William & Mary Law Review

Volume 61 | Issue 1 Article 3

10-2019

The Internet of Bodies

Andrea M. Matwyshyn

THE INTERNET OF BODIES

ANDREA M. MATWYSHYN*

ABSTRACT

This Article introduces the ongoing progression of the Internet of Things (IoT) into the Internet of Bodies (IoB)—a network of human bodies whose integrity and functionality rely at least in part on the Internet and related technologies, such as artificial intelligence. IoB devices will evidence the same categories of legacy security flaws that have plagued IoT devices. However, unlike most IoT, IoB technologies will directly, physically harm human bodies—a set of harms courts, legislators, and regulators will deem worthy of legal redress. As such, IoB will herald the arrival of (some forms of) corporate software liability and a new legal and policy battle over the integrity of the human body and mind. Framing this integrity battle in light of current regulatory approaches, this Article offers a set of specific innovation-sensitive proposals to bolster corporate conduct safeguards through regulatory agency action, contract, tort, intellectual property, and secured transactions and bankruptcy.

Yet, the challenges of IoB are not purely legal in nature. The social integration of IoB will also not be seamless. As bits and bodies meld and as human flesh becomes permanently entwined with hardware,

---

* Associate Dean of Innovation and Professor of Law and Engineering Policy, Penn State Law (University Park); Professor of Engineering Design, Penn State Engineering; Founding Director Penn State Policy Innovation Lab of Tomorrow (PILOT); Affiliate Scholar, Center for Internet and Society, Stanford Law School; Senior Nonresidential Fellow, Cyberstatecraft Initiative, Atlantic Council. She wishes to thank: Matt Blaze, Ian Brown, Trevor Callaghan, Andrea Coravos, Jennifer Chandler, Joshua Corman, Richa Dasgupta, Lilian Edwards, Jen Ellis, Thomas Eovaldi, Mark Geistfeld, James Green, Wendy Grossman, Oona Hathaway, Chris Hoofnagle, Elizabeth Jex, Mark Lemley, Karen Levy, Christopher Marsden, Brian Martin, Terrell McSweeny, Janine Medina, Miranda Mowbray, Alexander Nally, Frank Pasquale, Stephanie Pell, Judith Rauhofer, Martin Redish, James Rule, Suzanne Schwartz, Abigail Slater, Nicolas Terry, Marcia Tiersky, and Beau Woods.

software, and algorithms, IoB will test our norms and values as a society. In particular, it will challenge notions of human autonomy and self-governance. Legal scholars have traditionally considered Kantian autonomy as the paradigmatic lens for legal determinations impacting the human body. However, IoB threatens to undermine a fundamental precondition of Kantian autonomy—Kantian heautonomy. Damaged heautonomy renders both Kantian autonomy and deliberative democracy potentially compromised. As such, this Article argues that safeguarding heautonomy should constitute the animating legal principle for governance of IoB bodies. The Article concludes by introducing the companion essay to this Article, The Internet of Latour's Things. *This companion essay inspired by the work of Bruno Latour offers a sliding scale of "technohumanity" as a framework for the legal and policy discussion of what it means to be "human" in an age where bodies are the "things" connected to the Internet.*

TABLE OF CONTENTS

INTRODUCTION

"[F]reedom of thought ... is the matrix, the indispensable condition, of nearly every other form of freedom."
—J. Benjamin Cardozo.[1]

"This is your last chance. After this, there is no turning back. You take the blue pill—the story ends, you wake up in your bed and believe whatever you want to believe. You take the red pill—you stay in Wonderland and I show you how deep the rabbit-hole goes.... Remember ... all I'm offering is the truth. Nothing more."
—Morpheus, *The Matrix*.[2]

We are building an "Internet of Bodies"—a hybrid society where computer code and human corpora blend and where the human body is the new technology platform. In November 2017, the Federal Drug Administration (FDA) approved the first use of a "digital pill"[3] that communicates from inside the patient's stomach through sensors,[4] a smartphone,[5] and the Internet.[6] A year earlier, the FDA

1. Palko v. Connecticut, 302 U.S. 319, 326-27 (1937).

2. THE MATRIX (Warner Bros. Pictures 1999).

3. *FDA Approves Pill with Sensor that Digitally Tracks if Patients Have Ingested Their Medication*, U.S. FOOD & DRUG ADMIN. (Nov. 13, 2017), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm584933.htm [https://perma.cc/F2VV-RLM7]. The concept of a digital pill had been previously approved by the FDA in 2012. *See, e.g.*, Amy Maxmen, *Digital Pills Make Their Way to Market*, NATURE (July 30, 2012, 9:31 PM), http://blogs.nature.com/news/2012/07/digital-pills-make-their-way-to-market.html [https://perma.cc/FG9U-MYPF]; *see also* Peter Murray, *No More Skipping Your Medicine—FDA Approves First Digital Pill*, FORBES (Aug. 9, 2012, 11:15 AM), https://www.forbes.com/sites/singularity/2012/08/09/no-more-skipping-your-medicine-fda-approves-first-digital-pill/ [https://perma.cc/PR6T-5EKY].

4. Sensors for monitoring body functions may be as small as one millimeter. Amelia Heathman, *This 1mm Sensor Could Monitor Your Body in Real-Time*, WIRED (Aug. 4, 2016), http://www.wired.co.uk/article/wireless-sensors-monitor-body [https://perma.cc/FUB6-SD9Q].

5. The device transmits data to devices the patient (or a doctor) designates. Erin Kim, *'Digital Pill' with Chip Inside Gets FDA Green Light*, CNN MONEY (Aug. 3, 2012, 12:39 PM), https://money.cnn.com/2012/08/03/technology/startups/ingestible-sensor-proteus/ [https://perma.cc/LW6H-GGKY] ("The chip works by being imbedded into a pill.").

6. Robert Glatter, *Proteus Digital Health and Otsuka Seek FDA Approval for World's First Digital Pill*, FORBES (Sept. 14, 2015, 8:09 AM), https://www.forbes.com/sites/robertglatter/2015/09/14/proteus-digital-health-and-otsuka-seek-fda-approval-for-worlds-first-digital-medicine/ [https://perma.cc/8JFD-R4GS].

approved the first artificial pancreas—a device for Type 1 diabetics that is hard-wired into patients' bodies and relies on software to calibrate insulin levels on an ongoing basis.[7]

These FDA approvals are a harbinger of the next generation of innovation, one that merges the Internet of Things[8] and artificial intelligence with the human body. This "platformization" of the body holds great promise: it is already leading to groundbreaking changes in healthcare and in lifestyle convenience.[9] However, using the human body as a platform also introduces new categories of possible harm to the confidentiality, integrity, and availability of the bodies used as part of the hardware.[10]

Three months prior to the digital pill's approval, in August 2017, the FDA issued a safety communication warning patients with a particular implanted pacemaker that they should visit their doctors immediately for a firmware[11] update.[12] The notice warned patients that a potentially serious security vulnerability in the code of their embedded medical device might enable a third-party attacker to compromise their pacemaker system and potentially physically harm them.[13] This communication marked a critical moment in the history of innovation: it was the first FDA recall of a device solely for an information security issue.[14]

---

7. Susan Scutti, *'Artificial Pancreas' for Type 1 Diabetes Wins FDA Approval*, CNN (Sept. 29, 2016, 6:13 PM), https://www.cnn.com/2016/09/29/health/artificial-pancreas/index.html [https://perma.cc/C4RK-LKHD].

8. U.S. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 1-2 (2015) [hereinafter U.S. FED. TRADE COMM'N, INTERNET OF THINGS], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/W5DL-A4FT] (describing the Internet of Things as the totality of consumer and other devices that connect to the Internet).

9. *See* Glatter, *supra* note 6.

10. *Id.*

11. Firmware is computer code built into a piece of hardware. Margaret Rouse, *Definition: Firmware*, WHATIS.COM (Apr. 2017), https://whatis.techtarget.com/definition/firmware [https://perma.cc/VL6M-R7KB].

12. *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication*, U.S. FOOD & DRUG ADMIN. (Aug. 29, 2017), https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm573669.htm [https://perma.cc/8LB5-JHJ7].

13. *Id.*

14. *See* Evan Sweeney, *FDA Announces Firmware Update to Resolve Cybersecurity Vulnerabilities in Abbott Pacemakers*, FIERCEHEALTHCARE (Aug. 30, 2017, 10:15 AM), https://www.fiercehealthcare.com/privacy-security/fda-rolls-out-firmware-update-to-resolve-

The August 2017 pacemaker security recall was not, however, the first time that computer code put human bodies at risk of physical harm and death.[15] Indeed, a year prior, a patient's heart surgery had been unexpectedly interrupted[16] for five minutes[17] when one of the Internet-enabled machines attached to the patient's body crashed.[18] The machine had unexpectedly performed an anti-malware scan in the middle of the operation[19] and locked up the human interface—the interface upon which the surgeons were relying to keep the patient alive.[20]

This creeping merger of bodies with bits and bytes is also not limited to medical contexts. Employers are throwing "chip[ping] part[ies],"[21] embedding their employees' bodies with chips[22] that

---

cybersecurity-vulnerabilities-abbott [https://perma.cc/K8UZ-X83P]; *see also* Richard Staynings, *FDA Announces First-Ever Recall of a Medical Device Due to Cyber Risk*, CISCO BLOG (Aug. 30, 2017), https://blogs.cisco.com/healthcare/fda-announces-first-ever-recall-of-a-medical-device-due-to-cyber-risk [https://perma.cc/PSC8-P59R].

15. *See, e.g.*, Anne Marie Porrello, Death and Denial: The Failure of the THERAC-25, A Medical Linear Accelerator (unpublished computer science paper) (on file with California Polytechnic State University), http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/THERAC25.html [https://perma.cc/5X8L-4ZPN] (chronicling death or severe radiation injury to patients due to software malfunction).

16. Dan Goodin, *That Time a Patient's Heart Procedure Was Interrupted by a Virus Scan*, ARS TECHNICA (May 16, 2016, 1:58 PM), https://arstechnica.com/information-technology/2016/05/faulty-av-scan-disrupts-patients-heart-procedure-when-monitor-goes-black/ [https://perma.cc/9HE3-D38U].

17. [I]n the middle of a heart catheterization procedure, the hemo monitor pc lost communication with the hemo client and the hemo monitor went black. Information obtained from the customer indicated that there was a delay of about 5 minutes while the patient was sedated so that the application could be rebooted. It was found that anti-malware software was performing hourly scans.

MAUDE Adverse Event Report: Merge Healthcare Merge Hemo Programmable Diagnostic Computer, U.S. FOOD & DRUG ADMIN. (Feb. 8, 2016), https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/detail.cfm?mdrfoi__id=5487204 [https://perma.cc/LQV5-UJPE] [hereinafter *MAUDE Adverse Event Report*].

18. Jacob Brogan, *An Antivirus Scan Shut Down a Medical Device in the Middle of Heart Surgery*, SLATE (May 5, 2016, 4:34 PM), https://slate.com/technology/2016/05/antivirus-scan-shuts-down-merge-hemo-medical-device-during-heart-surgery.html [https://perma.cc/G9VM-VCRB].

