Abound 153
1. Gaming the System 153
2. Using the Technology as an Outward Looking Device 154

C. The Ethics of Nudges and Other Influences on Decision Making 155

II. POLYCENTRIC REGULATION OF WEARABLES IN THE WORKPLACE 157

A. Cybersecurity Best Practices For Wearable Firms 160
B. Employee and Customer Privacy and Confidentiality Implications for Wearables 164

III. LOOKING AHEAD TO WIDESPREAD USE 166

CONCLUSION 170

INTRODUCTION

¶1 It is an age-old philosophical question: are people ethical just because our human nature desires such nobility, or do we pay attention to ethics only from the fear of being caught? Memorably posed by Plato in *The Ring of Gyges*,[1] the provocateur Glaucon offers a scenario later picked up on by J.R.R. Tolkien.[2] The shepherd Gyges chances on finding a ring, which when he puts it on, makes him invisible. Smitten by such power, Gyges ends up seducing the impressed Queen of the land and together they take over the kingdom. Glaucon's challenge to his interlocutor, Socrates, is that once given the chance to get away with his actions, Gyges did as any person would: he did whatever he wanted because, in the final analysis, humans are ethical only for the fear of being caught.[3]

¶2 J.R.R. Tolkien in *The Lord of the Rings* elaborated upon this early example of wearable technology and the license it might give to our moral behavior. Any number of characters lusted after the ring and the ring-bearers found its intoxicating power to incrementally degrade their moral code. But what if wearable technology could have the opposite effect? What if, rather than empowering license, wearables could be used to support conscience? After all, moral philosophy and moral psychology agree that our conscience stands as an impediment to license. Our intuitions and feelings roil when we are faced with unethical temptations and hem in our desire to do whatever we please.[4] An entire field of moral psychology has demonstrated that we develop our conscience through our upbringing, with parents, family, friends, and teachers punishing bad actions, rewarding good actions, and generally instilling a neurological voice in our heads that reminds us of the importance and applicability of ethical values, especially during times of unethical temptations.[5] Could wearable technology provide a kind of updated, ongoing boost to the activation of such a conscience and/or help to develop it further?[6]

¶3 To be sure, there may be an odd alliance between Socrates, who believed human beings more nobly sought to be ethical as an independent good sewn into our human nature, and many contemporary neurobiologists and evolutionary biologists, who suggests that human beings are innately moral.[7] Others take a more moderate stance arguing that whether or not human beings are innately moral, it is clear that we are social creatures,[8]

---

[1] PLATO, THE REPUBLIC, http://classics.mit.edu/Plato/republic.mb.txt [http://perma.cc/UPY8-HTLT%5D].

[2] J.R.R. TOLKIEN, THE LORD OF THE RINGS Mariner Books; 50 Anv edition (August 14, 2012)

[3] Plato, *supra* note 1.

[4] *See, e.g.*, Oliver J. Sheldon and Ayelet Fishbach, *Anticipating and Resisting the Temptation to Behave Unethically*, PERSONALITY AND SOCIAL PSYCHOLOGY BULLETIN (May 22, 2015) (discussing why good people do bad things).

[5] *See generally* Daniel Patanella, PIAGET'S THEORY OF MORAL DEVELOPMENT, ENCYCLOPEDIA OF CHILD BEHAVIOR AND DEVELOPMENT, 1109–11 (Springer 2011) (discussing the development of morality).

[6] After all, while conventional wisdom suggests that our moral viewpoint is developed early on, other evidence points to the fact that because human beings always wish to fit in with a select group–even late in life–our moral conduct continues to evolve throughout life. *See* Robert A. Prentice, *Behavioral Ethics: Can it Help Lawyers (and Others) Be Their Best Selves*, 29 NOTRE DAME J.L. ETHICS & PUB. POL'Y 35, 46 (2015).

[7] *See* LARRY ARNHART, DARWINIAN NATURAL RIGHT: THE BIOLOGICAL ETHICS OF HUMAN NATURE (1998) (for discussions on this issue); *see also* FRANCIS COLLINS, THE LANGUAGE OF GOD (2007) (linking genetics with both the divine and ethics).

[8] *See* ROBERT C. SOLOMON, ETHICS AND EXCELLENCE (1993) (drawing on the Aristotlean tradition).

and thus ethics becomes central to how we navigate social relationships.[9] Yet even those who would take these positions recognize the importance of conscience and supports of it so that external regulation of our behaviors is deemed crucial for a moral life.[10]

¶4 Indeed, another strong strand of moral psychology argues that human beings' innate biases often hamper our capability of making objective ethical choices. Because we want to fit in, we recast information we receive to justify being part of our desired group.[11] We tend to be overconfident in our own abilities and therefore minimize risks.[12] We value our own self-interest over the self-interest of others.[13] Once we cross the line of taking a questionable action, we can find ourselves heading down a slippery slope of decisions as our ethical norms fade into the background.[14] When we step into a role, we jettison the values we would typically rely on and adopt another set of values that often justify problematic behavior.[15] As translated into the field of business ethics, more than a dozen such ethical biases have been documented with the central characteristic that these biases strongly challenge the functioning of our moral conscience.[16]

¶5 This problem, as Plato's *Ring of Gyges* demonstrates, is hardly new. It is a central issue of human nature and ethics. So what has been done? Accountability to loved ones and community is one social adaptation to the challenge of human license. Evolutionary biologists, for instance, have argued that religion can be seen as a cultural adaptation to the challenge of unchecked self-interest. A person may see no reason to give alms to the poor, for example, but a devout Muslim understands that by doing so, he demonstrates his commitment to a community that rewards such suspension of self-interest by rewarding the Muslim's long-term self-interested needs to belong to a community and the benefits (including economic) associated with such social membership.[17] Spiritual masters have counseled those wanting to improve their conduct to keep a running list of indiscretions so they can be more mindful of their errors and focus on their elimination.[18] Secularly, when the quality movement burst onto the business scene in the 1980s, one of the techniques advocated for eliminating mistakes was for managers to keep a running tab of "defects" on a pad of paper in their pocket so they could become more mindful of the need to correct their actions.[19]

---

[9] *See, e.g.*, WILLIAM C. FREDERICK, VALUES, NATURE & CULTURE IN THE AMERICAN CORPORATION (1995) (arguing that ethical behavior is the natural consequence of navigating three recurring value sectors).

[10] *See* TIMOTHY L. FORT, BUSINESS, INTEGRITY & PEACE (2007) (arguing that law is a one helpful component in assuring ethical conduct).

[11] *See* Prentice, *supra* note 6.

[12] *See* David Messick, Max Bazerman, & Lisa Stewart, *Avoiding Ethical Danger Zones*, Business Roundtable Institute for Corporate Ethics Bridge Paper at 13, http://www.corporate-ethics.org/pdf/danger_zones.pdfh [http://perma.cc/392E-LCBA]; *see also* Prentice, *supra* note 6.

[13] *See* Messick et. al, *supra* note 12; *see also* Prentice, *supra* note 6 at 62.

[14] *See* Messick et. al., *supra* note 12; *see also* Prentice, *supra* note 6 at 49.

[15] *See* Prentice, *supra* note 6 at 51.

[16] *See generally* Prentice, *supra* note 6.

[17] *See* DAVID SLOAN WILSON, DARWIN'S CATHEDRAL (2002) (pointing out the evolutionary advantages of religion as a community restricting individual self-interest).

[18] *See, e.g.,* IGNATIUS OF LOYOLA, SPIRITUAL EXERCISES AND SELECTED WORKS (George E. Gans, ed.) (2002)

[19] *See e.g.*, W. EDWARDS DEMING, OUT OF THE CRISIS (2000) (calling for the scrupulous detailing of quality defects in order to become more aware of them and to fix them).

¶6 In this context, there is a long history of recognizing the need for reminders that correct personal conduct so that we can overcome our natural biases and better access and/or further develop our own moral consciences. The question then becomes whether a powerful item we wear might have an opposite effect of Gyges and Frodo's ring; that instead, wearables might be able to *improve* ethical conduct. If that is true, how would this happen and, at least equally importantly, what risks might be associated with such a solution?

¶7 Broadly speaking the idea of a digital angel on one's shoulder raises three ethical issues that have gone largely unexplored in the literature.[20] First, does this notion of utilizing wearable technology have any practical possibilities and, if so, whether it is simply ethically problematic in the sense of undermining traditional goods such as autonomy and freedom from manipulation? The ethical issue pertaining to this question concerns whether such an analysis is simply a hypothetical thought experiment relegating to philosophical ruminations or whether we are examining something that might have real world possibilities that are ineliminably threatening. Because we argue that this technology is quite real, the practicalities of wearable technology make this an issue pertinent to public policy and to the ethical issues used to evaluate public policy, an analysis that is not readily concluded. Second, what are the accountability pressure points associated with wearables? This issue includes how a wearable, in fact, does provide accountability – that is, how does it effectively act as an angel, and not a demon, on your shoulder – as well as who has access to the measures of accountability? Should wearables provide accountability by reporting only to the wearer of the wearable, or should others have access to the information generated by the wearables? This leads immediately to a third, multifaceted issue: security and privacy. If any third party is to have access to any information provided by a wearable technology, how is the wearer's information protected?

¶8 With this in mind, Section II explores the use of wearable technology by employees with an emphasis on the realities of what that technology currently looks like and how it might evolve in the foreseeable future. Section III examines the cognitive issues related to ethics and, as a result, pertaining to wearable technology. Apart from the important normative dimensions of ethics, moral psychology informs how we frame moral issues and the point of wearable technology – at least from an ethical and public policy perspective – will include how such technology impacts our psychological assessments of the situations in which we find ourselves. Section IV then proposes a polycentric model of governance that is suited to address the issues of wearables, situated within a broader discussion of the Internet of things, with the identified ethical considerations in mind. Section V projects to the future of wearables and the application of the considerations and policies we have identified. The final Section then returns to a consideration of the ethics of wearables in light of our analysis and remaining issues that will be important to consider in the coming years.

[20] This is not to argue that these are the only issues or that the ones identified are the definitive issues. We do wish to argue that they are crucial issues worth our attention.

I. THE USE OF WEARABLES BY EMPLOYEES

¶9 In 2013, *Bloomberg Business* highlighted a trend that few could imagine would spark a revolution: employees donning wearables to improve productivity.[21] Tesco, a UK grocery store chain, required its distribution center employees to wear the then-new technology known as Motorola arm-mounted terminals.[22] These devices allowed Tesco to measure their employees' productivity, providing data points such as loading and unloading speeds and other similar metrics.[23] Other than the workers' lunch breaks, any activity, including trips to the bathroom or water fountain, lowered the workers' productivity score.[24] While Tesco has not discussed the success or merits of such initiatives, the devices reportedly increased productivity and efficiency,[25] resulting in an expanded use of the devices.[26] Any real or perceived impact on employee morale was left unmentioned.

¶10 Employee monitoring has garnered debate in the United States for years.[27] For example, monitoring using established technologies such as email and other digital communication is nearly resolved,[28] while social communications—such as when an

---

[21] Claire Suddath, *Tesco Monitors Employees With Motorola Armbands*, BLOOMBERG BUSINESSWEEK (Feb. 13, 2013), http://www.bloomberg.com/bw/articles/2013-02-13/tesco-monitors-employees-with-motorola-arm-bands [http://perma.cc/G925-8BR9].

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] *Id*. (citing Zoe Wood, *Tesco Calls Time On Megastores After Profit Warning Shock*, THE GUARDIAN, Jan. 14, 2012, http://www.theguardian.com/business/2012/jan/15/tesco-growth-megastores).

[26] *Id.* (noting that Tesco launched a similar program in Bangladesh in November 2012).