19. Fortunately, the heavily sedated patient survived the operation, but this outcome was not guaranteed. *Id.*

20. In its FDA incident report, the manufacturer of the equipment blamed the hospital technicians for a misconfiguration, stating that prominent disclaimers existed with the accompanying materials. *MAUDE Adverse Event Report*, *supra* note 17.

21. Jeff Baenen, *Wisconsin Company Holds 'Chip Party' to Microchip Workers*, CHI. TRIB. (Aug. 2, 2017, 7:32 AM), https://www.chicagotribune.com/bluesky/technology/ct-wisconsin-

connect with other devices[23] and transmit information[24] from employees' bodies.[25] Trucking companies sometimes now expect their drivers to wear clothing or devices that monitor location and alertness[26] and (ostensibly) "improve"[27] job performance.[28] Manufacturers

company-microchips-workers-20170801-story.html [https://perma.cc/3ARQ-L5RY]; *see* James Brooks, *A Swedish Start-Up Has Started Implanting Microchips into Its Employees*, CNBC (Apr. 3, 2017, 12:02 PM), https://www.cnbc.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html [https://perma.cc/Z4U2-NJ4C]; Rory Cellan-Jones, *Office Puts Chips Under Staff's Skin*, BBC NEWS (Jan. 29, 2015), https://www.bbc.com/news/technology-31042477 [https://perma.cc/PD8B-M8H9]; Trent Gillies, *Why Most of Three Square Market's Employees Jumped at the Chance to Wear a Microchip*, CNBC (Aug. 13, 2017, 9:00 AM), https://www.cnbc.com/2017/08/11/three-square-market-ceo-explains-its-employee-micro chip-implant.html [https://perma.cc/G74T-QC2R]; *Wisconsin Company Three Square Market to Microchip Employees*, BBC NEWS (July 24, 2017), https://www.bbc.com/news/world-us-canada-40710051 [https://perma.cc/UUE7-G8NQ].

22. Experts expect this practice to become a norm in future employment. Chris Morris, *Wisconsin Company Holds Party to Implant Workers with Microchips*, FORTUNE (Aug. 2, 2017), http://fortune.com/2017/08/02/wisconsin-company-holds-party-to-implant-workers-with-microchips/ [https://perma.cc/5BVF-VRCZ]. ("Noelle Chesley, an associate professor of sociology at the University of Wisconsin-Milwaukee, tells the Chicago Tribune she expects implanting microchips into employees will become the norm in years to come."). Some employees harbor reservations about the chips. Steven Melendez, *Why Would Anyone Let Their Employer Stick a Microchip into Their Body?*, FAST CO. (July 25, 2017), https://www.fastcompany.com/40444110/why-would-anyone-let-their-employer-stick-a-microchip-into-their-body [https://perma.cc/AJ3H-86C2].

23. Danielle Paquette, *Some Feared Hackers and the Devil. Others Got Microchipped.*, WASH. POST (Aug. 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/08/01/some-feared-hackers-and-the-devil-others-got-microchipped/ [https://perma.cc/H5CB-FKDH].

24. Although current chips generally do not transmit location, the capability is expected in the future. Gillies, *supra* note 21 ("A future version of the microchip could include GPS, and if an employee leaves the company, it won't be removed.").

25. *Microchipping at Work: US Employees Get Voluntarily Implanted at Staff 'Chip Party,'* ABC NEWS (AUSTL. BROAD. CORP.) (Aug. 1, 2017, 8:54 PM), http://www.abc.net.au/news/2017-08-02/microchip-workers-hold-chip-party/8765934 [https://perma.cc/9PF8-V3QA].

26. *See* Olivia Solon, *Eye-Tracking System Monitors Driver Fatigue, Prevents Sleeping at Wheel*, WIRED (May 28, 2013), https://www.wired.co.uk/article/eye-tracking-mining-system [https://perma.cc/6WZJ-K56N].

27. *See* Tim Collins, *The Life-Saving £180 Bracelet that Gives Tired Drivers an Electric Shock if They Begin to Fall Asleep at the Wheel,* DAILY MAIL (July 31, 2017, 8:31 AM), https://www.dailymail.co.uk/sciencetech/article-4746076/Steer-delivers-shocks-drivers-fall-asleep.html [https://perma.cc/U2KL-29ZA].

28. *See How the Internet of Things Is Transforming Construction*, WHITELIGHT GROUP (Aug. 18, 2014), https://whitelightgrp.com/2014/08/18/internet-things-transforming-construction/ [https://perma.cc/PC4C-G5ZM]. For a discussion of body-attached truck-driving devices, see, for example, Karen Levy, *After the Tornado*, YOUTUBE (Nov. 19, 2017, at 5:27), https://www.youtube.com/watch?time_continue=18&v=6kPjsfYSzp4 [https://perma.cc/346M-KMDN].

of "brain sensing"[29] Internet-enabled headbands[30] encourage "professionals" to use the device to monitor a "client's"[31] brain sensations[32] in real time.[33] Simultaneously, these same companies might encourage consumers to use the headbands[34] to facilitate "meditation,"[35] and developers to build out games and other applications incorporating brain data.[36] Other brain sensing headbands are appearing in classrooms, signaling to teachers and remote parents when children are (allegedly) paying attention in class.[37] Meanwhile, consumers are donning augmented reality devices in

29. The creators of this product describe it as a type of "brain-computer interface[ ]." *See Muse: The Brain Sensing Headband Changing the Way the World Thinks*, INDIEGOGO (Apr. 24, 2014), https://www.indiegogo.com/projects/muse-the-brain-sensing-headband#/ [https://perma.cc/P6NR-73X2].

30. *See Technology Enhanced Meditation*, CHOOSE MUSE, http://www.choosemuse.com/ [https://perma.cc/UZC8-C4Q9].

31. The website of the company in question alternates between using the word "patient" and "client." *What Is Muse Connect and What Are the Benefits of Using It?*, MUSE (Oct. 28, 2018), https://choosemuse.force.com/s/article/What-are-the-benefits-of-using-Muse-Connect [https://perma.cc/W5N4-JEPV] ("Monitor patient progress and improve patient outcomes.").

32. Specifically, the headband in question monitors "real-time brainwave information to measure states of focus, relaxation, and mind-wandering." *MUSE—The Head Sensing Headband*, ACUPUNCTURE TRADITIONAL CHINESE MED., https://www.acupunctureclinic.ie/wellness-online-store/ [https://perma.cc/S9NQ-BX67].

33. *See Join the Muse Professional Community*, MUSE PROFESSIONAL, https://choosemuse.com/muse-professionals/ [https://perma.cc/8J7F-K685] ("A personalized dashboard tracks your clients' at-home meditation practice with Muse, so you can view their progress in real time.").

34. Some IoB helmets also promise to stimulate neurons. Madhumita Venkataramanan, *Neuroelectrics' Wireless Brain Helmet Can Electrically Stimulate Your Neurons*, WIRED (May 4, 2015), http://www.wired.co.uk/article/stimulation-station [https://perma.cc/9U4W-FK5G].

35. *Muse: The Brain Sensing Headband*, AMAZON, https://www.amazon.com/muse-brain-sensing-headband-black/DP/B00LOQR37C [https://perma.cc/9AAC-GDRK].

36. *See Muse Developer*, MUSE, http://www.choosemuse.com/developer [https://perma.cc/PR6F-4QMS] ("Receive raw EEG, accelerometer, gyroscope, and battery data [;] [l]everage built-in algorithms for band powers, eye blinks, and jaw clenches.").

37. *Under AI's Watchful Eye, China Wants to Raise Smarter Students*, WALL ST. J. (Sept. 19, 2019, 5:30 AM), https://www.wsj.com/video/under-ais-watchful-eye-china-wants-to-raise-smarter-students/C4294BAB-A76B-4569-8D09-32E9F2B62D19.html [https://perma.cc/US5T-EAUB].

gaming,[38] and they are purchasing clothes[39] and accessories[40] that connect their bodies to the Internet, sharing corporeal information about themselves in real time.[41] Some consumers are even recreationally implanting chips into their bodies for the sake of convenience,[42] allowing their bodies to perform some of the tasks their phones do now.[43] In short, we are experiencing a creeping transformation where human bodies themselves are becoming connected to and sometimes reliant upon software, hardware, and the Internet for portions of their "default" functionality. This is the Internet of Bodies.

In addition to transforming individual bodies,[44] these Internet of Bodies devices also introduce a new level of peril for society in the aggregate. For the first time in our civilization, computer code will be able to physically damage (civilian) human bodies at scale. In other words, particularly as artificial intelligence becomes incorporated into the Internet of Bodies, the confidentiality, integrity, and availability of some human bodies will inevitably become compromised due to flawed and vulnerable software, either individually or *en masse*: the security compromises that plague our networks, devices, and databases today will shift inside (and physically damage) the human body tomorrow. Yet, the law is currently unprepared to

38. *See* Jacob Kleinman, *Augmented Reality Glasses: What You Can Buy Now (or Soon)*, TOM'S GUIDE (Feb. 14, 2018, 8:00 AM), https://www.tomsguide.com/us/best-ar-glasses,review-2804.html [https://perma.cc/E2VU-Y9DT].

39. *See* Michael Sawh, *The Best Smart Clothing: From Biometric Shirts to Contactless Payment Jackets*, WAREABLE (Apr. 16, 2018), https://www.wareable.com/smart-clothing/best-smart-clothing [https://perma.cc/T5ZC-H6EQ].

40. *See* Michael Sawh, *Put a Ring on It: The Best Smart Rings*, WAREABLE (Jan. 28, 2019), https://www.wareable.com/fashion/best-smart-rings-1340 [https://perma.cc/M2DT-ED2L].

41. *See* Ananya Bhattacharya, *Bluetooth-Enabled Vibrating Hotpants Are the Dumbest Smart Things at CES 2017*, QUARTZ (Jan. 6, 2017), https://qz.com/878137/bluetooth-enabled-vibrating-hotpants-are-the-dumbest-smart-things-at-ces-2017/ [https://perma.cc/Y2LW-XJX8].

42. Chips have been used with animal identification for over a decade. Morris, *supra* note 22.

43. Jefferson Graham, *Who Wants to Get 'Chipped'?*, USA TODAY (Aug. 1, 2017, 12:28 PM), https://www.usatoday.com/story/tech/talkingtech/2017/07/29/wa/520034001/ [https://perma.cc/Q7CH-6LZQ].

44. For example, the first Cyborg Olympics recently unveiled some of the innovation in progress in IoB technology. Bloomberg (@business), TWITTER (Nov. 17, 2016, 4:50 PM), https://twitter.com/business/status/799414438675632128 [https://perma.cc/C4Y5-9AZ7] ("Welcome to the first cyborg Olympics.").

address these harms and the social transformation that the Internet of Bodies will occasion.

This Article introduces and explains this (already happening) progression of the Internet of Things or "IoT" into the Internet of Bodies or "IoB."[45] As the "meatware"[46] of human bodies blends with software, hardware, and related technologies[47] in the Internet of Bodies era, jurists, legislators, and scholars will be faced with a dual

45. This author first defined the term Internet of Bodies (IoB) in a legal and policy context in 2016. *See* Andrea Matwyshyn, Northeastern/Princeton/Stanford, The Internet of Bodies, 9th Annual Privacy Law Scholars Conference for Berkeley Center for Law & Technology (June 2, 2016), https://www.law.berkeley.edu/research/bclt/past-events/2016-con ferences/june-2016-the-9th-annual-privacy-law-scholars-conference/program/ [https://perma.cc/YDE3-RM2U]; *see also* Wendy M. Grossman, *Dinosaur Bones*, NET.WARS (June 10, 2016, 6:56 PM), https://www.pelicancrossing.net/netwars/2016/06/dinosaur_bones.html [https://perma.cc/5NZW-FZFL]. Since then, the term has gained resonance with legal and policy audiences. *See Computers, Privacy & Data Protection 2018: The Internet of Bodies*, CPDP2018, https://web.archive.org/web/20180408073819/http://www.cpdpconferences.org/index.html [https://perma.cc/Y2R8-4VMS]. The notion of an "Internet of Bodies" appeared previously on a limited basis in the technology press and forums but without a clear definition or application to legal and policy contexts. *See, e.g.*, Pedro Domingos, *Shall We Have Internet of Bodies (IoB) Similar to Internet of Things (IoT)?*, QUORA, https://www.quora.com/Pedro-Domingos-Shall-we-have-Internet-of-Bodies-IoB-similar-to-Internet-of-Things-IoT [https://perma.cc/MLR9-3XN8]; *Internet of Bodies*, TUMBLR (Feb. 1, 2016), http://internet-of-bodies.tumblr.com/ [https://perma.cc/H2EM-FNUR]; Meghan Neal, *The Internet of Bodies Is Coming, and You Could Get Hacked*, VICE: MOTHERBOARD (Mar. 13, 2014, 2:20 PM), https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked [https://perma.cc/6TVQ-7D7R]; Avi Zins, *Internet of Bodies (IOB)*, SAÚDE ONLINE, https://saudeonline.grupo midia.com/blog/internet-of-bodies-iob-por-avi-zins [https://perma.cc/7SNP-4XP2]. The term "Internet of Bodies" has also been used by creative professional Ghislaine Boddington in a recent talk about the body as a digital canvas. *See Ghislaine Boddington's TEDx Talk*, WOMEN SHIFT DIGITAL, http://www.womenshiftdigital.com/ghislaines-tedx-talk-on-video/ [https://perma.cc/2U2A-XUWZ]. For work on the Internet of Bodies from other disciplines, see CARLO RATTI & MATTHEW CLAUDEL, THE CITY OF TOMORROW 85-87 (2016) (discussing urban planning); *Ghislaine Boddington*, BODY>DATA>SPACE, http://www.bodydataspace.net/who-we-are/core-team/ghislaine/ [https://perma.cc/LRA9-ZNDQ]. The term has also appeared elsewhere in the context of wearable clothing. *See* Erin Lewis, *Pechakucha Vol. 21 Erin Lewis—Internet of Bodies*, YOUTUBE (July 4, 2013), https://www.youtube.com/watch?v=6OeePCEumUw [https://perma.cc/P75L-M98F].

46. *See Meatware*, URB. DICTIONARY, https://www.urbandictionary.com/define.php?term=meatware [https://perma.cc/37Q4-PWK4].

47. In particular, machine learning algorithms and "artificial intelligence" become increasingly common as part of the functionality of Internet of Bodies devices. All of the concerns regarding security articulated in this Article extend to the machine learning components of IoB devices. Additionally, machine learning introduces a series of other code integrity risks depending on the nature of its functionality. These issues are explored in detail in Andrea M. Matwyshyn, Artifice and Intelligence (unpublished manuscript) (on file with author).

IoB legal challenge. First, they will need to address the unresolved policy and legal quandaries presented by the Internet of Things. Second, they will face a formidable challenge in addressing what a programmer might call the legal "legacy code"[48] problem of software liability more broadly. Just as companies struggle to address the "technical debt"[49] of their systems, the law now faces a somewhat parallel "legal technical debt" challenge. Multiple traditional bodies of law have failed to meaningfully update themselves across time to effectively address changing technology circumstances. As a consequence, resolving this "legal technical debt" will be doctrinally buggy as courts and regulators seek to redress and mitigate bodily harms caused by computer code: crafting suitable methods of redress for both physical and economic IoB harms will implicate a series of sometimes conflicting policy concerns.

Part I introduces the progression of IoT into IoB. Explaining three discrete generations of IoB—body external, body internal, and body melded—Part I locates our current social reality in this progression at stage two—body internal. Yet, using patent filings to reveal expected innovation, Part I argues that late second-generation body internal and early third-generation body melded technologies are already being actively developed. Next, Part I articulates four legacy problems of IoT that will impact the nature of future harms caused by IoB—the "better with bacon" problem of gratuitous Internet reliance and connection, the "builder bias" problem of extreme levels of known (but uncorrected) security vulnerability, the "magic gadget" problem of failing to anticipate failure, and the "mandatory soup" problem of diminishing consumer options for self-help. Part I then presents five areas of law where conflicts over IoB will be most pronounced—guidance from regulatory agencies, contracts, tort, intellectual property, and secured transactions and bankruptcy. Finally, Part I offers concrete approaches for building short term innovation-sensitive legal structures of IoB consumer protection.

Part II then expands on the critical difference between IoB and IoT: IoB's propensity to physically damage human bodies and

48. *See infra* Part I.B.

49. *See* Ward Cunningham, *Debt Metaphor*, YOUTUBE (Feb. 14, 2009), https://www.youtube.com/watch?v=pqeJFYwnkjE [https://perma.cc/SFL9-MQ9X].

minds. IoB presents the specter not only of negative consequences with respect to physical and psychological autonomy— in a Kantian sense—but also, even more fundamentally, third-generation IoB threatens to potentially erode Kantian *heautonomy*—the necessary *precursor* to autonomy. For these reasons, Part II argues that the touchstone for all regulation of IoB must be the safeguarding of heautonomy. Part II concludes by asking an uncomfortable theoretical question about our underlying assumptions regarding the human body: should the law assume the body to be a "bug" or a "feature"? The companion essay to this Article, *The Internet of Latour's Things*, grapples with the question of whether future law will view the corporeality of the human body as worthy of preservation (or elimination) in a society full of IoB bodies. Part III concludes.

I. THE INTERNET OF (HUMAN) THINGS: DEFINING THE "INTERNET OF BODIES"

Morpheus: The Matrix is everywhere. It is all around us. Even now, in this very room. You can see it when you look out your window or when you turn on your television. You can feel it when you go to work ... when you go to church ... when you pay your taxes.[50]

In the 1999 movie *The Matrix*, a computer programmer named Thomas A. Anderson, who uses the handle "Neo," finds out that the physical reality he experiences is actually a computer-generated illusion.[51] After taking a mysterious red pill, he discovers that underneath the superficially placid exterior of the world he inhabits, there lurks a linked invisible society of machine overlords.[52] The machines are powered by energy extrusions from millions of human bodies that have been physically networked together.[53] This web of bodies—the Matrix—allows the machine overlords to harness and commodify the bodies of humans, turning them into merely the

50. THE MATRIX, *supra* note 2.
51. *Id.*
52. *Id.*
53. *Id.*

"hardware" that powers both the machines and the software that perpetuates the simulacrum of the human-viewable world.[54]

The Matrix is, of course, just a movie; a majority of scientists do not believe that the world we currently inhabit is merely an illusion generated by a computer program.[55] However, we are unquestionably entering a technological age where the line between the human body and the machine is beginning to blur.[56] Many human bodies will soon become at least occasionally reliant on the Internet for some aspect of their functionality,[57] and the energy of the human body is already being used experimentally to mine cryptocurrency.[58] Just as the Internet of Things has networked our possessions into a "cloud"[59] of shared gadgetry, so too our bodies are slowly becoming networked into an "Internet of Bodies."[60]

---

54. *Id.*

55. *But see* Andrew Zimmerman Jones, *Are We Living in a Computer Simulation?*, PBS (July 8, 2015), https://www.pbs.org/wgbh/nova/article/are-we-living-in-a-computer-simulation/ [https://perma.cc/87RJ-TLUW]; Clara Moskowitz, *Are We Living in a Computer Simulation?*, SCI. AM. (Apr. 7, 2016), https://www.scientificamerican.com/article/are-we-living-in-a-computer-simulation/ [https://perma.cc/NX7M-YGJ7].

56. *See, e.g.*, Nathan Hurst, *This Digital Prosthesis Could Help Amputees Control Computers,* SMITHSONIAN.COM (Dec. 13, 2016), https://www.smithsonianmag.com/innovation/digital-prosthetic-could-help-amputees-control-computers-180961397/ [https://perma.cc/9R36-P3GA].

57. *What Is the Pancreas? What Is an Artificial Pancreas Device System?*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medicaldevices/productsandmedicalprocedures/homehealthandconsumer/consumerproducts/artificialpancreas/ucm259548.htm [https://perma.cc/6PCL-PJSS].

58. As the Institute for Human Obsolescence has described it: "A single human body at rest radiates 100 watts of excess heat.... The electricity generated is then fed to a computer that produces cryptocurrency." *Biological Labour*, INSTITUTE OF HUMAN OBSOLESCENCE, http://speculative.capital/ [https://perma.cc/Q9SA-7459]; *see also* Daniel Oberhaus, *You Could Mine 1 Bitcoin Per Month If You Harvested the Body Heat from 44,000 People*, VICE: MOTHERBOARD (Jan. 3, 2018, 10:00 AM), https://motherboard.vice.com/en_us/article/vby7ny/bitcoin-body-heat-mining [https://perma.cc/T8SH-57D2].

59. For a discussion of "the cloud," see, for example, Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed to?*, 51 IDAHO L. REV. 661, 670 (2015). Most robots will share information with third parties for processing purposes or just to store information in the cloud. *Id.*

60. For examples of devices in the Internet of Bodies, see *infra* notes 88-93 and accompanying text.

A. Three Generations of IoB

Morpheus: The pill you took is part of a trace program. It's designed to disrupt your input/output carrier signal so we can pinpoint your location.
Neo: What does that mean?
Cypher: It means fasten your seat belt Dorothy, 'cause Kansas is going bye-bye.[61]

In an iconic 1960 episode of *The Twilight Zone*, a misanthropic writer becomes convinced that the appliances in his home are conspiring against him, attempting to intimidate him.[62] His escalating tensions with the machines culminate in his typewriter, television, and telephone informing him that he needs to leave and in his electric shaver menacing him.[63] Ultimately, his car "encourages" his untimely exit.[64]

Despite recent reports of home smart assistants laughing maniacally and scaring their owners,[65] today's Internet of Things—meaning the totality of consumer and other devices that connect to the Internet[66]—usually reflects a less menacing version of *The Twilight Zone*'s sentient appliances.[67] According to some estimates, the number of IoT devices is expected to reach twenty-one billion devices by the year 2020.[68] These devices include everything from

61. THE MATRIX, *supra* note 2.

62. *The Twilight Zone: A Thing About Machines* (Cayuga Productions, CBS Television Network, Oct. 28, 1960).