[27] While one may think the law would protect employees, current trends seem to suggest that the law will not evolve or fundamentally alter already existing, but limited, protections. For example, while the Electronic Communications Privacy Act of 1986 ("ECPA") (18 U.S.C. § 2510-22) imposes some restrictions on access to electronic communications, it imposes few practical restrictions on employers desiring to monitor employee e-mail or voice mail where the employer provides the system that stores and receives the transmissions. ECPA only prohibits access to an electronic communication facility if it is done "without authorization" or in a manner that exceeds the authorization given. 18 U.S.C. § 2511. As can be seen above, there is little to suggest employers will not provide the wearable devices and provide incentives for gathering the desired information.

Case law has also evolved in a manner that would likely prevent protecting employees from wearable intrusions. For example, the Fourth Circuit, in *United States v. Simons*, 206 F.3d 392 (4th Cir., February 28, 2000), held that an employee lacks any reasonable expectation of privacy with regard to his use of the Internet when the employer has official policies regarding such use. In making this determination, the Court relied upon the Supreme Court case of *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (plurality opinion); 480 U.S. at 730-31 (Scalia, J., concurring in the judgment), to find that the employee's reasonable expectation of privacy should be analyzed in the context of the employment relationship. Exploring a two-prong approach, the Fourth Circuit noted "regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use" because the FBIS Internet "clearly stated that [it] would 'audit, inspect, and/or monitor' employees' use of the Internet . . . [which] placed employees on notice that they could not reasonably expect that their Internet activity would be private." 206 F.3d at 398. One can thus argue that it is the company's privacy policy that defines the scope of any expectation of privacy when considered in light of the employee.

[28] *See generally*, Susan Park, *Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy*, 51 AM. BUS. L.J. 779, 800 (2014) (discussing the rights of employees relating to communications); Edward J. Imwinkelried, *The Applicability of Privileges to Employees' Personal E-mails: The Errors Caused by the Confusion Between Privilege Confidentiality and Other Notions of Privacy*, 2014 Mich. St. L. Rev. 1, 7 (2014) (discussing an employee's protection of personal work email);

employer demands social media and other Internet passwords[29]—has remained a matter for debate. And, of course, many potential employers gather personal information through less invasive means,[30] attempting to 'discover' hidden pasts prior to hiring an individual. Yet despite the growing use of employee tracking technology, such as the tracking of location information through GPS-enabled vehicles,[31] wearables as a participant in the employee's decision-making process is still in its infancy.[32] Such trends provide context for the ethical considerations discussed below as the law generally does not protect employees (or job applicants) from information that is willingly shared[33] and/or information that is gathered after consent is provided.[34] But such consent may only be in name only. Did Gollum, or Gyges, consent to wearing their rings, or did forces beyond their control push them to?

¶11 In increasing numbers, employees are using wearables to improve basic data entry and other repetitive, yet time consuming tasks such as price checking and appointment reminders.[35] For example, executive vice president of market development and corporate communications at FedEx Mike Glen notes: "Wearable technology is already having a significant impact on FedEx team members who are involved with package sorting and pickup and delivery."[36] Similarly, in 2012, United Parcel Service, Inc. ("UPS") adopted a new "wearable" scanning system for its package-handling employees.[37] The device has a hands-free imager worn on a finger and a small terminal worn on the employee's wrist or hip.[38] The technology allows UPS employees to quickly image barcodes,[39] thereby improving time on site and repetitive data entry.

¶12 Each of these wearables allows businesses to monitor location, time spent, and improve overall efficiency. Yet such technologies also have the potential to run afoul of civil rights protections given the volume of private data accumulated,[40] including, at times,

---

[29] *See* Park, *supra* note 28 (exploring the current law and suggesting a more balanced approach to regulation).

[30] *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 289-90 (2011) ("Unfortunately, the American legal system has failed to: (1) keep up with today's powerful monitoring technology, and (2) provide the necessary privacy protection to employees.").

[31] *See On Your Tracks: GPS Tracking in the Workplace*, 2011 NAT. WORKERS RIGHTS INST. 1, https://epic.org/privacy/workplace/gps-traking.pdf [https://perma.cc/9VVJ-TGJC].

[32] *See e.g.,* Ron Miller, *New Firm Combines Wearables And Data To Improve Decision Making*, TECH CRUNCH (Feb. 24, 2015), http://techcrunch.com/2015/02/24/new-firm-combines-wearables-and-data-to-improve-decision-making/. Anisha Mehta, Comment: *"Bring Your Own Glass:" The Privacy Implications of Google Glass in the Workplace*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 607, 608 (2014).

[33] *See id.*

[34] Several states, including California and Texas, have laws preventing equipment tracking without express consent. However, in most places, it is legal for firms to outfit their employees with wearables, as long as they are clear about what is being tracked and why. *See* Aviva Rutkin, *Wearable Tech Lets Boss Track Your Work, Rest and Play*, NEW SCIENTIST, Oct. 18, 2014, at 22.

[35] *See* H. James Wilson, *Wearables in the Workplace*, HARV. BUS. REV., Sept. 2013, at 23.

[36] *Q&A with Mike Glen, Fedex Services*, ACCESS (Nov. 2013), http://access.van.fedex.com/qa-mike-glenn-fedex-services/ [perma.cc/7CXE-PZJ6].

[37] Jacques Couret, *UPS Using 'Wearable' Scanning System*, ATLANTA BUS. CHRONICLE (Aug. 2, 2012), http://www.bizjournals.com/atlanta/news/2012/08/02/ups-using-wearable-scanning-system.html [perma.cc/8B27-MEN9].

[38] *Id*.

[39] *Id*.

[40] *See* Wilson, *supra* note 35.

off-hours information. For example, in 2015 a lawsuit was brought against Intermex, a money transfer service, for requiring employees to download a job management application called Xora onto company-issued iPhones.[41] Employees became concerned, however, when they discovered the Xora app was tracking all of the employees' whereabouts, even when they were not working.[42] One employee deleted the Xora app and was fired for refusing to allow such monitoring, initiating the lawsuit.[43]

¶13 Despite various media outlets focusing on some of the negative implications of employee monitoring, there are plenty of under-reported examples of these technologies being used to improve employment environments and the employee experience alike. For example, in 2009 Bank of America monitored the interactions of co-workers at their call centers.[44] During a six-week period, employees wore sensors made by Sociometric Solutions to record "where employees went and who they talked to, how the tone of their voice and the movements of their body changed throughout the day."[45] The monitoring reportedly indicated that social employees are more productive, resulting in a change of working environment at Bank of America to encourage more informal socializing.

¶14 Wearable technologies can also provide timely, current, and highly accurate information to assist field service technicians in assessing repair and service needs. Similarly, optical wearables can be used for photo and data collection.[46] The potential for work-related wearable use by employees is seen by many businesses as a major growth area. For example, a February 2015 Salesforce Research study entitled "Putting Wearables to Work" surveyed "500 wearable tech adopters who said they were currently using, piloting, or planning to implement wearable technology in the enterprise in some form."[47] Seventy-nine percent of adopters agree that wearables are or will be strategic to their company's future success.[48] Seventy-six percent report improvements in business performance since implementing wearable devices in the enterprise [49] And early adopters such as construction, manufacturing, energy, oilfield services, and medical industries have now developed a short, yet supportable, improvement in efficiency with fewer job-related mistakes.[50]

¶15 The use of technology to monitor, and influence the decision making, of an employee is a complex, multi-faceted topic for debate. This section focuses on technology as an assistive agent in the decision making process of employees. First, it briefly examines the

---

[41] *See* Williams Pelegrin, *This Company Fired an Employee When She Deleted an App That Stalked Her Every Move*, DIGITAL TRENDS (May 12, 2015), http://www.digitaltrends.com/mobile/employee-fired-delete-tracking-app-news/ [perma.cc/TD2P-Z7M3].

[42] *Id*.

[43] *Id*. *See also* Adriana Gardella, *Employer Sued for GPS-Tracking Salesperson 24/7*, FORBES (June 5, 2015), http://www.forbes.com/sites/adrianagardella/2015/06/05/employer-sued-for-gps-tracking-salesperson-247/ - 2715e4857a0b262a49ae36d4 [perma.cc/58UP-QGSG].

[44] *See* Rutkin, *supra* note 34.

[45] *Id*.

[46] *See* Andre Bourque, *Wearable Tech Will Soon Be Work Attire in These 4 Industries*, ENTREPRENEUR (May 13, 2015), http://www.entrepreneur.com/article/246040 [perma.cc/B2UV-V7J3].

[47] SALESFORCE RESEARCH, PUTTING WEARABLES TO WORK: SPECIAL REPORT 2 (2015), https://secure2.sfdcstatic.com/assets/pdf/misc/StateOfWearablesReport.pdf [perma.cc/9852-TSWS].

[48] *See id*. at 3.

[49] *Id*.

[50] *See* Erin Griffith, *Search: How Do I Punch This Rivet Hole?*, FORTUNE (Oct. 4, 2014), http://fortune.com/2014/10/09/wearable-technology-blue-collar-jobs/ [perma.cc/L2N5-B753].

tried and tested methods of influencing individual choice. Next, it progresses into considering some of the omnipresent wearable technologies that together gather a large amount of personal information and in the process create an individualized employment experience. It then considers the use of wearable technology—and behavioral intervention architecture—as an influence on decision making of the employee. The section concludes by examining some of the legal and ethical issues that will need to be addressed as this technology becomes more widely utilized.

A. Technology Helps Shine New Light on Old Knowledge

¶16 Whether we realize it or not, many of us are familiar with the use of personal information gathering, environmental monitoring, and the technology-based influencing of our behavior. Consider Bally's on the Vegas Strip. That Vegas Casinos (and many others) have long used personal information combined with environmental information, including the personal information of those gathered by you, to ply their craft, earning the moniker "engineers of addiction."[51]

¶17 Most modern gaming is based in part on the psychological principle of a Skinner Box,[52] but modern casinos today rely upon so much more. For example, most casinos rely upon information provided both by the individual when they fill in forms use loyalty cards. This information is valuable, to put it mildly. Caesar's Entertainment creditors, for example, appraised Caesar's "vast store of customer data as the company's most valuable asset, worth about $1 billion."[53] To take another example, it has been claimed that:

> Harrah's can create a portrait of the person's risk profile, including how much money a player typically loses before they stop playing and what kinds of gifts to give them to keep them on the gaming floor. Sometimes, that can be a penthouse suite; other times, it can be as little as giving a player $15 in cash.[54]

Not only does the casino know how to keep the average gambler on the floor, the casino knows how to keep the particular *individual* on the floor along with the least expensive manner in which to accomplish this goal. Moreover, casinos know how to design interiors to create an internal maze causing individuals to focus on the machines instead of the

---

[51] Andrew Thompson, *Engineers of Addiction Slot Machines Perfected Addictive Gaming. Now, Tech Wants Their Tricks*, THE VERGE (May 6, 2015), http://www.theverge.com/2015/5/6/8544303/casino-slot-machine-gambling-addiction-psychology-mobile-games.

[52] In the now infamous experiment, B.F. Skinner put pigeons in a box which released a pellet of food when they pressed a lever. Skinner was interested, however, in how reinforcement fit into the process. Thus, he altered the rate of return, (i.e. he released pellets in a random reinforcement schedule). However, when Skinner altered the box such that pellets came out on random presses — a system dubbed— the pigeons pressed the lever more often. B.F. Skinner, *'Superstition" in the Pigeon*, 38 J. EXPERIMENTAL PSYCHOLOGY 168 (1948). The process, now dubbed variable ratio enforcement, is often likened to a slot machine. COMM. ON THE SOC. AND ECON. IMPACT OF PATHOLOGICAL GAMBLING ET AL., PATHOLOGICAL GAMBLING: A CRITICAL REVIEW 39-40 (1999), http://www.nap.edu/openbook.php?isbn=0309065712 [perma.cc/H24Z-9CXB].

[53] *See* Thompson, *supra* note 51. *This American Life* charted the lurid and unsettling extreme of how such datacan be used in a story about a Harrah's casino in Indiana that enticed a woman to keep playing with unlimited hotel suites, diamond jewelry, and free trips to the Kentucky Derby. In the end, she lost her inheritance worth more than $125,000. *466: Blackjack*, THIS AM. LIFE (June 8, 2012), http://www.thisamericanlife.org/radio-archives/episode/466/blackjack [http://perma.cc/8D2R-YNK6].