63. *Id.*

64. *Id.*

65. *See* Christina Bonnington, *Alexa Is Creepily Laughing at People for No Reason*, SLATE (Mar. 7, 2018, 6:28 PM), https://slate.com/technology/2018/03/amazons-alexa-is-creepily-laughing-for-no-reason-its-just-the-start.html [https://perma.cc/9F9X-YRZM].

66. *See* U.S. FED. TRADE COMM'N, INTERNET OF THINGS, *supra* note 8, at 5-6 (summarizing the findings of a workshop held earlier in the year on the topic).

67. However, a recent first-person account of a technology journalist chronicled her begging her home IoT devices to make her a cup of coffee, and a later "emotional" overreaction from her coffee machine due to her absence. *See* Kashmir Hill & Surya Mattu, *The House that Spied on Me,* GIZMODO (Feb. 7, 2018, 1:25 PM), https://gizmodo.com/the-house-that-spied-on-me-1822429852 [https://perma.cc/5N8S-34SN].

68. Nathan Eddy, *Gartner: 21 Billion IoT Devices to Invade by 2020*, INFO. WEEK (Nov. 10, 2015, 11:05 AM), https://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081 [https://perma.cc/FL9A-XWAR].

toys[69] to toasters[70] to cars[71] to hospital respirators[72] to industrial control systems.[73]

According to a recent Federal Trade Commission (FTC) report, our society is merely "at the beginning of this [IoT] technology trend."[74] While asserting that IoT devices potentially offer substantial benefit to consumers in connected medicine and other contexts, the FTC report highlighted the concerning reality that our existing legal paradigms are not optimally suited for the Internet of Things context.[75] In particular, the FTC explained that IoT has created challenges for meaningful consumer consent, privacy, and security.[76]

In a consonant vein, Professor Scott Peppet has argued that in the Internet of Things "the near impossibility of truly de-identifying ... data, the likelihood that Internet of Things devices will be inherently prone to security flaws, and the difficulty of meaningful consumer consent in this context—create very real discrimination,[77] privacy,[78] security,[79] and consent[80] problems."[81] Other scholars have

---

69. *See Electronic Toy Maker Vtech Settles FTC Allegations that It Violated Children's Privacy Law and the FTC Act*, U.S. FED. TRADE COMM'N (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated [https://perma.cc/E3V7-KBYV].

70. *See* Joel Hruska, *The Internet of Things Has Officially Hit Peak Stupid, Courtesy of This Smart Toaster*, EXTREME TECH (Jan. 5, 2017, 4:11 PM), https://www.extremetech.com/electronics/242169-internet-things-officially-hit-peak-stupid-courtesy-smart-toaster-griffin-technology [https://perma.cc/5PX3-N4QR].

71. *See* Jonny Evans, *Just Say No to Connected Cars*, COMPUTERWORLD (July 8, 2015, 10:25 AM), https://www.computerworld.com/article/2945367/just-say-no-to-connected-cars.html [https://perma.cc/BC37-QLSJ].

72. *Philips Hospital Respiratory Care*, PHILIPS, https://www.usa.philips.com/healthcare/solutions/hospital-respiratory-care [https://perma.cc/D75M-Y52S].

73. *See Internet of Things and Industrial Control Systems*, U.K. CTR. FOR THE PROT. OF NAT'L INFRASTRUCTURE, https://www.cpni.gov.uk/internet-things-and-industrial-control-systems [https://perma.cc/QR9E-KQ8B].

74. *See* U.S. FED. TRADE COMM'N, INTERNET OF THINGS, *supra* note 8, at i.

75. "Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach." *Id.* at v.

76. Professor Peppet also highlighted the problems of consent. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 140-46 (2014).

77. Professor Peppet provides the example of an Internet of Things breathalyzer explaining: "the consumer is essentially led to the incorrect assumption that this small black device is merely a good like any other—akin to a stapler or ballpoint pen—rather than a data source and cloud-based data repository." *Id.* at 90.

78. Peppet, for example, argues in favor of data minimization and use constraints: "As a first regulatory step, we should constrain certain uses of Internet of Things data if such uses

focused on behavioral impacts occasioned by a world permeated by the Internet of Things. For example, Professor Meg Leta Jones has asserted that the goal of the Internet of Things, which she dubs the "Internet of Other Peoples' Things,"[82] is to enable "ubiquitous connection"[83] and that "[p]erforming the boundary work necessary to managing one's information becomes increasingly difficult as we move deeper into the Information Age."[84] Professor Paul Ohm and Blake Reid have asked what it means to regulate software when everything around us contains software.[85] Meanwhile, Professor Christina Mulligan has argued that as software becomes increasingly present in consumer goods, Internet of Things merchants will use the licenses to the software contained in these devices to undesirably and materially, contractually restrict both the permitted uses and resale or transfer of devices.[86] Finally, Professor Irina Manta and David Olson have argued that while Internet of Things "[p]rice

---

threaten consumer expectations." *Id.* at 150.

79. "Internet of Things Devices May Be Inherently Prone to Security Flaws," argues Peppet. *Id.* at 133-36.

80. Peppet explains the consent problem as follows:

> The technical problem is simple: coupled with Big Data or machine learning analysis, massive amounts of sensor data from Internet of Things devices can give rise to unexpected inferences about individual consumers. Employers, insurers, lenders, and others may then make economically important decisions based on those inferences, without consumers or regulators having much understanding of that process. This could lead to new forms of illegal discrimination.

Id. at 118.

81. *Id.* at 85. Peppet advocates four approaches to regulating the Internet of Things:

> (1) broadening existing use constraints—such as some state law on automobile EDRs—to dampen discrimination; (2) redefining "personally identifiable information" to include biometric and other forms of sensor data; (3) protecting security by expanding state data-breach notification laws to include security violations related to the Internet of Things; and (4) improving consent by providing guidance on how notice and choice should function in the context of the Internet of Things.

Id. at 149.

82. Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 639 (2015).

83. *Id.* at 641.

84. *Id.* at 645.

85. Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1673-74 (2016).

86. Christina Mulligan, *Personal Property Servitudes on the Internet of Things*, 50 GA. L. REV. 1121, 1122-24 (2016).

discrimination can increase total market welfare in some cases, especially in comparison to monopoly pricing; it also can decrease total market welfare if the pricing is done in such a way as to decrease allocative efficiency."[87]

Building on this prior scholarship, this Article asks what it means for existing legal paradigms and for the next generation of innovation when the "things" that are attached to the Internet are human bodies. In brief, this Article argues that this "Internet of human things" or, more succinctly, this "Internet of Bodies" will cause us to materially reframe our legal conversations when computer code regularly begins to cause *physical* harms to human bodies. But before embarking on this legal analysis, let us define the Internet of Bodies and assess how it mirrors and differs from the Internet of Things.

The Internet of Bodies might be divided into three generations of technologies—body external, body internal, and body melded.[88]

1. First-Generation IoB: Body External

The first generation of IoB devices has already become a familiar fixture in our lives. These devices are seemingly ubiquitous, including everything from "lifestyle" connected fitness tracking devices[89] and "smart" glasses[90] to "smart" exoskeletons,[91] connected breast pumps,[92] and brain-sensing[93] headbands.[94] Specifically, these

87. Irina D. Manta & David S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.*, 67 ALA. L. REV. 135, 157 (2015).

88. *See infra* Parts I.A.1-3.

89. *See, e.g.*, FITBIT, https://www.fitbit.com/home [https://perma.cc/PF46-EWL6].

90. *See* Daniel Van Boom, *China's Police Get Face-Recognizing Glasses Ahead of New Year*, CNET (Feb. 7, 2018, 8:05 PM), https://www.cnet.com/news/china-new-year-police-glasses-ai-cctv [https://perma.cc/DGE3-58DD].

91. *See* Timothy Burke, *Paraplegic in Robotic Exoskeleton Performs World Cup First Kick*, DEADSPIN (June 12, 2014, 3:19 PM), https://deadspin.com/paraplegic-in-robotic-exoskeleton-performs-world-cup-fi-1590050190 [https://perma.cc/RN2M-YLUH].

92. *See* Zoe Kleinman, *CES 2018: Willow and Freemie Breast Pumps Offer Mums Freedom*, BBC NEWS (Jan. 11, 2018), http://www.bbc.com/news/technology-42643971 [https://perma.cc/E3EM-9VJH]. For example, Willow, a connected breast pump, syncs with the Willow app. *See Frequently Asked Questions*, WILLOW, https://www.willowpump.com/faq/ [https://perma. cc/UC3S-NE2M].

93. These headbands include headbands for patients lacking motor function. *See* Mark Honigsbaum, *Could This $300 Headset Transform the Lives of 'Locked-In' Patients?*, GUARDIAN (July 11, 2014, 6:00 AM), https://www.theguardian.com/technology/2014/jul/11/

first-generation IoB devices encompass three categories of body-external products—IoB "medical devices" approved by the FDA,[95] "general wellness"[96] IoB devices that present "low risk" and promote "healthy lifestyle" (and are, therefore, not regulated by the FDA),[97] and various other non-health enterprise, educational, and recreations body-attached devices that connect to the Internet, directly or indirectly.[98]

First-generation IoB medical devices include devices such as Internet-enabled robotic surgery machines[99] and connected prosthetics[100] that a patient operates from a mobile phone.[101] In comparison, the "general wellness/lifestyle" first-generation IoB category encompasses familiar devices such as fitness trackers,[102] health

kickstarter-headset-locked-in-syndrome-communication [https://perma.cc/MAB8-G7UN].

94. IoB headbands also allow gamers to race drones with their minds. *See* Anthony Cuthbertson, *Watch: World's First Mind-Controlled Drone Race*, NEWSWEEK (Apr. 25, 2016, 8:50 AM), http://www.newsweek.com/watch-worlds-first-mind-controlled-drone-race-451965 [https://perma.cc/RCU3-CK9E].

95. *See infra* notes 99-101 and accompanying text.

96. The FDA "defines general wellness products as products that meet the following two factors: (1) are intended for only general wellness use, as defined in this guidance, and (2) present a low risk to the safety of users and other persons." U.S. FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES 2 (2016) [hereinafter GENERAL WELLNESS] (emphasis omitted), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf [https://perma.cc/A2EN-C728].

97. *See id.* at 1; *infra* notes 102-06 and accompanying text.

98. *See infra* notes 107-27 and accompanying text.

99. These first-generation IoB prosthetics are not external, but second-generation body-embedded prosthetics are also already in trials and use. *See* Elaine Yau, *Forget Pokemons—In World First, Hongkonger Applies Augmented Reality to Surgery*, S. CHINA MORNING POST (Aug. 25, 2016, 12:00 PM), http://www.scmp.com/lifestyle/health-beauty/article/2008395/hongkonger-uses-augmented-reality-surgery [https://perma.cc/G9RM-SMRR]; *see also* Homa Alemzadeh et al., *Adverse Events in Robotic Surgery*, PLOS ONE, Apr. 2016, at 2, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4838256/ [https://perma.cc/H356-4GSG].

100. *See, e.g.*, *'Smart Leg' Makes Engineering Prize Shortlist*, BBC NEWS (May 16, 2016), http://www.bbc.com/news/science-environment-36302784 [https://perma.cc/DJ75-TFH8].

101. *See, e.g.*, Eric Limer, *Meet the Man with iPhone-Controlled Bionic Arms*, GIZMODO (Apr. 13, 2013, 5:40 PM), https://gizmodo.com/5994603/meet-the-man-with-iphone-controlled-bionic-arms [https://perma.cc/U79P-FPKK].

102. *See, e.g.*, FITBIT, *supra* note 89.

monitoring tattoos,[103] electronic skin[104] with an organic circuit,[105] and "smart" watches with lifestyle monitoring capability.[106]

But it is the last category of these first-generation IoB devices—enterprise, educational, and recreational devices—that presents perhaps the fastest growing category of first-generation IoB devices. For example, connected glasses[107] and helmets[108] regularly offer workers information in real time in enterprise settings, and exoskeleton projects for soldiers offer new fighting capabilities.[109] Brain sensing headbands that rely on external EEG electrodes are now used in some classrooms, seeking to monitor student attention.[110] Recent patent filings indicate that Amazon has developed a wristband that conducts ultrasonic tracking of a worker's hands to monitor efficiency in performance of an assigned task,[111] and providing

---

103. *See, e.g.*, Rose Etherington, *Biostamp Temporary Tattoo Electronic Circuits by MC10*, DEZEEN (Mar. 28, 2013), https://www.dezeen.com/2013/03/28/biostamp-temporary-tattoo-wearable-electronic-circuits-john-rogers-mc10/ [https://perma.cc/MYY8-GE36].

104. *See* John Boyd, *Electronic Skin Can Track Your Health and Fitness*, FORBES (Apr. 16, 2016, 2:20 AM), https://www.forbes.com/sites/jboyd/2016/04/17/electronic-skin-can-track-your-health-and-fitness [https://perma.cc/XQN4-YTYQ].

105. *See 'Electronic Skin' to Monitor Your Health*, BBC NEWS (Apr. 4, 2017), http://www.bbc.com/news/av/technology-39485527/electronic-skin-to-monitor-your-health [https://perma.cc/7S5Q-7ZNL].

106. *See, e.g.*, *Apple Watch*, APPLE, https://www.apple.com/watch/ [https://perma.cc/TP4N-2U5A].

107. *See* Scott Stein, *Google Glass Returns: This Time, It's Professional*, CNET (July 18, 2017, 9:18 AM), https://www.cnet.com/news/google-glass-2-goes-for-enterprise/ [https://perma.cc/9T8Q-F476].

108. *See* Jenna McKnight, *Daqri's Augmented-Reality Construction Helmet Aims to "Change the Nature of Work,"* DEZEEN (Jan. 27, 2016), https://www.dezeen.com/2016/01/27/daqri-smart-construction-helmet-augmented-reality-wearable-technology/ [https://perma.cc/L94Y-NAFH].

109. Neil C. Bhavsar, *Can Science Transform Us Into Superheroes?*, FUTURISM (Mar. 22, 2017), https://futurism.com/can-science-transform-us-into-superheroes/ [https://perma.cc/TE43-EL93] (citing Dan Lamothe, *Meet the Exoskeleton the Navy Is Testing to Make Sailors Stronger*, WASH. POST (Sept. 3, 2014), https://www.washingtonpost.com/news/checkpoint/wp/2014/09/03/meet-the-new-exoskeleton-the-navy-is-testing-to-make-sailors-stronger/ [https://perma.cc/RVT8-4G89]).

110. *See* WALL ST. J., *supra* note 37.

111. U.S. Patent Application No. 15/083,083, Pub No. 2017/0278051 (filed Mar. 28, 2016) (published Sept. 28, 2017) (Amazon Technologies, Inc., applicant), http://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20170278051&IDKey=0E2634BC1119&HomeUrl=http%3A%2F%2Fappft.uspto.gov%2Fnetacgi%2Fnph-Parser%3FSect1%3DPTO1%2526Sect2%3DHITOFF%2526d%3DPG01%2526p%3D1%2526u%3D%2Fnetahtml%2FPTO%2Fsrchnum.html%2526r%3D1%2526f%3DG%2526l%3D50%2526s1%3D20170278051.PGNR.%2526OS%3D%2526RS%3D [https://perma.cc/PV5D-CVXC].

haptic feedback to guide the employee's hands in the correct direction.[112] Clothing company L.L.Bean has announced that it is connecting its coats and boots to the blockchain[113] using sewn-in sensors,[114] becoming the latest participant in the broader fashion trend of connected clothing[115] with human-computer interfaces.[116] The Massachusetts Institute of Technology and Microsoft Research have developed temporary tattoos a wearer attaches to her body, allowing her to control various devices wirelessly as a convenience.[117] Gaming devices such as virtual skin[118] and augmented[119] or virtual reality headsets[120] allow for recreational blending of physical and digital reality. Networked in-ear translators help with live multilingual communication,[121] and eye-mapping applications[122] turn

112. Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.),* N.Y. TIMES (Feb. 1, 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html [https://perma. cc/8ZDR-SRH8].

113. For a discussion of blockchain technology and how "the recent development of Bitcoin and blockchain technologies has rekindled excitement about their potential among technologists and industry," see Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 313 (2017).

114. Kim S. Nash, *L.L. Bean to Link Boots, Coats to a Blockchain*, WALL ST. J. (Feb. 7, 2018, 1:27 PM), https://blogs.wsj.com/cio/2018/02/07/l-l-bean-to-link-boots-coats-to-a-blockchain/ [https://perma.cc/6DPN-VE3L].

115. *See, e.g.*, Rachel Metz, *Your Next Password May Be Stored in Your Shirt Cuff*, MIT TECH. REV. (Oct. 31, 2017), https://www.technologyreview.com/s/609264/your-next-password-may-be-stored-in-your-shirt-cuff [https://perma.cc/CT3Z-H3E8].

116. For example, connected underwear has been developed to assist workers in lifting tasks as a type of exoskeleton. Maya Dangerfield, *Lab-Created Underwear Could Prevent Back Pain*, CNN BUS. (Aug. 30, 2017), http://money.cnn.com/video/technology/future/2017/08/30/lab-created-underwear-could-prevent-back-pain.cnnmoney/index.html [https://perma.cc/KQ2A-CL3E].

117. Alice Morby, *DuoSkin Temporary Tattoos Can Remotely Control Devices*, DEZEEN (Aug. 17, 2016), https://www.dezeen.com/2016/08/17/mit-media-lab-researchers-duoskin-temporary-tattoos-control-devices/ [https://perma.cc/RFS5-NASQ].

118. *See* The Verge (@verge), TWITTER (July 6, 2017, 11:50 PM), https://twitter.com/verge/status/883216517776773120 [https://perma.cc/UVD7-KLWQ] ("This 'wearable skin' makes virtual reality feel way too real.").

119. *See, e.g.*, Chelsea Gohd, *Magic Leap Shows Off Their New Augmented Reality Headset,* FUTURISM (Dec. 22, 2017), https://futurism.com/magic-leap-shows-new-augmented-reality-headset/ [https://perma.cc/4A6S-3N2Q].

120. *See* Will Greenwald, *The Best VR (Virtual Reality) Headsets of 2018,* PC MAG (Dec. 5, 2017, 12:13 PM), https://www.pcmag.com/article/342537/the-best-virtual-reality-vr-headsets [https://perma.cc/LLM4-WEHC].

121. *See* David Pierce, *Doppler's Futuristic Earbuds Sound Great. They Also Speak Spanish*, WIRED (Oct. 19, 2016, 6:56 AM), https://www.wired.com/2016/10/dopplers-futuristic-earbuds-sound-great-also-speak-spanish [https://perma.cc/Y5Y5-MB5E]; *Discover the Technol-*

eyes into a mouse.[123] Similarly, both Facebook[124] and Microsoft[125] have disclosed that each company is currently working on brain-control interfaces that will allow users to operate computing devices with only their thoughts and the help of external thought-sensing devices.[126] Meanwhile, Nissan has announced work on "[b]rain-to-[v]ehicle" technology that will allow drivers to use "signals from their own brain to make the drive even more exciting."[127] These

---

ogy Behind the System, WAVERLY LABS, http://www.waverlylabs.com/ [https://perma.cc/A4FU-6D2E] ("The Pilot Speech Translation companion app connects the Pilot earbud to our cloud-based translation engine for access to all of our translation features.").

122. *See, e.g.*, Victoria Woollaston, *We Wore Eye-Tracking Goggles on the Tube, in the Name of 'Science,'* WIRED (Oct. 7, 2016), http://www.wired.co.uk/article/exterion-eye-tracking-london-underground [https://perma.cc/DV5W-MHP8].

123. *See* Jing Cao, *The Man Who Created LeapPad Wants to Turn Your Eyes into a Mouse,* BLOOMBERG (Aug. 26, 2016, 7:00 AM), https://www.bloomberg.com/news/articles/2016-08-26/the-man-who-created-leappad-wants-to-turn-your-eyes-into-a-mouse [https://perma.cc/Y2G9-FESF].

124. *See* Thomas Claburn, *Zuckerberg's Absolutely Mental: Brain Sensors that Read YOUR MIND at 100 Words a Minute,* REGISTER (Apr. 20, 2017, 12:02 AM), https://www.theregister.co.uk/2017/04/20/facebook_brain_typing/ [https://perma.cc/ZMY3-YVK4]; Jolene Creighton, *Zuckerberg: Facebook Is Working on a Brain Interface That Lets You "Communicate Using Only Your Mind,"* FUTURISM (Apr. 18, 2017), https://futurism.com/zuckerberg-facebook-will-reveal-a-brain-interface-that-lets-you-communicate-using-only-your-mind/ [https://perma.cc/6ADL-XLBB]; Andrew Griffin, *Facebook Secretly Building Technology to Read People's Minds So They Can 'Type Directly from the Brain,'* INDEP. (Apr. 20, 2017, 8:55 AM), http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-mind-reading-brain-technology-building-8-regina-dugan-pentagon-a7692481.html [https://perma.cc/V967-4854]; Mark Zuckerberg, *Live at F8!*, FACEBOOK (Apr. 18, 2017), https://www.facebook.com/zuck/videos/10103658355917211/ [https://perma.cc/3RRF-29YD].

125. Microsoft's patent explains that neurological data would "modulate a continuous user interface" and that "[n]eurological data can be gathered through a variety of techniques. One non-invasive technique is electroencephalography (EEG)." U.S. Patent Application No. 15/152403, Publication No. 20170329392 (filed May 11, 2016) (published Nov. 16, 2017) (Keskin et al., applicant), http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=20170329392.PGNR [https://perma.cc/Q8ST-ZNUZ]. Microsoft has a second patent application for "changing the state of an application by detecting neurological user intent data associated with a particular operation of a particular application state." U.S. Patent Application 15/152,401, Publication No. 9,864,431 (filed May 11, 2016) (published Jan. 9, 2018) (Keskin et al., applicant), http://patft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9864431.PN.&OS=PN/9864431&RS=PN/9864431 [https://perma.cc/C3NE-YAMP].