[54] *See* Thompson, *supra* note 51.

space,[55] and to control perspective to increase focus on the gaming that is occurring.[56] Once the casinos understand the environmental and personal dynamics, they use that information to create a personalized system of tolerance, reward thresholds and trust in the payout system all designed to "hook and hold" players' long term interest.[57]

¶18 Such issues are brought into even sharper relief when the information-gathering is no longer inferred from context but is instead generated in real time from imbedded wearable technologies.[58] Imagine when the lessons learned in well-established reward-based environments, such as casinos, are incorporated into the workplace. The following sub-sections explore the technology that is moving us from inferred preferences into real-time information-gathering, impacting both employer and employee decision-making and much more in the process.

1. Simple Feedback Devices

¶19 Similar to the behavioral therapy technique of snapping a rubber band,[59] simple feedback devices—especially those that draw your attention to the device in order to alert you to danger or to break current thought processes[60]—are considered by many to be potentially life-altering, enhancing the health and well-being of users. For example, the Lumo Lift[61] tracks a wearer's posture and activity and gently vibrates when the wearer has a bad posture.[62] Haptic technology,[63] especially tactile feedback,[64] has been employed in life saving devices. For example, thermo-sensitive fire fighter gloves provide temperature and retreat warning to firefighters through the use of a vibration response,[65] and heart patients wear a haptic tactile device that alert the individual if their heart rate is dangerously high.[66] Similarly, the 2015 Hyundai Cockpit Concept envisions applications for connected devices inside and outside of vehicles, including the use of driver heart rate monitoring,

---

[55] *See* NATASHA DOW SCHULL, ADDICTION BY DESIGN: MACHINE GAMBLING IN LAW VEGAS 41 (2012) (discussing the use of space).

[56] *See id*. at 44 (discussing tricks used to focus attention).

[57] *See id*. at 200 (discussing the tricks used to hold attention over).

[58] One wonders when casinos will begin to see the advantages in players using a wearable device, such as a Fitbit, to remind people to get up and move, and to reward them for such behavior (all while gathering even more personal information).

[59] *See* Max Mastellone, *Aversion Therapy: A New Use for the Old Rubber Band*, 5 J. BEHAV. THERAPY & EXPERIMENTAL PSYCHIATRY 311 (1974).

[60] Known as haptic feedback or vibrating alerts, both provide information through the use of our senses. In essence, **haptics** is about conveying information to the user or operator through their sense of touch, whilst vibration alerting is about capturing a user's attention after an event or in an emergency.

[61] *See* Lumo BodyTech, Inc., http://www.lumobodytech.com/ (last visited Nov. 27, 2015) [http://perma.cc/MDJ7-AH3W].

[62] *See id.*

[63] Haptic technology, haptics, or kinesthetic communication, is tactile feedback technology that recreates the sense of touch by applying forces, vibrations, or motions to the user. For an explanation, see Gabriel Robles-De-La-Torre, *Haptic Technology, An Animated Explanation*, INT'L SOC'Y FOR HAPTICS, *available at* http://isfh.org/ (last visited Mar. 18, 2015).

[64] In general, tactile feedback is thought to interact with the fingertips and the shape and position sensors under the fingertips.

[65] *See* Christof Breckenfelder et al., *A Cognitive Glove Sensor Network for Fire Fighters*, in 8 AMBIENT INTELLIGENCE & SMART ENVIRONMENTS, VOLUME 8: WORKSHOP PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON INTELLIGENT ENVIRONMENTS, IOS Press, (2010) http://ebooks.iospress.nl/publication/27982 [http://perma.cc/C5L9-FTFX].

[66] *See* Haptic Health Feedback Monitoring, U.S. Patent No. 20080319279A1.

driver alertness monitor with rest recommendation messages, and blind spot and safe following distance warnings.[67] The Cockpit uses an augmented reality heads-up display system and wearables to alert drivers to changing road conditions and dangerous situations, all in a transparent windshield projection and/or vibrating wearable wristband.[68]

¶20 Each of these technologies may be thought of as inputs in an individual's decision-making process—such as by helping to sense environmental conditions or alert individuals to hazardous conditions—allowing an individual to change his/her course of action. Yet at their most basic, even the most advanced feedback devices do nothing more than alerting an individual to a situation. Thus, while these devices inform the decision-making process, individuals remain in control of their responses–until third parties, including employers, gain access to that data, as discussed below.

2. Wearables and Behavior

¶21 Wearables that monitor an individual's behavior may be able to alert individuals to behavioral patterns of which they had no conscious awareness.[69] Since much of an individual's "gut" reaction is based on past experience, individuals must to be reminded that viewing our past is often tinted with many biases.[70] In this way, intuition can lead us astray.[71]

¶22 Even something as simple as monitoring one's gaze can lead to a important insights into an individual and their decision-making process.[72] For example, in March 2015, researchers from the University of California, Merced, Lund University in Sweden and University College London, published a study entitled: *Biasing Moral Decisions By Exploiting the Dynamics of Eye Gaze*. The study challenges the long-held belief that the decisions people make are rooted in a pre-existing moral framework.[73] Professor Michael

---

[67] *See Hyundai Showcasing Augmented Reality, Wearables and ADAS Tech at 2015 CES*, GREEN CAR CONG. (Jan. 5, 2015), http://www.greencarcongress.com/2015/01/20150105-hyundai.html [http://perma.cc/YV56-Z87J].

[68] *See id*.

[69] *See* Jack B. Soll et al., *Outsmart Your Own Biases*, 93 HARV. BUS. REV. 64 (2015) (providing discussion of various unconscious behavioral biases).

[70] *See* Emre Soyer & Robin M. Hogarth, *Fooled by Experience*, HARV. BUS. REV., May 2015, at 73.

[71] *See* John Beshears et al., *Test Yourself: Are You Being Tricked by Intuition?*, HARV. BUS. REV. (Apr. 2, 2015), https://hbr.org/2015/04/test-yourself-are-you-being-tricked-by-intuition [https://perma.cc/C8Y5-9DZT].

[72] Previous research has shown that judgments and decisions between simple concrete alternatives, in particular faces and foodstuffs, can be influenced by manipulating saliency, attention, or exposure in various ways, *see e.g.,* Shinsuke Shimojo, Claudiu Simion, Eiko Shimojo, & Christian Scheier, *Gaze Bias Both Reflects and Influences Preference*, 6 NATURE NEUROSCIENCE 1317(2003) (arguing that gaze is actively involved in preference formation); K. Carrie Armel, Aurelie Beaumel, & Antonio Rangel, *Biasing Simple Choices by Manipulating Relative Visual Attention,* 3 JUDGMENT AND DECISION MAKING 396 (2008) (arguing that visual attention is controlled by manipulating the amount of time subjects fixate on two alternatives); William E. Baker, *When Can Affective Conditioning and Mere Exposure Directly Influence Brand Choice?* 28 J. ADVERTISING 31 (1999) (examining if affective conditioning and exposure influence brand choice); Milica Milosavljevic, Vidhya Navalpakkam, Christof Koch, & Antonio Rangel, *Relative Visual Saliency Differences Induces Sizable Bias In Consumer Choice*, 22 J. CONSUMER PSYCHOL. 67 (2012) (showing that show that at rapid decision speeds, visual saliency influences choices more than preferences do); Gregory Koop & Joseph Johnson, *The Response Dynamics Of Preferential Choice*, 67 COGNITIVE PSYCHOL. 151 (2013) (developing a formal computational model of joint information sampling and preference accumulation).

[73] Philip Pärnamets et al., *Biasing Moral Decisions by Exploiting the Dynamics of Eye Gaze*, 112 PROC.

Spivey notes: "People often assume that their moral opinions are stable preferences that already exist in their hearts and mind . . . But we hypothesized that many of your moral decisions may arise on the fly, as a result of how you look at and interact with your environment."[74] Researchers found that participants' responses to moral questions could be manipulated by tracking the movement of their eyes.[75] Participants unwittingly chose a randomly selected response more frequently when the timing of their decision was manipulated based on eye gaze.[76] In fact, researchers found that when participants were prompted to respond to a moral question, participants often chose the response they happened to be looking at when receiving the prompt.[77] As noted by Professor Philip Pärnamets, "The process of arriving at a moral decision is not only reflected in people's eye gaze, but can also be determined by it."[78]

¶23 The take home point for the immediate purposes is that wearables, especially devices worn on the face, can gather information such as gaze, focus direction, shifts in focus and attention grabbing environmental stimuli. In this way, wearables may be able to assist individuals in noticing their own internal—and often hidden—biases, aiding decision-making through nudges if technical, legal, and ethical issues may be overcome.

3. Wearables and 'The Nudge'

¶24 Behavioral insight intervention, described in the seminal work *Nudge* by Richard Thaler and Cass Sunstein,[79] has taken the world by storm. Building from the work of Nobel Laureate Daniel Kahneman,[80] who is widely regarded as one of the most important researchers explaining what influences the human decision making process,[81] "'Nudging' involves structuring the choices that people make so as to lead them towards particular outcomes."[82] By way of brief explanation, there are three levels of nudges, the first two of which have been widely used, in various environments for a number of years. 'First Degree Nudges,' such as simple warnings or reminders, are designed to respect the decision-making autonomy of the individual and serve no other purpose than to enhance the individual's reflective decision-making process.[83] For example, the devices described as

OF THE NAT'L ACAD. OF SCI. 4170 (2015), http://www.pnas.org/content/early/2015/03/10/1415250112.full.pdf+html [perma.cc/HW7E-2C75].

[74] James Leonard, *Study: Moral Decisions Can Be Manipulated by Tracking Eye Gaze, University of California, Merced*, UNIV. NEWS (Mar. 16, 2015), http://www.ucmerced.edu/news/2015/study-moral-decisions-can-be-manipulated-tracking-eye-gaze [http://perma.cc/6QE3-TZZ2].

[75] *See* Pärnamets, *supra* note 73, at 4171.

[76] *See id*. at 4172–73.

[77] *See id*.

[78] Ellie Zolfagharifard, *How To Force Someone To Make The Right Choice: Study Says Our GAZE May Be All It Takes To Change Moral Decisions*, DAILY MAIL (Mar. 18, 2015), http://www.dailymail.co.uk/sciencetech/article-2999433/How-force-make-right-choice-Study-says-GAZE-takes-change-moral-decisions.html [http://perma.cc/B7RL-32GD].

[79] *See generally* RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009).

[80] *See generally* DANIEL KAHNEMAN, THINKING, FAST AND SLOW, MACMILLAN PUBS (2011).

[81] *See* Roger Lowenstein, *Book Review: Thinking, Fast and Slow by Daniel Kahneman*, BLOOMBERG (Oct. 27, 2011), http://www.bloomberg.com/bw/magazine/book-review-thinking-fast-and-slow-by-daniel-kahneman-10272011.html [http://perma.cc/M6NF-G3YF].

[82] Robert Baldwin, *Nudge: Three Degrees of Concern,* LSE POL'Y BRIEFING PAPER NO. 7, Feb. 1 2015, at 2, http://ssrn.com/abstract=2573334.

[83] *See id*.

'feedback devices' above would fall within the category of First Degree Nudges; alerting, but leaving the reaction to the information within the decision making of the individual. A 'Second Degree Nudge' is designed to use 'choice architecture'[84] to build on behavioral limitations in an effort to bias a decision in the desired direction.[85] Again, many of us are familiar with the use of this concept; for example, the use of a default rule with an opt-out option is a choice architecture decision that has been shown to have a powerful influence on individual behavior.[86] Increasing in order of potential impact on the decision making process, a 'Third Degree Nudge' involves behavioral manipulation that uses "a message with an emotional power that blocks the consideration of all options."[87] Commentators argue that this type of behavior manipulation directly impacts an individual's ability to act in accordance with her or his own preferences.[88] But what does this mean for creating the little angel on an employee's shoulder?