126. *See* Andrew Orlowski, *Microsoft Wants to Patent Mind Control*, REG. (Jan. 15, 2018, 3:28 PM), https://www.theregister.co.uk/2018/01/15/microsoft_bci_patent_application/ [https://perma.cc/95R4-XT5H].

127. Some reports state that the driver is required to wear an electrode skullcap. Gareth Corfield, *If You Won't Use Your Brain Our Machine Will Use It for You, Nissan Tells Drivers*,

many examples highlight the reality that IoB is already here and quickly expanding. These examples also portend that our future is one where IoB is likely to be legally and socially transformational, for better or worse.[128]

It is noteworthy that unlike many of the earliest first-generation IoB devices whose stated purpose was "self-archival," i.e., a user's personal data collection for self-reflection and tracking,[129] today's first-generation IoB devices often explicitly disclose that furthering third-party "big data" research[130] is a prime motivator for their data collection.[131] This "big data" motivation in particular often drives IoB products marketed for employment and educational settings.[132] In one case, a brainwave headband company targeted educational institutions,[133] ostensibly to assist with monitoring students' attention levels[134] in educational settings.[135] The company also recently

---

REG. (Jan. 4, 2018, 6:18 PM), https://www.theregister.co.uk/2018/01/04/nissan_brain_controlled_car_wheeze/ [https://perma.cc/63W9-DMZ9].

128. *See supra* notes 74-87 and accompanying text.

129. *See supra* notes 102-06 and accompanying text.

130. For example, DNA samples are uploaded and available through the Internet allowing for cloud-based user analysis in real time. João Medeiros, *DNA Analysis Will Build an Internet of Living Things*, WIRED (Jan. 8, 2016), http://www.wired.co.uk/article/dna-analysis-internet-living-things [https://perma.cc/GGX9-7UEA].

131. In a medical context, the U.K.'s National Health Service has experimented with Google DeepMind's Stream application. Jo Best, *DeepMind and the NHS: What It's Really Like to Use Google's Kidney Health App*, ZDNET (Jan. 10, 2018, 11:00 AM), http://www.zdnet.com/article/deepmind-and-the-nhs-what-its-really-like-to-use-googles-kidney-health-app/ [https://perma.cc/9YTC-4TGU].

132. As explained by Kate Crawford and Jason Schultz, "it is possible to generate a detailed picture about a person's health, including information the person may never have disclosed to a health care provider." Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 98 (2014).

133. Reviews of both the science behind the product and its efficacy have been mixed, at best, with one critique calling it "malfunctioning" and "cringeworthy." AJ Dellinger, *This Malfunctioning Brain-Scanning Headband Was the Most Cringeworthy Demonstration at CES 2016,* DAILY DOT (Jan. 14, 2016, 1:21 AM), https://www.dailydot.com/debug/brainco-brain-control-technology-ces/ [https://perma.cc/6JLB-A5WL]; Paige Rogers, *Company to Collect Brain Wave Data on 1.2 Mil Students in the Classroom*, NOQ REP. (Dec. 4, 2017), https://noqreport.com/2017/12/04/company-collect-brain-wave-data-1-2-mil-students-classroom/ [https://perma.cc/793W-ZQYV].

134. Other brain sensing headband research similarly focuses on attention-level monitoring. Alexandra Simon-Lewis, *This Brain-Imaging Headband Can Reveal How Boring You Are*, WIRED (Feb. 27, 2017), http://www.wired.co.uk/article/brain-imaging-headband-communicate [https://perma.cc/9T8P-DVB5].

135. Ms. Smith, *Company with No Privacy Policy to Collect Brainwave Data on 1.2 Million Students*, CSO (Dec. 5, 2017, 9:00 AM), https://www.csoonline.com/article/3239969/security/

announced its intention to collect data on over a million students to create "the world's biggest brainwave database."[136] In another case, the "Brainternet" project used external EEG nodes and a Raspberry Pi computer to connect a human brain to the Internet in real time[137] in order to continuously monitor brain activity; its creators hope to build a brain application programming interface[138] with bidirectional inputs and outputs.[139]

Legal scholarship has considered a portion of this innovation in the context of what was initially known as the "Quantified Self" movement,[140] primarily assessing the medical desirability and privacy implications of connected devices with health applications.[141] Professor Nicolas Terry expands this analysis to issues of autonomy and data control, explaining that the Quantified Self movement presents an inherent dichotomy of control—while patient collection of "medically inflected" data is encouraged, the definite copy of a

company-with-no-privacy-policy-to-collect-brainwave-data-on-1-2-million-students.html [https://perma.cc/6RRP-GLM4]. Part of the question underlying such devices, however, is what they are actually measuring and whether the collected metrics, in fact, demonstrate optimal student development. *See* Mark Molloy, *Intelligent People Are More Easily Distracted at Work, Study Claims,* TELEGRAPH (Jan. 19, 2016, 11:54 AM), http://www.telegraph.co.uk/news/newstopics/howaboutthat/12107840/IQ-Intelligent-people-are-more-easily-distracted-at-work.html [https://perma.cc/GTS9-LVRJ].

136. Smith, *supra* note 135.

137. Patrick Caughill, *Researchers Have Linked a Human Brain to the Internet for the First Time Ever*, FUTURISM (Sept. 14, 2017), https://futurism.com/researchers-have-linked-a-human-brain-to-the-internet-for-the-first-time-ever/ [https://perma.cc/P7K4-4P78].

138. Wits University, *Biomedical Engineers Connecting a Human Brain to the Internet in Real Time*, MED. XPRESS (Sept. 14, 2017), https://medicalxpress.com/news/2017-09-biomedical-human-brain-internet-real.html [https://perma.cc/X62T-SDHJ].

139. Caughill, *supra* note 137 ("Brainternet can be further improved to classify recordings through a smart phone app that will provide data for a machine-learning algorithm. In future, there could be information transferred in both directions—inputs and outputs to the brain.").

140. *See* Kashmir Hill, *Adventures in Self-Surveillance, A.K.A. The Quantified Self, A.K.A. Extreme Naval-Gazing*, FORBES (Apr. 7, 2011, 11:34 AM), http://www.forbes.com/sites/kashmirhill/2011/04/07/adventures-in-self-surveillance-aka-the-quantified-self-aka-extreme-navel-gazing/ [https://perma.cc/32TX-S8B3]; *The Quantified Self: Counting Every Moment*, ECONOMIST (Mar. 3, 2012), http:// www.economist.com/node/21548493 [https://perma.cc/N9LV-7DCS].

141. Professor Nathan Cortez explains, "[w]hen viewed more broadly, mobile health is part of broader cultural and technological evolutions, including the march towards more personalized medicine, the 'quantified self' movement, the 'lifelogging' phenomenon, and the rising era of 'big data.'" Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1197-98 (2014) (footnotes omitted).

health record will always reside with the medical provider.[142] Similarly, Professor Craig Konnoth explains that the Quantified Self movement positions itself as a way of "knowing oneself,"[143] and Professor Frank Pasquale warns that the Quantified Self combined with Big Data offer "frightening opportunities to cure and exploit human vulnerabilities."[144]

Building on the era of the Quantified Self, the age of the Internet of Bodies presents the next iteration of these concerns: IoB adds legal concerns regarding the *physical safety* and continued functionality of the attached human bodies themselves.[145] It also adds a new autonomy question: the inability to disconnect in some cases. Use of some IoB devices becomes progressively less optional. Perhaps your employer or your school now requires that you wear a location tracking badge or perhaps your medical device manufacturer (mandated by your insurance provider) discontinues all devices without Internet connectivity. In other words, IoB impacts legal interests in *physical* safety—the integrity, availability, and functional autonomy of human bodies, not merely legal concerns with respect to the confidentiality of data originating from those bodies.[146]

Thus, IoB transforms legal questions of data commodification into legal questions about the commodification and physical control of the human body itself. Indeed, the newest first-generation IoB devices sometimes invert the relationship between the attached body and the remote machines, using human bodies purely as fungible and rentable commodities for their physicality and energy

142. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 84 (2014) ("At root such patient curation of health data bespeaks autonomy.... However, it fails to take into account ... the canonical version of the record will remain in the provider's control ... [and] that only the provider-curated copy is protected by HIPAA-HITECH.... A similarly dichotomous result is likely as the medically quantified self develops.").

143. Craig Konnoth, *Health Information Equity*, 165 U. PA. L. REV. 1317, 1341-42 (2017) ("[T]he 'quantified-self' movement promotes data streams as the best form of self-conceptualization and knowledge. This movement promotes the use of devices that not only 'solve problems related to health,' but also produce data ... as a way of knowing oneself.") (footnote omitted).

144. Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 684 (2013) ("An era of 'big data' promises exhilarating and frightening opportunities to cure and exploit human vulnerabilities.").

145. *See infra* notes 283-93 and accompanying text.

146. *See id.*

extrusion, a non-data driven purpose. For example, one Japanese inventor developed a way to rent another person's body as a telepresence "robot" to allow someone to attend a meeting both physically and remotely.[147] In another case, research using external caps of brain electrodes enabled gamers to control the conduct of another player's body through the Internet in order to play a question-and-answer game.[148] Finally, a Dutch startup recently developed suits intended to extract heat from the human body and repurpose it for cryptocurrency mining.[149] Referring to these first-generation IoB cryptocurrency mining suits, Professor Mark Lemley recently quipped, "It only took 18 years for us to actually implement the Matrix."[150]

Professor Lemley's dark humor points to an important and perhaps ethically uncomfortable inversion—the human body is now being leveraged as a functional vehicle to power external, Internet-connected processes.[151] Even when the research described above seeks to generate mature interface technologies[152] with tangible safety[153] and other[154] applications, the "thing-ified" nature of the human body implicit in the undertaking may trigger safety and dignitary concerns (and incredulous callbacks to "body snatcher"

147. Will Knight (@willknight), TWITTER (Jan. 29, 2018, 10:52 PM), https://twitter.com/willknight/status/958231499509149697 [https://perma.cc/6R3C-VNSS] ("'Human Uber,' developed in Japan, provides a way to attend events remotely using another person's body.").

148. George Dvorsky, *This Gamer Used His Thoughts to Control the Movements of Another Player*, GIZMODO (Nov. 6, 2014, 12:30 PM), https://io9.gizmodo.com/new-brain-interface-allows-for-mind-to-mind-video-gamin-1655415879 [https://perma.cc/W37N-N423].

149. Camille Charluet, *This Startup Uses Body Heat to Mine Crypto—for When Robots Take Our Jobs*, NEXT WEB (Dec. 12, 2017, 12:21 PM), https://thenextweb.com/insider/2017/12/12/startup-uses-body-heat-to-mine-crypto-for-when-robots-take-jobs/ [https://perma.cc/UB2G-WP74].

150. Mark Lemley (@marklemley), TWITTER (Dec. 15, 2017, 10:55 AM), https://twitter.com/marklemley/status/941743490316222465 [https://perma.cc/HQL9-UYBQ].

151. *See* INSTITUTE OF HUMAN OBSOLESCENCE, supra note 58.