4. The Techno-Connected Employee

¶25 For employees, much of this research could be the launching point for focusing the use of wearable technology in a manner that directly impacts their professional decision-making process. Imagine the following hypothetical. Employee John arrives at work and changes into his work clothes; a Fitbit,[89] Google Glass-like device,[90] and an undershirt called Polo Tech shirt.[91] As a condition of his employment, John has a personal online profile that contains his basic information, such as gender, age, resting heart rate, and delivery preferences. Each of these data points are fed into the business metrics, such as improving warehouse efficiency as measured by a reduction in time per order. John's personal data is combined with fellow employee data to identify patterns that result in less time spent per order. The business has been able to use data to improve its efficiency and has hopefully accomplished this without stressing John's health. But, what if the business wishes to improve employee performance in a less tangible manner? What if the business wishes to improve an employee's ethical responses in situations of identifiable stakeholder conflict? This is the businesses' desire to put an angel on each employees shoulder, and it is closer to reality than one might think.

¶26 In this scenario, John is a stockbroker caught in the stakeholder conflict of making the best recommendation for his client versus the reality of maximizing return for both his firm and himself. John often faces such an ethical dilemma, so the various wearables

---

[84] *See id*.

[85] *See id*.

[86] For example, automatically enrolling individuals on pension schemes has increased saving rates for those employed by large firms in the United Kingdom from 61 to 83 percent. *See Who We Are,* THE BEHAVIOURAL TEAM, http://www.behaviouralinsights.co.uk/about-us [perma.cc/FAX3-444X].

[87] *See* Baldwin, *supra* note 82, at 2.

[88] *See id*.

[89] *See* FITBIT, http://www.fitbit.com/ (last visited May 24, 2015) [perma.cc/L45T-6FD9].

[90] Reports of Google Glass's death have been greatly exaggerated. It is not dead. Instead a revamped version, aimed toward business, will be launched in 2015. *See* James Cook, *A New Version of Google Glass is Coming in 2015*, BUSINESS INSIDER (Dec. 1, 2014), http://www.businessinsider.com/a-new-version-of-google-glass-is-coming-in-2015-2014-12#ixzz3QcIwajt4 [http://perma.cc/F3HY-836R].

[91] *See* The PoloTech Shirt, RALPH LAUREN, http://www.ralphlauren.com/shop/index.jsp?categoryId=46285296 (last visited May 24, 2015) [http://perma.cc/3GUW-Q7EW].

providing feedback to John know his pattern of information that signals that John is facing a difficult decision. Perhaps his heartrate elevates, he begins to sweat, maybe he speaks at a faster pace, or does a combination of all of these things and more. The more times John faces such a dilemma the more information is gathered. John is the integral part of a data feedback loop, providing information to build a more personalized response from the immersive technology. As data becomes more aligned with the identification of situations in which John faces an ethical dilemma, the immersive technology, such as Google Glass or the HoloLens,[92] places a transparent series of prompts on the screen and vibrates at a higher rate on John's wrist. Google Glass prompts or nudges[93] John to identify various stakeholders, to consider his employer's Code of Conduct, and to use a decision matrix to identify alternative behaviors and responses. As John continues to provide data suggesting that he has yet to return to a pre-stressed state, the Fitbit vibrates at a faster rate.

¶27 Similar to many cognitive behavioral theories,[94] John is receiving feedback for not resolving the ethical dilemma in a manner that he is comfortable with as evidenced by his failure to return to a pre-conflict steady state. John can continue to receive prompts, information, and nudges that match with his employer's expectations on resolving his ethical conflict.

¶28 To take a real-world example, Morgan Stanley's Code of Conduct lists four core values: (1) Putting Clients First, (2) Leading with Exceptional Ideas, (3) Doing the Right Thing, and (4) Giving Back.[95] Imagine if a transparent screen in front of John's face could display these four Core Values. What if the screen prompted John to consider questions that directed him toward a deeper consideration of each of the values? Prompts could include:

- Is my action legal?
- Is my action consistent with Morgan Stanley's business principles and this Code?
- Could my action be perceived as inappropriate or unethical?
- Could my action damage my or Morgan Stanley's reputation, or embarrass me or Morgan Stanley?
- How would my action appear as a headline in tomorrow's newspaper?[96]

---

[92] *See e.g.,* Christina Warren, *Microsoft HoloLens Won't Be the Next Google Glass, And That's a Good Thing*, MASHABLE (Jan. 21 2015), http://mashable.com/2015/01/21/microsoft-hololens-and-google-glass/ [http://perma.cc/2QZQ-4LGJ].

[93] "The idea of nudging is based on research that shows it is possible to steer people towards better decisions by presenting choices in different ways." *Nudge Nudge, Think Think, The Use Of Behavioural Economics In Public Policy Shows Promise*, ECONOMIST (Mar. 24, 2012), http://www.economist.com/node/21551032 [http://perma.cc/7BJ6-CHL8].

[94] *See e.g*., Judith S Beck, COGNITIVE BEHAVIOR THERAPY: BASICS AND BEYOND 19–20 (2011); Rachman, *The Evolution Of Cognitive Behaviour Therapy*, *in* David Clark, Christopher Fairburn, & Mark Gelder, SCIENCE AND PRACTICE OF COGNITIVE BEHAVIOUR THERAPY 1, 1 (1996) (discussing the history on cognitive therapy).

[95] *See* MORGAN STANLEY, MORGAN STANLEY CODE OF CONDUCT: CULTURE, VALUES, AND CONDUCT 3 (2015), https://www.morganstanley.com/about-us-governance/pdf/ms-code-of-conduct.pdf [perma.cc/3X6V-KD7B].

[96] *See* MORGAN STANLEY, LIVING OUR BUSINESS PRINCIPLES, MORGAN STANLEY CODE OF CONDUCT 7 (2011), https://www.morganstanley.com/about/company/governance/pdf/FinalCode2011.pdf

John would not need to actually articulate a response, in fact, he would not need to make a decision reflecting the values, he could ignore or reject the conclusion arrived at using the prompts, but Morgan Stanley managers could rest assured that John had at least viewed the Core Values and was prompted through a series of questions asking him to reflect on his choices in light of the Core Values.[97]

¶29 Each of these prompts is a nudge, i.e., an alert designed to provide information to the individual to influence decision making. The scenario becomes a little less comfortable when we add in a less transparent nudge. As described above, the business could monitor John's eye gaze and then nudge John into selecting the business' desired outcome by displaying a key choice at the optimum time. In this example, has the company merely nudged John into a moral choice, or has the company actually used its influence to alter John's decision-making process? Although this is a nuanced distinction, issues concerning the use of such technology in this manner must be addressed from both practical and ethical points of view.

B. Issues Abound

¶30 It would seem that there is a clear answer to our first ethical question of whether the use of wearable technology to influence behavior is a hypothetical thought experiment or whether it is a practical, realistic phenomena. It is not only possible; it has already happened.[98] Thus, the methodological question turns from speculative philosophy – akin to Plato's Ring of Gyes or Tolkien's fiction – to concrete policy issues, both within the corporation and societally as well.

¶31 That is even truer with respect to the issue of accountability. Wearable technology does provide a concrete mechanism for individuals to monitor their own behavior. Just as technology can impact physical health by reporting the number of steps one has taken during the day or calories ingested, it can also provide feedback to the wearer on how their body changes when they are engaged in certain activities, including those that violate commonly accepted ethical behaviors.

1. Gaming the System

¶32 In the case of wearables, employees are now willingly encouraged and are often rewarded for providing such information. For example, according to the *Harvard Business Review*: "About 90% of companies now offer wellness programs, some of which encourage employees to use Fitbit and other devices that measure the quantity and intensity of their workouts and to employ simple visual and motivational tools to track their progress and help sustain their engagement."[99] However, commentators have expressed concerns over the reliability of the data from the wearable technology.[100] For example, some

---

[perma.cc/T2Q8-SD7J].

[97] *Id*. ("When in doubt, stop and reflect.").

[98] See *supra* Section II.

[99] *See* Wilson, *supra* note 35, at 24.

[100] *See generally* Lucas Mearian, *Data from Wearable Devices Could Soon Land You in Jail*, COMPUTERWORLD (Dec. 8, 2014), http://www.computerworld.com/article/2855567/data-from-wearable-devices-could-soon-land-you-in-jail.html [http://perma.cc/V2AN-LV4Q] (discussing limitation of the current devices); Margaret Littman, *Data From Wearable Devices is Being Eyed As Evidence in the Courtroom*, ABA J. (Apr. 1, 2015)

wearable devices log activity just by a wave of the hand, while others may not.[101] Additionally, people often fail to charge, sync, or wear their devices,[102] thereby thwarting efforts to gather information at key moments in time.

¶33 Interestingly, research into individuals'—and groups'—ability to game systems of performance monitoring has drawn considerable attention in recent months. For example, in 2014 employees at Mindshare wore one of three devices: an accelerometer wristband, a portable brainwave monitor, or a posture coach.[103] The study highlights two important points for further research and consideration. First, according to Chris Brauer of the University of London: "People recognise that effectively they're on the clock, that they're being tracked, and as a result they raise their game."[104] However, the study also highlights potential ethical issues. First, the devices recorded enough data to make detailed profiles of individual employees: their lifestyle, exercise, and sleep habits.[105] And secondly, as noted by Professor Ethan Bernstein points out, such devices could also trigger the "transparency paradox," which occurs when some workers obsess over hitting their sensor-related targets.[106] In these instances, employees fail to focus on doing the best job overall, which makes them more likely to cheat and less likely to take potentially useful risks.[107]

2. Using the Technology as an Outward Looking Device

¶34 While the majority of this article has focused on technology that measures the individual's responses to the environment, some of the newest technology is being designed to measure the emotions of others and to provide feedback to the user based on information received about individuals in their environment. For example, Microsoft was recently awarded a patent for "a wearable emotion detection feedback system."[108] According to the various documents within the patent filing, sensors, including depth cameras and a microphone mounted on the nose bridge, pick up visual and audio information from an identified individual in the environment.[109] Information about the individual, including things like "subtle variations in speech rhythm and amplitude, choice of words, type and speed of gestures, eye focus and body posture"[110] is gathered and sent back to Microsoft for analysis.[111] Microsoft then uses that information to make an

---

http://www.abajournal.com/mobile/mag_article/data_from_wearable_devices_is_being_eyed_as_evidence_in_the_courtroom [https://perma.cc/C8CJ-DK2P?type=source] (discussing the misuse and gaming of the device analytic measures).

[101] *See* Littman, *supra* note 100.

[102] *See id*.

[103] *See* Rutkin, *supra* note 34.

[104] *See id*.

[105] *See id*.

[106] *See* Ethan Bernstein, *The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Contro,* 57 ADMIN. SCI. Q. 181, 181(2012).

[107] *See* Rutkin, *supra* note 34.

[108] The patent was filed in October 2012 and awarded in May 2015, according to a public filing by the U.S. patent office. *See* Amir Mizroch, *Microsoft Awarded Patent for Emotion Detecting Eyeglasses*, WALL ST. J. (Apr. 29, 2015, 9:33 AM), http://blogs.wsj.com/digits/2015/04/29/microsoft-awarded-patent-for-emotion-detecting-eyeglasses/ [perma.cc/BS8G-JKLQ].

[109] U.S. Patent No. D565,584.

[110] Mizroch, *supra* note 108.

[111] *See id*.

"emotional determination" which is then relayed back to the wearer through the glasses.[112] As can be imagined, Microsoft hopes to gather enough big data and personal information to enable it to decode subtle hints based on context and to pass on this context specific information to the viewer/user. And while this is still in the patent stage, it is hoped that devices would be able to communicate in a connected information network, thereby building the amount of contextual information that can be analyzed.[113]

C. The Ethics of Nudges and Other Influences on Decision Making

¶35 The fact that wearable technology is becoming prevalent will continue to raise ethical issues as to whether this is a good phenomena or a bad one. However one comes out on that question, the reality is that it is here. The fact that wearable technology can make an individual more personally aware of their own conduct does not seem to raise a particularly strong ethical concern either. An individual can simply choose whether or not to use the technology.[114] If they do, there may well be significant benefits associated with its use insofar as the technology can counter psychological biases that otherwise might blind an individual from the consequences of their actions.

¶36 However, what happens when employees are faced with haptic wearable devices, nudge based choice architectures, and business policy promoted through opaque influences? Professors Richard H. Thaler and Cass R. Sunstein emphasize that a nudge should be "easy and cheap to avoid" but the nudge has power in so far as it impacts on the decision-maker of limited cognitive capacity, information, and self-control.[115] However, Professor Robert Baldwin argues that "those very limitations arguably mean that the target is unlikely to be well-placed to exercise the opt-out in cases of Second and Third Degree nudges. With Third Degree nudges, the position is especially poor because the target will be 'blocked' to a greater extent from resorting to the opt-out."[116]

¶37 Imagine if the individual is not only 'blocked' from opting out through choice architecture but is further inhibited by business reward based incentives, group influence, and job longevity.

¶38 Professor Sunstein raises several potential issues: (1) wearables pose issues of paternalism, (2) that they threaten autonomy, (3) that they risk coercion, (4) that they pose risks for dignity, and (5) manipulation becomes a concern.[117] With nearly every category, ethical risks are magnified. For example, in external hands and without notice, consent, or oversight, there is a real risk of the holder of information provided by wearables to be tools for manipulation and, with such manipulation, coercion and humiliation (the opposite of

---

[112] *See id*. The field, known as emotional analytics, is becoming popular amongst consumer behaviorists. Elizabeth Dwoskin & Evelyn M. Rusli*, The Technology that Unmasks Your Hidden Emotions*, WALL ST. J. online (Jan. 28, 2015). For one such company, see *Emotional Dynamics*, EMOTIVE ANALYTICS, http://www.emotiveanalytics.com/emotional-dynamics.php [perma.cc/WFX6-DMPT] (last visited Jan. 18, 2016).

[113] *See* Mizroch, *supra* note 108.

[114] Relying on basic, generally accepted notions of consent being a guarantor of ethical decision making.

[115] *See* RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009).

[116] *See* Baldwin, *supra* note 82, at 2.

[117] *See* Cass R. Sunstein, *Nudging and Choice Architecture: Ethical Considerations*, YALE J. REG. 32 YALE J. REG. 413, 428 (2015).

; Cass R. Sunstein, *Do People Like Nudges?*, (July 29, 2015), http://ssrn.com/abstract=2604084.

dignity).[118] Those same concerns give rise to potential loss of autonomy, but that depends on other dynamics. As Professor Sunstein argues, we live in a world of nudges, but their presence does not mean that we are forced into a particular direction.[119] We may be nudged by a default mechanism in an opt-out contract agreement, but we retain choice.[120]

¶39 Nudges, of course, are not new. Just as Frodo, Bilbo, and Gollum faced perennial challenges associated with a magic ring, so to have humans dealt with the issues of nudges from the time we were born. Families and other mediating institutions nudge by encouraging some set of actions over other sets of actions and especially insofar as they provide feedback mechanisms such that family members experience the consequences of their actions.[121] Because human beings are social creatures,[122] we live in communities. In those institutions, nudges – if not outright elbow jabs – are part of the life we navigate. The same holds true outside of our families as well, including in the workplace.

¶40 Muslims may be nudged to give alms to the poor in order to be considered a good member of their religious community, but the person retains the choice as to whether to give alms or not.[123] The same holds true, for better or for worse, with one's membership on a team, in an inner city gang, in a rural militia, in a nursing home, or in a business.[124]

¶41 A nudge that notifies us that our heart rate is consistent with lying does not force anything; but it does nudge us to consider our action.[125] Being fully blocked from an action by an electronic gadget does raise more issues than those associated with a simple reminder. Combining being blocked from opting out through a choice architecture with additional losses in terms of group influence and job longevity may well create a coercive combination of pressures, with nudges becoming morally problematic. In a worst-case scenario, insular, humiliating communities may result, what have sometimes been called quarantining institutions.[126]

¶42 At the same time, Professor Sunstein is surely right that nudges – from the angle on our shoulder to the close friend and trusted mentor – can encourage us to become better persons than we might be otherwise. Who, among us, has not needed the nudge – or the slap in the face – to come to our senses? Thus, it seems to be an overreaction to claim that the use of wearables in nudging ethical behavior is inherently problematic. It may well not be and it is, in some respects, simply another inevitable feature of life. At the same time, wearables introduce a new form of ever-present pressures of living in a community and do so in a way that raises anew all the issues Professor Sunstein identifies. In certain situations and in certain combinations, nudges can become problematic. In other times and places, they can be morally uplifting.

¶43 Beyond these ethical considerations, of course, lay the issue of privacy and who is allowed to review the information gathered, and what related security issues (for example, the ability to hack wearable technology) arise. It thus requires policy questions to address

---

[118] Sunstein, *Nudging and Choice Architecture, supra* note 117, at 31.
[119] *Id*. at 33.
[120] *Id.*
[121] TIMOTHY L. FORT, ETHICS AND GOVERNANCE 51 (2001).
[122] See, ARNHART, *supra* note 7 (providing a modern, scientifically-based argument of Aristotle's position on the natural socialness of human beings).
[123] WILSON, supra note 17.
[124] FORT, *supra* note 121, at 14.
[125] *See* Ramsey *supra* note 66; *see also* GREEN CAR CONGress, *supra* note 67.
[126] FORT, *supra* note 121, at 17.

consent, accountability, privacy, and security concerns. These questions are not easy exactly because wearables are ambivalent. Their use for good or bad do have situational dependency. Our sense, however, is that many superb scholars will address the parade of horribles that can result from wearable technology. Without diminishing those real problems we will analyze now the good of this emerging technology. The immediacy of the need for their development means that they are currently being developed directly within public policy and law. With that in mind, we turn to how these issues are – or can be – addressed.

II. POLYCENTRIC REGULATION OF WEARABLES IN THE WORKPLACE

¶44 This Part explores the growth of wearable technologies in the private-sector context as part of the broader movement toward the so-called "Internet of things."[127] The rise of "smart products" from Internet-enabled refrigerators to self-driving cars holds the promise to revolutionize business and society. From 2013 to 2020, the number of Internet-enabled devices is expected to increase from 11 to 50 billion.[128] This explosion in use raises difficult issues for policymakers seeking to craft rules of the road for the companies offering these new products and services. Considering the full gambit of novel issues presented by the Internet of things is outside the scope of this Article.[129] Yet the Internet of things does provide an invaluable lens through which to view the issue of regulating wearables to ensure their secure and ethical use. Thus far, though, this topic has not received significant attention in the literature.[130] This raises two pertinent and interrelated questions for the immediate purposes: At what level should regulation take place in such a fast-moving marketplace? And what forms should those regulations take to enhance cybersecurity and safeguard employee privacy?

¶45 Although this Article has largely taken an optimistic approach to the study of wearable technologies in the employee context, such technologies could of course be prone to abuse by employers even as they hold the potential to empower employees. For example, an employer could provide various biometric sensors to employees so that they have accurate information about how much they are remaining physically active throughout the day, as well as how their time breaks down during working hours. So long as this information remains under the exclusive control of the employee, who has been informed and consents to the sensors, such an approach could provide useful insights that

---

[127] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 94–95 (2014).

[128] *Id.*

[129] For more on this topic, *see generally* Peppet, *supra* note 127.

[130] *Cf.* Mehta, *supra* note 32, at 607; David Halpern, Patrick Reville, & Donald Grunewald, *Management and Legal Issues Regarding Electronic Surveillance of Employees in the Workplace*, J. BUS. ETHICS 176 (2008); Adam D. Moore, *Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy*, 10 BUS. ETHICS Q. 697, 701-02 (2000) (discussing how circumstances, such as job scarcity and high unemployment, create an environment wherein employees agree to employer monitoring more out of fear of adverse consequences than actual consent); Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 829 (2012) (discussing the ethics of professional self-regulation); Alexander Rengel, *Privacy-Invading Technologies and Recommendations for Designing a Better Future for Privacy Rights*, 8 INTERCULTURAL HUM. RTS. L. REV. 177, 214–15 (2013) (discussing among other things the ethics and privacy implications of RFID implants); Philip Cochran et al., *Radio Frequency Identification and the Ethics of Privacy*, 36 ORG. DYNAMICS 217, 219 (2007) ("Such new technologies ultimately reshape the way in which individuals work and live as well as the ways that organizations are designed and function.").

could help enhance both worker health and productivity; an individualized Hyundai Cockpit redesigned for an array of situations. However, it would be all too easy for employers to gain access to that data and use it without consent in promotion and retention decisions. Already, as reported on *Planet Money*, people provide various functions as "Mechanical Turks" for companies like Amazon and are in some cases under close scrutiny during the performance of their duties.[131] A true parade of horribles is possible.[132] However, such considerations of the demonic power of having a 'devil on your shoulder' are a subject for future research. We limit ourselves here to considering the cybersecurity and employee privacy of using wearables in the private sector, and how such a system can and should be regulated to guarantee civil rights in the United States and abroad.

¶46 The dual arenas of cybersecurity and employee privacy are interlinked and central to the future of the Internet of Things, including wearables. Cyber attacks have already entered the Internet of things with reports of not only webcams and televisions being hacked, but even refrigerators and cars.[133] Professor Scott Peppet has noted, for example, that, "Data-security researchers have found vulnerabilities in Fitbit fitness trackers, Internet-connected insulin pumps, automobile sensors, and other products."[134] As the web becomes ever more mobile and distributed, it is essential that policymakers take note of the regulatory complexity arising from such a network and for firms to begin to internalize cybersecurity best practices to protect consumers and employees alike. So far, though, lawmakers have not been up to the challenge:

> [B]oth current FTC enforcement practices and state data-breach notification laws are unprepared to address Internet of Things security problems. In particular, were Fitbit, Nike+ FuelBand, Nest Thermostat, or any other Internet of Things manufacturers to have users' sensitive sensor data stolen, no existing state data-breach notification law would currently require public disclosure or remedy of such a breach.[135]

¶47 We thus seek to help jumpstart a conversation about the role of regulation in this space, particularly to help safeguard civil liberties and promote cybersecurity. Yet such "regulation" need not take the form of black-letter law. For example, Professor Lawrence Lessig identified four modalities of cyber regulation: architecture, law, the market, and norms that "may be used individually or collectively" by policymakers.[136] Especially in an emerging field such as wearables, significant space should be left for innovation to help usher in the emergence of best practices. Otherwise, top-down regulation risks "crowding out" smaller-scale innovative efforts.[137] Such sentiments are part and parcel of the literature on polycentric governance.

---

[131] *See The People Inside Your Machine*, PLANET MONEY (Jan. 30, 2015), http://www.npr.org/blogs/money/2015/01/30/382657657/episode-600-the-people-inside-your-machine [http://perma.cc/KB3T-SKXF].

[132] For example, see footnotes 42–44 and accompanying text, which discusses the Intermex example.

[133] *Id.*

[134] Peppet, *supra* note 127, at 94–95.

[135] *Id*.

[136] *See* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662–63 (1998).