152. *See generally* Rajesh P.N. Rao et al., *A Direct Brain-to-Brain Interface in Humans*, PLOS ONE, Nov. 2014, http://journals.plos.org/plosone/article?id=10.1371/journal.pone.011133 [https://perma.cc/HQ68-UGPL].

153. Dvorsky, *supra* note 148 ("[F]or example, the brain of a sleepy airplane pilot dozing off at the controls could stimulate the copilot's brain to become more alert.").

154. George Dvorsky, *New Brain-Link Tech Means We Can Now Play 20 Questions with Our Minds*, GIZMODO (Sept. 25, 2015, 3:00 PM), https://io9.gizmodo.com/new-brain-link-tech-means-we-can-now-play-20-questions-1732991346 [https://perma.cc/BYY5-SS4F] ("The researchers are hopeful, for example, that a similar system could be used by people with Broca's aphasia.").

movies).[155] These uncomfortable questions of third-party processes controlling human bodies become even more pronounced in the context of second-generation IoB—IoB devices that are embedded inside the body.

2. Second-Generation IoB: Body Internal

Second-generation IoB technologies refer to those IoB devices where a portion of the device resides inside the body or accesses the body by breaking the skin.[156] For example, pacemakers have long included digital components,[157] and cochlear implants now include functionality reliant on Bluetooth.[158] Digital pills (already approved for the market by the FDA)[159] rely on a 3D-printed circuit and a transmitter inside a capsule.[160] Along similar lines, several companies[161] are currently racing to bring an IoB artificial "pancreas"[162]

---

155. *Invasion of the Body Snatchers*, IMBD, https://www.imdb.com/title/tt0049366/ [https://perma.cc/C73B-YH23].

156. *See* David Horrigan, *The Internet of Bodies: A Convenient—and, Yes, Creepy—New Platform for Data Discovery*, LEGALTECH NEWS (Jan. 7, 2019, 11:30 AM), https://www.law.com/legaltechnews/2019/01/07/the-internet-of-bodies-a-convenient-and-yes-creepy-new-platform-for-data-discovery [https://perma.cc/SF9Q-W8DF].

157. Lisa Vaas, *Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking*, NAKED SECURITY (Oct. 22, 2013), https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/ [https://perma.cc/R24R-UEKM].

158. *True Wireless™ Accessories*, COCHLEAR, http://www.cochlear.com/wps/wcm/connect/us/home/treatment-options-for-hearing-loss/wireless-accessories [https://perma.cc/4N2R-T6NK].

159. *FDA Approves Pill with Sensor that Digitally Tracks if Patients Have Ingested Their Medication*, U.S. FOOD & DRUG ADMIN. (Nov. 13, 2017), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm584933.htm [https://perma.cc/C92K-CJLR] ("Abilify MyCite (aripiprazole tablets with sensor) has an ingestible sensor embedded in the pill that records that the medication was taken.").

160. After the pill is ingested, it is powered by chlorine ions inside the stomach and relays information through the Internet with the help of a dongle and smartphone. Kelsey Atherton, *Take Two Robots by Mouth*, POLITICO (Dec. 13, 2017, 5:21 AM), https://www.politico.com/agenda/story/2017/12/13/five-drugs-for-the-future-000592 [https://perma.cc/T99W-R683].

161. *See, e.g.*, Stacy Lawrence, *Medtronic Artificial Pancreas May Hit the Market Next Spring, as Pivotal Trial Nears Final Data*, FIERCE BIOTECH (Apr. 7, 2016, 11:59 AM), https://www.fiercebiotech.com/medical-devices/medtronic-artificial-pancreas-may-hit-market-next-spring-as-pivotal-trial-nears [https://perma.cc/2TJD-8HRY]; *Admetsys to Exhibit Smart Pancreas™ at Massachusetts Institute of Technology (MIT) Enterprise Forum 2015 Startup Spotlight*, PR URGENT (June 15, 2015), http://prurgent.com/2015-06-15/pressrelease387382.htm [https://perma.cc/E7LR-FPAG] [hereinafter *Admetsys to Exhibit Smart Pancreas™*].

162. Paul Karoff, *Artificial Pancreas System Aimed at Type 1 Diabetes Mellitus*, HARV. GAZETTE (Jan. 4, 2016), http://news.harvard.edu/gazette/story/2016/01/artificial-pancreas-

to market—an implantable Internet-connected, sometimes 3D printed[163] "pancreas" managed by software and a mobile phone app.[164] Indeed, the FDA has already approved the first of these artificial pancreas devices.[165] Sensor-enabled sutures can now collect data on healing wounds,[166] and chips with cameras can report information from inside the heart during surgery.[167]

Prosthetics manufacturers have also embarked upon "smart" product[168] development, announcing that the next generation of

---

system-aimed-at-type-1-diabetes-mellitus/ [https://perma.cc/Z8ZH-29CA] ("The artificial pancreas is not a replica organ; it is an automated insulin delivery system designed to mimic a healthy person's glucose-regulating function."). Intended as a next generation insulin pump, these devices would engage in continuous monitoring of a patient's glucose levels, releasing insulin into the body when needed. *Admetsys to Exhibit Smart Pancreas™*, *supra* note 161.

163. 3D printing is also being used with prosthetic limbs. Ian Birrell, *3D-Printed Prosthetic Limbs: The Next Revolution in Medicine*, GUARDIAN (Feb. 19, 2017, 1:59 AM), https://www.theguardian.com/technology/2017/feb/19/3d-printed-prosthetic-limbs-revolution-in-medicine [https://perma.cc/VH7Q-BWPX]; Meghan Neal, *3D Bioprinters Could Make Enhanced, Electricity-Generating 'Superorgans*,*'* VICE: MOTHERBOARD (June 13, 2014, 2:15 PM), http://motherboard.vice.com/read/3d-bioprinters-could-make-enhanced-electricity-generating-superorgans [https://perma.cc/3SSC-B2RF]. Ultimately, patients may be able to print new prosthetics at home with advancements in 3D printing. Matt Reynolds, *Print Your Own Prosthetic: This Code Can Be Used by Anyone to Create Their Own Bionic Limbs*, WIRED (Nov. 5, 2016), http://www.wired.co.uk/article/samantha-payne-bionic-arm-builder [https://perma.cc/9JXL-E6NP].

164. Karoff, *supra* note 162 ("The closed-loop system consists of an insulin pump, a continuous glucose monitor placed under the user's skin, and advanced control algorithm software embedded in a smartphone that provides the engineering brains, signaling how much insulin the pump should deliver to the patient based on a range of variables, including meals consumed, physical activity, sleep, stress, and metabolism.").

165. *The Artificial Pancreas Device System*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/medicaldevices/productsandmedicalprocedures/homehealthandconsumer/consumerproducts/artificialpancreas/default.htm [https://perma.cc/A235-VJB6].

166. Patrick Collins, *Researchers Invent "Smart" Thread that Collects Diagnostic Data When Sutured into Tissue*, TUFTSNOW (July 18, 2016), http://now.tufts.edu/news-releases/researchers-invent-smart-thread-collects-diagnostic-data-when-sutured-tissue [https://perma.cc/9WXQ-T4L8].

167. Eric Butterman, *A Way to Your Heart?*, ASME (June 2016), https://www.asme.org/engineering-topics/articles/bioengineering/a-way-to-your-heart [https://perma.cc/H2XJ-J4E7]. Virtual reality rigs are also recording surgery for training purposes. Gian Volpicelli, *What's Next for VR Surgery?*, WIRED (Apr. 14, 2016), http://www.wired.co.uk/article/wired-health-virtual-reality-surgery-shafi-ahmed [https://perma.cc/P7LJ-6QH3].

168. For example, one such prosthesis uses "15 different sensors that are measuring different parameters with every step that the person is taking, and that data is being processed by three different onboard computers." Rob Hawley, *Wounded Veteran Among Those Benefiting from 'Smart' Prosthetic Ankle*, CBS N.Y. (Nov. 18, 2015, 2:54 PM), https://newyork.cbslocal.com/2015/11/18/bionx-biom-prosthetic-ankle/ [https://perma.cc/2FGK-F9EM].

prosthetics will be hardwired into patients' nerves[169] and muscles,[170] thereby merging flesh with computer code and hardware.[171] The Department of Veterans Affairs Center for Innovation has also launched programs aimed at creating a series of open-source "smart" prosthetics for wounded veterans.[172] Meanwhile, the Defense Advanced Research Projects Agency (DARPA) has been funding the development of next generation bionic arms,[173] and DARPA's Revolutionizing Prosthetics program successfully fitted a paralyzed woman with two nodes directly on her brain, allowing her to pilot a plane in a simulation.[174] Recent research[175] also demonstrated that with the help of an electrode array implanted in the brain, amputees will be able to move digits on a prosthesis with their thoughts alone, even without extensive training.[176] To wit, a monkey recently

169. DARPA (@DARPA), TWITTER (Oct. 27, 2016, 3:47 PM), https://twitter.com/DARPA/status/791773227190194182 [https://perma.cc/5L2D-HV7H] ("Video: Interface connecting prosthetic hand to nervous system helps amputees feel just how hard to squeeze.... #HAPTIX.").

170. *See* Andrea Powell, *AI Is Fueling Smarter Prosthetics Than Ever Before*, WIRED (Dec. 22, 2017, 12:13 PM), https://www.wired.com/story/ai-is-fueling-smarter-prosthetics-than-ever-before/ [https://perma.cc/9KBT-2B25].

171. *See* Hawley, *supra* note 168 ("Carignan says his company wants to tie sensors into the existing muscles and nerves of the patient so they could have more active control over how the ankle works.").

172. *VA to Launch Innovation Creation Series for Prosthetics and Assistive Technologies*, U.S. DEP'T VETERANS AFF. (May 15, 2015, 11:56 AM), https://www.blogs.va.gov/VAntage/19925/va-launches-innovation-creation-series-prosthetics-assistive-technologies/[https://perma.cc/N9AY-9YDA]. A generation of young amputees is also currently nudging innovation and optional enhancement in IoB technology. Maria Doyle, *Teachers Design Smart, Connected Prosthesis for Double Amputee*, LINKEDIN (Mar. 16, 2015), https://www.linkedin.com/pulse/teachers-design-smart-connected-prosthesis-double-amputee-maria-doyle?trk=portfolio_article-card_title [https://perma.cc/BU2E-32SH] ("Concepts include: Connecting with trail maps and conditions via the Internet [and] [t]racking performance.").

173. *See* B.J. Murphy, *DARPA Hands Off Bionic Luke Arm to Military Medical Center*, SERIOUS WONDER (Dec. 24, 2016), http://www.seriouswonder.com/darpa-hands-off-bionic-luke-arm-military-medical-center/ [https://perma.cc/YQL6-KLY6].

174. Abby Phillip, *A Paralyzed Woman Flew an F-35 Fighter Jet in a Simulator—Using Only Her Mind*, WASH. POST (Mar. 3, 2015), https://www.washingtonpost.com/news/speaking-of-science/wp/2015/03/03/a-paralyzed-woman-flew-a-f-35-fighter-jet-in-a-simulator-using-only-her-mind/ [https://perma.cc/2WPU-C3ZG]; *see also About Braingate*, BRAINGATE, https://www.braingate.org/about-braingate/ [https://perma.cc/7TSA-XCYS] (explaining that "micro-electrodes" implanted in the brain can be used to operate external devices).