[137] *See, e.g.*, Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010) (citing Andrew F. Reeson & John G. Tisdell, *Institutions, Motivations and Public Goods: An Experimental Test of Motivational Crowding*, 68 J. ECON. BEHAVIOR &

¶48 According to Professor Michael McGinnis, "[t]he basic idea [of polycentric governance] is that any group . . . facing some collective action problem should be able to address that problem in whatever way they best see fit."[138] This could include using existing governance structures or crafting new systems to meet the needs of users.[139] In other words, "[a] system of governance is *fully polycentric* if it facilitates creative problem-solving at all levels . . . ."[140] This multi-level, multi-purpose, multi-functional, and multi-sectoral model,[141] championed by scholars including Nobel Laureate Elinor Ostrom and Professor Vincent Ostrom, challenges orthodoxy by demonstrating the benefits of self-organization, networking regulations "at multiple scales,"[142] and examining the extent to which national and private control can in some cases coexist with communal management. A polycentric approach recognizes that diverse organizations working at multiple levels can create different types of policies that can increase levels of cooperation and compliance, enhancing "flexibility across issues and adaptability over time."[143]

¶49 Professor Ostrom created an informative framework of eight design principles for the management of common pool resources that helps to guide discussion. These include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain";[144] (2) "proportional equivalence between benefits and costs";[145] (3) "collective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[146] (4) "monitoring . . . by the appropriators or by their agents";[147] (5) "graduated sanctions" for rule violators;[148] (6) "conflict-resolution mechanisms [that] are readily available, low

---

ORG. 273 (2008) (finding "externally imposed regulation that would theoretically lead to higher joint returns 'crowded out' voluntary behavior to cooperate")).

[138] Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care*, Workshop on Self-Governance, Polycentricity, and Development, at 1 (Conference on Self-Governance, Polycentricity, and Development, Renmin University, in Beijing, China) (2011).

[139] *Id.* at 1–2.

[140] *Id.* at 3.

[141] Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39(1) POL'Y STUD. J. 163, 171–72 (Feb. 2011), http://php.indiana.edu/~mcginnis/iad_guide.pdf [http://perma.cc/D2QF-J3YF] (defining polycentricity as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

[142] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Political Theory and Policy Analysis, Working Paper Series No. 08–6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf?sequence=1 [http://perma.cc/3SBM-VQA8].

[143] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change* 9 PERSP. ON POL. 7, 9 (2011); *cf.* Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 157 (2008) (discussing the legitimacy of polycentric regimes, and arguing that "[a]ll regulatory regimes are polycentric to varying degrees").

[144] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 32 (1998).

[145] Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 (citing ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 90 (1990)).

[146] BUCK, *supra* note 144, at 32.

[147] *Id*.

[148] *Id*.

cost, and legitimate";[149] (7) "minimal recognition of rights to organize";[150] and (8) "governance activities [being] . . . organized in multiple layers of nested enterprises."[151]

¶50 Not all of Professor Ostrom's design principles are applicable in cyberspace given that they were designed primarily for managing small-scale resources, such as forests and lakes. However, some do have salience. For example, the IAD Framework notes the importance of user participation in crafting rules to govern the environment. This could take the form of market leaders establishing industry norms that could then be shared through information sharing organizations such as industry councils.[152] Over time, if sufficient uptake is forthcoming, such best practices could be codified through state or federal regulation permitting graduated sanctions for rule breakers. Such an approach is being undertaken to a greater or lesser extent in the cybersecurity space as may be seen by the efforts of norm entrepreneurs such as Microsoft and Google,[153] along with the spreading of information sharing efforts.[154] Tech firms active in the wearable space may follow this example, providing a space for group monitoring that could help lay a foundation for good governance that would push back against security breaches or unreasonable privacy encroachments. However, a first step to such efforts requires the identification of cybersecurity best practices, which is no easy feat given the rapidly evolving nature of the technology and threat environment.

A. Cybersecurity Best Practices For Wearable Firms

¶51 Intimately related to the privacy implications of wearables discussed next is the need for enhanced cybersecurity. Yet enhancing cybersecurity is nearly as difficult as protecting privacy. This starts with the problem of defining "cybersecurity" and "cyber attacks," which like "privacy" eschew easy classification. For purposes of this Article, though, we use terminology provided by the National Academy of Sciences and the U.S. Cyber Emergency Response Team ("CERT"). According to the U.S. National Academy of Sciences, cyber attacks refer to "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[155] "Cybersecurity" then may be considered "[t]he

---

[149] *Id*.

[150] Ostrom, *supra* note 145.

[151] *Id*.

[152] *See, e.g.*, Microsoft: Cyber Trust Blog, Putting Information Sharing into Context, http://blogs.microsoft.com/cybertrust/2015/01/27/putting-information-sharing-into-context/ [http://perma.cc/Q9DU-4NYC] (last visited Mar. 18, 2015).

[153] *See Microsoft's Security Development Lifecycle*, MICROSOFT, http://www.microsoft.com/security/sdl/default.aspx (last visited Mar. 18, 2015) [perma.cc/4WJF-7GR6]; Gregg Keizer, *Google Raises Bug Bounties to $20,000*, COMPUTERWORLD (May 7, 2012), http://www.computerworld.com/article/2503788/security0/google-raises-bug-bounties-to--20-000.html [http://perma.cc/Y4LJ-43PQ]; *Microsoft BlueHat Prize*, MICROSOFT, http://www.microsoft.com/security/bluehatprize/ (last visited Mar. 18, 2015) [http://perma.cc/X7QQ-CGGP].

[154] *See, e.g.*, VIRUSTOTAL, https://www.virustotal.com/ (last visited MAR. 18, 2015) [perma.cc/CWZ3-KVB3].

[155] COMM. ON OFFENSIVE INFO. WAREFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin eds., 2009). *Cf.* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 822-32 (2012) (defining cyber attacks as consisting "of any action taken to undermine the function of a computer network for a political or national

activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[156] Yet, as headlines regularly attest, enhancing cybersecurity and managing cyber attacks is far easier said than done with high-profile breaches regularly impacting companies, countries, and the international community.[157] The focus here, though, is on the private sector, notably investigating cybersecurity lapses across platforms and the need for more proactive measures that build in cybersecurity best practices from the inception of new products and services including wearables.

¶52 Before delving into some of the cybersecurity issues facing wearables in particular, it is worth having some context. Many firms are experiencing cyber attacks of increasing sophistication with greater regularity. From 2000 to 2008, for example, the Computer Security Institute ("CSI") and CSI/FBI surveys found that the proportion of organizations reporting an attack ranged from 43 to 70 percent.[158] Thus, recent breachesof cyber attacks–Target and Sony aside–have been a problem for the private sector since at least the late 1990s.[159] However, detection capabilities do not seem to be improving apace with the evolving and multifaceted cyber threat. For example, Mandiant, a cybersecurity firm, has reported that its survey results have revealed a *drop* in the number of firms that have been able to detect cyber attacks on their own networks.[160] One recent example was a company with an active breach for over six years.[161] Moreover, firms of all sizes and across various sectors are at risk, if not always equally. According to the National Computer Security Survey ("NCSS"), for example, companies in the agriculture, computer system design, and chemical and drug manufacturing sectors experienced the most incidents.[162] In the aggregate, cyber attacks have been estimated by McKinsey & Co., a consultancy, to cost some $3 trillion in lost productivity by 2020,[163] though estimates vary greatly due to the difficulties of cost of cyber attacks (such as the value of lost trade secrets) and will ultimately depend on myriad factors including the growth of the "Internet of things."[164]

---

security purpose").

[156] *Explore Terms: A Glossary of Common Cybersecurity Terminology*, NICCS, http://niccs.us-cert.gov/glossary#cybersecurity (last visited July 14, 2014) [http://perma.cc/J4NP-DCZV].

[157] *See generally* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE (2014).

[158] *See* Robert Richardson, *CSI Computer Crime & Security Survey*, CSI at 13 (2008), *available at* http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf [http://perma.cc/9PEC-K6VE] [hereinafter *2008 CSI Survey*].

[159] For more discussion about the evolution of cyber attacks, see Chapters 1, 3, and 4 of SHACKELFORD, *supra* note 157.

[160] Press Release, Beyond the Breach, Mandiant (Apr. 10, 2014), http://investors.fireeye.com/releasedetail.cfm?ReleaseID=839454 [http://perma.cc/X6AN-V9EE] (reporting a drop from 37 to 33 percent from 2012 to 2013).

[161] *Id.*

[162] *See* Ramona R. Rantala, *Cybercrime Against Businesses, 2005,* U.S. DEP'T JUSTICE, BUREAU JUSTICE STAT. SPECIAL REP., at 1, 11 (Sept. 2008), http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf [http://perma.cc/SK2P-MMYL].

[163] *See* Brian Taylor, *Cyberattacks Fallout Could Cost the Global Economy $3 Trillion by 2020*, TECH. REPUBLIC (Feb. 20, 2014), http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/ [http://perma.cc/2V4R-ZTMH].

[164] *See* 2013 COST OF CYBER CRIME STUDY: UNITED STATES, PONEMON INST. 1 (2013), http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf [http://perma.cc/2CTP-SFSN]; Ben Fox Rubin, *Google's Nest, Others Hatch New Internet of Things*

¶53 The cyber threat is often broken down into the categories of cyber war, cybercrime, cyber espionage, and cyber terrorism to aid policymakers and managers in getting a better handle on this problem, but this exercise is fraught with difficulties due to problems of overlap and attribution among other issues.[165] Instead, it may be more beneficial to consider the best ways to manage cyber attacks of all stripes from the bottom up, consistent with the literature on polycentric governance discussed above, which requires instilling an array of organizational, technological, and managerial cybersecurity best practices to proactively manage the cyber threat. At the most basic level, it is vital for firms to avoid the attractiveness of a reactive approach to enhancing cybersecurity due to the difficulties of cyber cost-benefit analysis (that is, infinite investment does not breed infinite security).[166] Wearable tech firms, as with all organizations, need to be mindful of the importance of securing their supply chains and supplier networks from purposeful attacks and latent security gaps.[167] The Target breach, after all, which exposed around 40 million credit card numbers, was the result of lax security from a HVAC supplier that, for an unknown reason, had access to a myriad of Target systems well beyond the HVAC networks.[168] At the next level up, wearable firms need to be mindful of protocol vulnerabilities such as those in the Domain Name System ("DNS"), which can cause customers to unwittingly go to the wrong website and enter their credentials. An imperfect fix in the form of a DNS Security Extension is available, but many companies have not paid to have it installed.[169] Other cyber risk mitigation techniques such as the growing use of cyber risk insurance should also be utilized to protect wearable firms and employees. This is especially vital to better secure sites on mobile devices, which are roughly where PCs were in the 1990s in terms of cybersecurity.[170] According to one 2011 report, "The pace of change in this technology is quite dramatic. Only a few years ago, malware for smartphones and cellular devices was unheard of."[171] Now it is common to turn iPhones into microphones, making boardrooms as porous for eavesdroppers as the office water cooler.[172]

¶54 At the next level up, it is vital for wearable firms and their clients to invest in the creation of comprehensive cybersecurity strategies that are regularly updated and

Group, CNET (July 15, 2014), http://www.cnet.com/news/googles-nest-others-hatch-new-internet-of-things-group/ [http://perma.cc/7MVV-RTXS].

[165] SHACKELFORD, *supra* note 157, at 6.

[166] *See, e.g.*, Scott Dynes, *Information Security Investment Case Study: The Manufacturing Sector*, CTR. DIGITAL STRATEGIES at 9 (2006), http://www.tuck.dartmouth.edu/cds-uploads/research-projects/pdf/InfoSecManufacturing.pdf [http://perma.cc/NFN8-84LX].

[167] *See, e.g.*, SCOTT CHARNEY & ERIC T. WERNER, MICROSOFT, CYBER SUPPLY CHAIN RISK MANAGEMENT: TOWARD A GLOBAL VISION OF TRANSPARENCY AND TRUST 5 (2011); SHACKELFORD, *supra* note 157, at 193.

[168] *See* Ensign, *infra* note 176; *In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes*, KREBS ON SEC. (Sept. 18, 2014), http://krebsonsecurity.com/tag/target-data-breach/ [http://perma.cc/9Z7G-JB97].

[169] SHACKELFORD, *supra* note 157, at 334.

[170] *See* David Goldman, *Your Smartphone will (Eventually) be Hacked*, CNN (Sept. 17, 2012), http://money.cnn.com/2012/09/17/technology/smartphone-cyberattack/.

[171] *From the Eye of the Storm: 2011 Information Security Predictions*, INFO. SEC. (Jan. 6, 2011), http://www.infosecurity-us.com/view/14954/from-the-eye-of-the-storm-2011-information-security-predictions/ [http://perma.cc/XED7-KCTM].

[172] *See* Christopher Butkin, *Spies Can Listen to Your iPhone Microphone Even if It is Switched OFF, Experts Reveal*, MIRROR (June 10, 2014), http://www.mirror.co.uk/news/technology-science/technology/spies-can-listen-your-iphone-3670347 [http://perma.cc/6FT5-36NW].

communicated to their employees as part of an overarching (and ideally audited) cyber hygiene campaign.[173] Such education is vital both to inform employees of their legal obligations under various state and federal laws, but also of their civil rights. It also raises another set of ethical issues: to what extent do individuals (and companies) have responsibilities to contribute to a safe, sustainable cyber environment? Knowledge about the potential impact wearable users can have on the larger environment can influence sustainable practices just as has been the case with environmental issues.[174] Ultimately (and depending on their unique cyber threat matrix), wearable firms should also take various proactive measures from regular penetration testing to the use of cybersecurity analytics and insider threat mitigation techniques to further safeguard various stakeholders.[175] A useful first step is provided by the 2014 National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework"),[176] which was born in February 2013 when President Obama issued an executive order that, among other things, tasked NIST with establishing a framework of private-sector best practices that companies could adopt to better secure critical infrastructure.[177] The Framework harmonizes consensus standards and industry best practices to provide, its proponents argue, a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk.[178] Although the NIST Framework has only been out for a relatively short time, already private-sector clients are receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[179]

---

[173] For more on this topic, see Chapter 5 of SHACKELFORD, *supra* note 157.

[174] For more on this topic, see Scott J. Shackelford & Timothy L. Fort, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, UNIV. ILL. L. REV. (forthcoming 2016).

[174] *Id*.

[175] *Id*.

[176] *See* Rachel Louise Ensign, *Cybersecurity Due Diligence Key in M&A Deals*, WALL ST. J. (Apr. 24, 2014), http://blogs.wsj.com/riskandcompliance/2014/04/24/cybersecurity-due-diligence-key-in-ma-deals/ [http://perma.cc/CS33-678M]; *How to Conduct Due Diligence for a Merger or Purchase of a Business or LLC*, NY COUNSEL, http://www.nyccounsel.com/starting-a-business-startups/checklist-how-to-conduct-due-diligence-for-a-merger-or-purchase-of-a-business/ (last visited Aug. 12, 2014) [http://perma.cc/7SB3-PQDM]; Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks that Target and Degrade the Grid*, 40 WM. MITCHELL L. REV. 647, 729 (2014) (discussing due diligence in reference to the NIST Framework).

[177] *See* WHITE HOUSE PRESS SEC'Y, EXECUTIVE ORDER ON IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 [http://perma.cc/5RKF-X9M2]; Mark Clayton, *Why Obama's Executive Order on Cybersecurity Doesn't Satisfy Most Experts*, CHRISTIAN SCI. MONITOR (Feb. 13, 2013), http://www.csmonitor.com/USA/Politics/2013/0213/Why-Obama-s-executive-order-on-cybersecurity-doesn-t-satisfy-most-experts [http://perma.cc/85FZ-K534].

[178] *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. at 11,741. *See also* Scott J. Shackelford et al. *Toward a Global Standard of Cybersecurity Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, __ TEX. J. INT'L L. __ (forthcoming 2015) (exploring the extent to which the NIST Framework will help shape a standard of cybersecurity care).

[179] *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework [perma.cc/CP97-E5NK]. *See also* Trope & Humes, *supra* note 176, at 83 (discussing an array of reasons including pending DHS regulations as to why the NIST Framework may not be truly voluntary).

B. Employee and Customer Privacy and Confidentiality Implications for Wearables

¶55 A related critical issue to security is employee privacy since, after all, there is no privacy without security. Privacy is a multi-faceted concept meaning different things to different stakeholders in different parts of the world. It encompasses (among much else) freedom of thought, of bodily integrity, solitude, information integrity, and the protection of reputation and personality.[180] More than 150 years after Warren and Brandeis first presented the right to privacy to U.S. jurists for their consideration in a famous law review article, privacy has become a central player in U.S. law,[181] even as defining privacy in a comparative cultural context remains exceedingly difficult. The task is made more complex still by the rapidly advancing technology discussed earlier.[182] But to the extent that any agreement has been forthcoming, privacy is generally considered to be that which is asserted by individuals against the demands of a curious and intrusive society.[183]

¶56 Countries around the world strike the balance between the protection of individual privacy and promoting an informed, public debate in many varied ways that flex as perceived national emergencies and social trends ebb and flow.[184] In the United States, this balancing act between privacy and the public's right to know dates back to at least the 1960s. The *New York Times Co. v. Sullivan*[185] and, later, *Hustler Magazine, Inc. v. Falwell*[186] cases, for example, saw the courts support a robust interpretation of the First Amendment and impose heavy burdens of proof on plaintiffs seeking to challenge free speech.[187] Eventually, even the most tangential relationship to a matter of public interest became sufficient to convert a private person into a public figure, giving rise to what Justice Harlan said was "a severe risk of irremediable harm to individuals involuntarily exposed to [publicity] and powerless to protect themselves against it."[188]

¶57 Privacy, and the related concept of confidentiality, arise in the wearables context in that the intimate details of peoples' private lives may be exposed depending on the technology in question. Specifically, wearables present worrying scenarios whereby an

---

[180] *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (advocating a pragmatic approach to conceptualizing privacy).

[181] Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights of Public Figures*, 19 AM. BUS. L.J. 125, 126-27 (2012) (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (calling for the common law to protect the privacy of the individual)).

[182] *See supra* Sections II-III.

[183] Shackelford, *supra* note 181, at 27 (citing Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989) (stating that the common law tort of invasion of privacy is predicated by an assumption of the personal harm that comes from violating the social norm)).

[184] *See* Emmanuel Gross, *The Struggle of a Democracy Against Terrorism-Protection of Human Rights: The Right to Privacy Versus the National Interest –The Proper Balance,* 37 CORNELL INT'L L.J. 27, 28-30 (2004) (recognizing that national tragedies can cause legal responses that limit privacy in extreme and irrational ways).

[185] 376 U.S. 254 (1964).

[186] 485 U.S. 46 (1988); *see also* Donna R. Euben, Comment, *An Argument for an Absolute Privilege for Letters to the Editor After* Immuno Ag v. Moor-Jankowski, 58 BROOKLYN L. REV. 1439, 1454-55 (1993) (discussing cases where hyperbole, rhetoric, and satire have been given First Amendment protection).

[187] Maria Sguera, Note, *The Competing Doctrines of Privacy and Free Speech Take Center State After Princess Diana's Death*, 15 N.Y.L. SCH. J. HUM. RTS. 205, 215–16 (1998).

[188] Time, Inc. v. Hill, 385 U.S. 374, 410 (1967) (Harlan, J., concurring in part and dissenting in part); *see also* Sguera, *supra* note 187, at 219-20 (detailing cases of involuntary public figures).

employee's private information was breached, intentionally or unintentionally, making that person into a figure of public interest. Once that breach occurs in the United States, the person would be deemed an involuntary public figure and would have substantially limited privacy rights for the remainder of his or her life, in contrast to European, particularly German, citizens (an aside relevant for multinational firms).[189] Nor has the presence of guiding international law on the subject caused privacy rights to converge. Many nations agree in principle that the individual's right to privacy is a human right recognized in international treaties including the 1948 Universal Declaration of Human Rights, and the 1966 International Covenant on Civil and Political Rights.[190] But it is in answering what constitutes infringement of this right that cultural differences begin to arise.[191] A step was taken in this direction, though, in late 2013 when the UN General Assembly unanimously backed a "right to privacy in the digital age" in the aftermath of former NSA contractor Edward Snowden's revelations.[192] Multinational companies, including the likes of Google, are also pushing for globalized privacy standards.[193] Fighting against this desire for global convergence of privacy standards, though, are domestic courts, particularly the U.S. Supreme Court and the European Court of Human Rights, the latter of which is causing privacy law to converge in Europe even as it diverges more with the United States.[194]

¶58 Indeed, the well-documented European approach to privacy protections has particular salience in the private-sector wearables context. For example, the European Data Protection Supervisor ("EDPS") issued a series of guidelines regulating the protection of personal data by EU entities that could be instructive to companies seeking to develop robust privacy regimes to guarantee employee rights. Specifically, under Section 5 of the regulation, data subjects have the rights to:

- **Access** any personal data held by an EU institution as well as learn whether or not their data is being processed and for what purpose;
- **Rectify** "without delay of inaccurate or incomplete data" and to have that data blocked if it is contested;
- **Erase** data that is used unlawfully or is unduly sensitive;

---

[189] In Germany, for example, courts have developed a tripartite approach to classify privacy rights, delineating permanent public figures (e.g., prominent politicians), celebrity public figures (e.g., famous actresses), and temporary public figures (e.g., victims of violent crimes) in a way that few if any other civil law jurisdiction has attempted. For more information on this topic, see Shackelford, *supra* note 181, at 186.

[190] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III), at art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."); International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI) A, U.N. GAOR, 21st Sess., U.N. Doc. A/6456, at art. 17 (Dec. 16, 1966) (reiterating text from Universal Declaration of Human Rights).

[191] *See, e.g.*, Ioannis Karakostas, *Public Figures and Right of Privacy in Greek Private Law*, INST. GLOBAL L. (1998), http://www.ucl.ac.uk/laws/global_law/publications/institute/docs/karakostas.pdf [perma.cc/SB3X-LNQZ] (discussing how Greek courts have interpreted the U.N. Resolutions).

[192] *General Assembly Backs Right to Privacy in Digital Age*, UN NEWS CTR. (Dec. 19, 2013), http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1= - .UtKxrPYjBkU [perma.cc/W7LU-URR4].

[193] *See* Paul Hale, *Google Backs Calls for Global Privacy Standards*, THINQ (Oct. 28, 2010), http://www.thinq.co.uk/2010/10/28/google-backs-calls-global-privacy-standards/ [perma.cc/ZRH8-BZJ2] (following on the heels of the backlash against Google's Street View site).

[194] *See* Shackelford, *supra* note 181, at 207.

- **Notify third parties** about data that has been deleted, rectified, or blocked;
- "**Object** at any time to the processing of data relating to them"[195]

¶59 Companies wishing to be market leaders in the employee privacy wearable context can and should include such transparent policies in their programs. For example, there should be a right for all employees to access any data coming from provided wearables, to rectify inaccurate information, have control over how the data is shared with the firm and/or third parties, and to retain the right to object to and ultimately erase the information if it is unduly sensitive. Such standards could be written into corporate ethical guidelines, such as by amending Morgan Stanley's Code discussed above. This is not meant as an exhaustive list, but merely a starting point to help jumpstart a conversation about helpful guidelines to ensure that employee privacy is neither sacrificed on the mantles of security or productivity growth.

¶60 Aside from the applicable law and best practices, ethical considerations also pervade the employee privacy context surrounding wearables providing ample opportunities for nudging. Nor is this a new problem. More than a decade ago, for example, a Las Vegas casino began using active RFID tags on restaurant employees to track their activity, prompting employee complaints similar to those discussed in Section II.[196] Indeed, *all* of these policy issues–accountability, security, and privacy–are essentially timeless for the very reasons Plato set out thousands of years ago. The fact that they continually recur is not grounds for giving up on them as a hopelessly irresolvable set of ethical dilemmas. Instead the social reality of humans living together, with continually evolving technological changes, means that individuals, companies, governments, and other organizations must be prepared to address them in the future.

III. LOOKING AHEAD TO WIDESPREAD USE

¶61 Although neither the law nor regulation has yet to delineate the parameters and permissible limits of the use of wearables in the employment context, the legal community and case law has fleshed out some related areas that provide guidance for where the law may head in the near future. For example, while the law may seek to protect unsuspecting employees or unauthorized gathering of information, current trends lead to the conclusion that few protections will exist when an employee consents to the information gathering and use within the employment context.[197] And, when employees are provided incentives to allow information gathering, there is little evidence that refutes the hypothesis that the right incentive will encourage an employee to consent to providing treasure troves of personal

[195] GUIDELINES ON THE RIGHTS OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA 7 (2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf [perma.cc/5J6V-NHRM].

[196] *See* Will Sturgeon, *Las Vegas Casino Goes for RFID*, SILICON.COM (Apr. 15, 2005), http://www.siliconinvestor.com/readmsgs.aspx?subjectid=54298&msgnum=928&batchsize=10&batchtype=Previous [perma.cc/8K4F-XFSL].

[197] *See* Adam D. Moore, *Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy*, 10 BUS. ETHICS Q. 697, 701–02 (2000).

information.[198] When conflicts of interest are a genuine concern of the business implementing the use of wearables, one wonders if the argument could not be made of a "business interest" thereby eliminating the need for consent to gather and use the information.[199] In fact, the Federal Trade Commission released a report on the *Internet of Things*[200] in January of 2015 which supports the extension of existing law into the area of wearables, by advancing the proposition that:

> The consensus at the FTC seems to be that there should be 'privacy by design' incorporated into such devices to avoid security breaches and unauthorized access and misuse of personal information, and that consumers should have some notice and choice with regard to sharing their data. No one advocated special regulations for this aspect of data sharing, but the FTC wants to have a general federal privacy statute that would be broad, flexible and not technology specific, that would allow the FTC to give guidance on data security and online tracking, among other things.[201]

¶62 The Federal Trade Commission, federal law, and various state and federal cases have all found that employees are to be treated as a distinct class within the wearable context.[202] Regardless of the examination focal point—that of employees or consumers—the trend is to design the regulation of information gathering through the notice and consent paradigm richly established within U.S. law. Equally central is the role of ethics, especially when members of the community have already declared a "creepiness" of the technology in question.[203] Many people wonder if the use of technology as an "angel on your shoulder" reduces personal autonomy and self-governing, inhibiting effective polycentric regulation and ignoring the literature on nudging to effect positive change.[204] For example, as previously discussed eye-tracking software[205] combined with technology that nudges a

---

[198] For example, the Cleveland Clinic, a self-insured medical center with an estimated 40,000 employees, offers discounts on its insurance plans when certain health and fitness goals are attained. The program boasts a participation rate of 60 percent. *See* Jennifer Booton, *You May Be Forced To Wear A Health Tracker At Work*, MARKETWATCH (Mar. 12, 2015), http://www.marketwatch.com/story/you-might-be-wearing-a-health-tracker-at-work-one-day-2015-03-11 [perma.cc/J2R6-ZAT4].

[199] It is not as if many employees are not monitored, including near constant videotaping, even while performing the most mundane of tasks. *See* Ashlee Kieler, *Panera Bread Wants To Tape Its Employees While They Make Your Food*, CONSUMERIST (Mar. 18, 2015), http://consumerist.com/2015/03/18/panera-bread-wants-to-tape-its-employees-while-they-make-your-food/ [perma.cc/CHD4-YC4R].

[200] *See generally* FEDERAL TRADE COMMISSION, INTERNET OF THINGS (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [perma.cc/WR8G-SRGS].

[201] Dee Pridgen, *ABA Consumer Protection Conference Focuses on Big Data, Internet of Things and Ad Substantiation Standards*, PUBLIC CITIZEN, (Feb. 15, 2015) http://pubcit.typepad.com/clpblog/2015/02/aba-consumer-protection-conference-focuses-on-big-data-internet-of-things-and-ad-substantiation-standards.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+ConsumerLawPolicyBlog+%28Consumer+Law+%26+Policy+Blog%29 [perma.cc/7Q7G-CZLH].

[202] *See* Moore, *supra* note 197.

[203] *See* Todd Essig, *'Big Data' Got You Creeped Out? Transparency Can Help*, FORBES (Feb. 27, 2012), http://www.forbes.com/sites/toddessig/2012/02/27/big-data-got-you-creeped-out-transparency-can-help/ [perma.cc/M3AX-S7RZ].

[204] *See* Sunstein, *supra* note 117.

[205] *See* Arryn Robbins & Michael C. Hout, *New Technologies Track Our Eyes—And Read Our Minds*, SCI. AM. (Dec. 18, 2014), http://www.scientificamerican.com/article/new-technologies-track-our-eyes-and-read-our-

participant into a particular decision making path[206] certainly reduces personal autonomy, but the question remains if this is necessarily a bad thing.

¶63 Not surprisingly, the answer is that it depends. It depends on who uses the technology, the degree of nudging and coercion employed, and who gets to see the information produced by the technology. The newness of the technology makes wearables seem scary. That might be a fair assessment. But the ethical, practical, and regulatory issues raised are of the same kind as has been dealt with throughout human history. We should neither dismiss wearables' impact on positive behavior out of hand, nor embrace it naively. We should engage it as rigorously and thoroughly as has been done in previous instances.

¶64 As the more widespread use of 'angel on your shoulder' technology occurs, new issues begin to arise in terms of the use of the data, possibly leaving to the newest of problems; how should we use and regulate big data and the Internet of Things more generally?[207] Monitoring employees has been an ongoing issue, but until recently it was done on a manageable data scale. When big data analytics is combined with the increasingly available data storage and processing power, the issues may become magnified. Consider the examples of Amazon[208] and Target.[209] Both employers have monitored employees for considerable time; both arguing the monitoring improves efficiency and customer satisfaction.[210] Yet, both firms have also discovered the problems associated with creating data systems that fail to recognize the less than obvious limitations of the use of the data and the negative impacts it can have on behavior. As noted authority Konstantin Kakaes comments: "Bad use of data can be worse than no data at all."[211]

¶65 Yet the new reality of the wearable revolution is becoming apparent to some, as biohacker Hannes Sjoblad notes: "The weakness in wearables is that people get bored, . . . It is simply another thing that clutters people's lives [..] but we want something which is always on, always there and does not disturb your life."[212] Assuming that Sjoblad is correct, one must wonder if the ubiquitous integration of the connected body will not reduce the employees' attention to information gathering. One must wonder if one day employees – and consumers for that matter – will not become so accustomed to non-stop

---

minds/?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed%3A%2Bsciam%2Fmind-and-brain%2B%28Topic%3A%2BMind%2B%2526%2BBrain%29 [perma.cc/5R2L-SCVZ].

[206] See Maxim Lott, *Gov't Knows Best? White House Creates 'Nudge Squad' To Shape Behavior*, FOX NEWS (July 30, 2013), http://www.foxnews.com/politics/2013/07/30/govt-knows-best-white-house-creates-nudge-squad-to-shape-behavior/ [perma.cc/3J3Z-MS4M]. For the book, see THALER & SUNSTEIN, *supra* note 115.

[207] See EXEC. OFF. OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), http://images.politico.com/global/2014/05/01/big_data_privacy_report_may_1_2014.pdf [perma.cc/6HFG-NE74].

[208] *See* Hamilton Nolan, *The Lamentations of Amazon Customer Service Agents*, GAWKER (June 20, 2014), http://gawker.com/the-lamentations-of-amazon-customer-service-agents-1593896869 [perma.cc/J33Z-T3ND].

[209] *See* Hamilton Nolan, *Target Manager: "If You Weren't Cheating, You Weren't Trying*," GAWKER (Feb. 25, 2014), http://gawker.com/target-manager-if-you-werent-cheating-you-werent-try-1530768069 [perma.cc/43BU-4ZAK].

[210] *See id*.

[211] Konstantin Kakaes, *The Big Dangers Of 'Big Data'*, CNN (Feb. 4, 2015) http://www.cnn.com/2015/02/02/opinion/kakaes-big-data/ [perma.cc/8L47-F6CC].

[212] Charlie Osborne, *Chips Under The Skin: Biohacking, The Connected Body Is 'Here To Stay,* ZDNET (Feb. 17, 2015), http://www.zdnet.com/article/chips-under-the-skin-the-connected-body-is-here-to-stay/ [perma.cc/MG7A-WJ3Q].

information gathering that we must begin to engage in a discussion about the best means to ensure "knowing consent," a topic that the authors have previously argued as a growing problem within the online, interconnected world.[213] Assuming the question follows the same trajectory of existent law – that being that notice, not actual knowledge, is the legal standard[214] – then we are again left with considering the ethical dilemma without regulatory or legal protections.

¶66 The issue of fading raises long-term issues. Wearables, in some ways, are new and therefore capture our collective attention. Their novelty may fade, and with it, the appetite for notices and consent as well. The opportunity for manipulation, however, will likely continue. This means that the necessary ethical and regulatory infrastructure for managing wearables is durable beyond temporal headlines.

¶67 Consequently, any ethical discussion on the use of wearables must recognize the reality of the growth of the use of wearables by employees, but must temper the expectations of an employer monitoring, gathering and compiling data in a manner that will be overly intrusive or "creepy' feeling to the employee. Moreover, employers must be aware to the impact that data monitoring and gathering may have on the employee and must never underestimate the fragile nature of privacy lost. In addition, it is important that employees draw bright lines between employer activities that are designed to overcapture or unnecessarily monitor employees, versus the employer that seeks to create a more efficient, appreciated, and engaged employee. A large part of this issue is resolved through the implementation of transparent guidelines for information gathering and continued updates about new uses to which the data shall be put, such as by adapting the EU EDPS guidelines discussed above.

¶68 The use of wearables presents opportunities for the employee and employer to have a level of psychological accountability without the need to have an authority figure present. However, this can have negative consequences, such as the individuals desire to game the system to garner approval. Thus, wearables that provide direct feedback, especially those that nudge, must be utilized with an eye toward limiting the impact of the absent authority figure phenomenon. While self-awareness is a positive, the use of data to more widely encourage accountability may become an issue, especially when rewards are competitive.

¶69 Finally, privacy must become a focus of current and future discussions. The European Data Protection Supervisor provides a useful series of guidelines regulating the protection of personal data that should be used as the starting point for a robust discussion in terms of employees and wearable devices. Employees should have the right to know when information is being gathered and to what use the information is being put. Most importantly, employees must have the ability to correct incorrect or misleading information. And, as a point of discussion, employees should be granted the right to insist upon reward-based systems that consider more than information obtained from wearables.

---

[213] *See* Anjanette H. Raymond, *It's Time the Law Begins to Protect Consumers from Significantly One-Sided Arbitration Clauses within Contracts of Adhesion*, 91 NEBRASKA L. REV. 666, 667 (2013).

[214] *See* Anjanette H. Raymond, *Yeah, But Did You See the Gorilla? Creating and Protecting an 'Informed' Consumer in Cross Border Online Dispute Resolution*, 19 HARV. NEGOT. L. REV. 129, 130 (2014).

CONCLUSION

¶70 The potential for technology, especially wearables, to provide an 'angel on your shoulder' is no longer a matter of debate. The technology exists, and at times it is already being used to assist, influence, and nudge individual's decision-making processes. Moreover, the gathering of such information allows individuals to self-regulate consistent with polycentric governance and may allow authority figures to use information to increase accountability. Unfortunately, accountability does not ensure, however, that authority figures are using the captured information to ensure positive, moral decision making, nor does it ensure individuals are not using the information to game reward systems. Thus, we argue that cybersecurity and privacy guidelines, such as envisioned by the EDPS and the NIST Framework, should be implemented from the bottom-up. Market leaders should act as norm entrepreneurs, working to identify cybersecurity and privacy best practices and help ensure that the angel on your shoulder does not turn into a devil.