175. Guy Hotson et al., *Individual Finger Control of a Modular Prosthetic Limb Using High-Density Electrocorticography in a Human Subject*, J. NEURAL ENGINEERING, Feb. 2016, at 10.

176. George Dvorsky, *Brain Implant Will Let Amputees Move Individual Fingers on*

controlled its wheelchair wirelessly using a brain implant and its thoughts,[177] part of research toward the development of brain-controlled robotic exoskeletons for humans.[178]

Indeed, the potential health outcomes from these second-generation IoB technologies may be life-altering for many patients. For example, a brain implant currently in trials is expected to demonstrate the ability to restore sight to the blind,[179] and a different brain implant has already helped a paralyzed man regain his sense of touch.[180] Similarly, recent innovations in brain bypass[181] technologies have allowed quadriplegics to operate their limbs with the assistance of brain-implanted microelectrodes, external machines, and a sleeve.[182] A locked-in sufferer of Lou Gehrig's disease has also successfully tested a brain implant of four sensor strips that wirelessly connected to a computer interface and allowed the patient to type out messages using her eyes and "brain clicks"[183]—the thought

---

Prosthetics with Thoughts Alone, GIZMODO (Feb. 16, 2016, 3:10 PM), https://gizmodo.com/brain-implant-lets-amputees-move-individual-fingers-on-1759445814 [https://perma.cc/WN69-JKW3].

177. Sankaranarayani Rajangam et al., *Wireless Cortical Brain-Machine Interface for Whole-Body Navigation in Primates*, SCI. REP., Mar. 2016, at 1, https://www.nature.com/articles/srep22170 [https://perma.cc/8LQW-WTR2].

178. *See* Loura Hall, *NASA's Ironman-Like Exoskeleton Could Give Astronauts, Paraplegics Improved Mobility and Strength*, NASA (Aug. 7, 2013), https://www.nasa.gov/offices/oct/home/feature_exoskeleton.html [https://perma.cc/J3UE-GRSV]; George Dvorsky, *This Monkey Is Controlling a Wheelchair With Its Mind*, GIZMODO (Mar. 3, 2016, 9:00 AM), https://gizmodo.com/this-robotic-wheelchair-is-being-controlled-by-a-monkey-1762391710 [https://perma.cc/8RZJ-B89C].

179. Dom Galeon, *A New Vision-Restoring Brain Implant Could Give Sight to the Blind*, FUTURISM (Feb. 13, 2017), https://futurism.com/4-theres-a-brain-implant-that-could-restore-vision-to-the-blind/ [https://perma.cc/NN4N-HEB2].

180. Jess Vilvestre, *A Paralyzed Man Just Regained the Sense of Touch, Thanks to a Brain Implant*, FUTURISM (Oct. 14, 2016), https://futurism.com/a-paralyzed-man-just-regained-the-sense-of-touch-thanks-to-a-brain-implant/ [https://perma.cc/W936-RYMA].

181. Neural bypass experiments are expected to yield significant results in the near future. *See, e.g.*, Beth Mole, *Using Synthetic Nervous System, Paralyzed Man Is First to Move Again*, ARS TECHNICA (Apr. 13, 2016, 4:40 PM), https://arstechnica.com/science/2016/04/with-synthetic-nervous-system-paralyzed-man-is-first-to-move-again/ [https://perma.cc/SK5E-258J]; Antonio Regalado, *Reversing Paralysis*, MIT TECH. REV. (Mar./Apr. 2017), https://www.technologyreview.com/s/603492/10-breakthrough-technologies-2017-reversing-paralysis/ [https://perma.cc/SH8R-3ZM7].

182. George Dvorsky, *Brain Implant Enables Quadriplegic Man to Play* Guitar Hero *with His Hands,* GIZMODO (Apr. 13, 2016, 1:00 PM), https://gizmodo.com/brain-implant-enables-quadriplegic-man-to-play-guitar-h-1770566874 [https://perma.cc/9438-VRWL].

183. Mariska J. Vansteensel et al., *Fully Implanted Brain-Computer Interface in a Locked-*

of "mov[ing] her hand for approximately 1 second."[184] Many promising second-generation IoB medical devices offer potentially transformational outcomes.

However, just as with first-generation IoB devices, while the earliest second-generation IoB devices have usually been classified as medical devices by the FDA,[185] later second-generation IoB may include devices whose manufacturers may consider them to be "healthy lifestyle" and nonmedical devices.[186] Indeed, the FDA considered most first-generation IoB devices to be nonmedical,[187] and the FDA has flagged that a number of relevant guidance documents may evolve in the future because of the 21st Century Cures Act of December 2016.[188] Meanwhile, technologically, the line between first-generation and second-generation IoB "healthy lifestyle"/nonmedical technology is already beginning to blur.

In Patient with ALS, 375 NEW ENG. J. MED. 2060, 2060-63 (2016).

184. *Id.* The machine activates whenever she thinks about moving her hand for about one second. *Id.*

185. For example, pacemakers fall into the most regulated category, Class III medical devices. Class III devices pose the greatest risk and, thus, are subject to a rigorous premarket approval (PMA) process. *See* Medtronic, Inc. v. Lohr, 518 U.S. 470, 476-77 (1996); 21 C.F.R. § 870.3680 (2012); 21 C.F.R. § 870.3710 (2011).

186. The FDA defines a device as follows:

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is: 1. recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them, 2. intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or 3. intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes. The term "device" does not include software functions excluded pursuant to section 520(o).

Is the Product a Medical Device?, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm [https://perma.cc/M7MA-5UMC].

187. GENERAL WELLNESS, *supra* note 96, at 2-5.

188. *Digital Health*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medicaldevices/digitalhealth/ [https://perma.cc/QR7Y-WTDZ]. The Cures Act was signed into law on December 13, 2016. *21st Century Cures Act*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/regulatoryinformation/lawsenforcedbyfda/significantamendmentstothefdcact/21stcenturycuresact/default.htm [https://perma.cc/2P68-6FWF].

For example, a team of researchers in Australia is currently working on ingestible electronic capsules that monitor gas levels in the human intestinal tract to track variability driven by food consumption.[189] Ingestible digital pills such as this one are likely to (attempt to) enter the market as a "healthy lifestyle" device.[190] While medical uses are foreseeable, the FDA may also analyze this digital pill as primarily monitoring the effects of selective food consumption in healthy bodies.[191] Therefore, much like a connected fitness tracker, this digital gas monitoring pill may fall outside the definition of a "medical device."[192] Consider also a swallowable "smart" vitamin absorption/sleep tracker that sends information about your body to your phone using Bluetooth, which then in turn uploads the information to the tracker company's cloud.[193] This IoB product would also potentially be deemed akin to a fitness tracker and, therefore, perhaps not necessarily classified as a medical device.[194] As a consequence, it too may fall within the "healthy lifestyle" device categorization and outside the definition of a medical device. But some second-generation IoB devices will fall squarely outside either of these health-related categories and reflect selective, aesthetic human self-augmentation.[195]

---

189. Beth Mole, *With Ingestible Pill, You Can Track Fart Development in Real Time on Your Phone*, ARS TECHNICA (Jan. 9, 2018, 7:30 AM), https://arstechnica.com/science/2018/01/with-ingestible-pill-you-can-track-fart-development-in-real-time-on-your-phone/ [https://perma.cc/54AP-A97D] (noting the digital pill is paired with a receiver and mobile phone in order to report gas production conditions inside the human body in real time).

190. *Id.*

191. *See id.*

192. *See* GENERAL WELLNESS, *supra* note 96, at 3, 6-7. The FDA also does not currently review vitamin "supplements" for safety and effectiveness before they are marketed, instead relying on manufacturers to verify their safety. *Dietary Supplements: What You Need to Know*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/food/dietarysupplements/usingdietarysupplements/ucm109760.htm [https://perma.cc/4RWC-RNDY].

193. *Cf.* Mole, *supra* note 189.

194. If the FDA chooses to take a similar hands-off approach, this device would fall primarily under the FTC's jurisdiction to police health claims. *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Issues Enforcement Policy Statement Regarding Marketing Claims for Over-the-Counter Homeopathic Drugs (Nov. 15, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-issues-enforcement-policy-statement-regarding-marketing [https://perma.cc/N6GQ-P3AT].

195. Also consider the Circadia, an implantable device that allows for wellness tracking of "biomedical data and transmit[s] it to the Internet via Bluetooth." Dom Benoscek, *NIFTIT Partners with Grindhouse Wetware*, NIFTIT BLOG (Dec. 3, 2013), niftit.com/niftit-grindhouse-wetware/ [https://perma.cc/KAY3-B3YM].

While occupational and recreational self-augmentation using second-generation IoB may seem the stuff of dystopian science fiction or merely the unusual hobby of (overly)enthusiastic computer scientists[196] and controversial artists,[197] this practice is, in reality, no longer limited to fiction and the social avant-garde.[198] Indeed, estimates contend that approximately 50,000 to 100,000 people in the United States[199] currently have microchips implanted in their bodies.[200] Employers are encouraging their employees to chip themselves for convenience,[201] repurposing technologies long used safely on animals.[202] Chips can be used to store contact information for emergencies or Bitcoin wallet addresses,[203] and chips can be custom programmed to, for example, place a phone call when tapped to a phone,[204] open or lock a door,[205] or buy a smoothie.[206]

One company already sells a do-it-yourself implant kit for a few hundred dollars[207] which allows for purchasers to modify their

196. *See infra* Part II.B.

197. *See* Stuart Jeffries, *Neil Harbisson: The World's First Cyborg Artist*, GUARDIAN (May 6, 2014, 2:59 AM), https://www.theguardian.com/artanddesign/2014/may/06/neil-harbisson-worlds-first-cyborg-artist [https://perma.cc/HM9B-99PZ].

198. *See* Trevor Callaghan (@trevolafoam), TWITTER (Sept. 17, 2016, 3:24 AM), https://twitter.com/trevolafoam/status/777090730472923136 [https://perma.cc/99PS-XMKD] ("Implant Party! #FutureFest16").

199. The practice is also gaining in popularity in other countries such as Australia. Emma Reynolds, *Australians Embracing Super-Human Microchip Technology*, NEWS.COM.AU (Aug. 25, 2016, 8:32 AM), http://www.news.com.au/technology/gadgets/wearables/australians-embracing-superhuman-microchip-technology/news-story/536a08003cb07cba23336f83278a5003 [https://perma.cc/QX8D-VAKM].

200. Yael Grauer, *A Practical Guide to Microchip Implants*, ARS TECHNICA (Jan. 3, 2018, 7:30 AM), https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/ [https://perma.cc/995P-PN84].

201. *See* Associated Press, *Companies Start Implanting Microchips into Workers' Bodies*, L.A. TIMES (Apr. 3, 2017, 10:15 AM), http://www.latimes.com/business/technology/la-fi-tn-microchip-employees-20170403-story.html [https://perma.cc/WY2B-59RQ].

202. *See Microchipping of Animals FAQ*, AM. VETERINARY MED. ASS'N, https://www.avma.org/KB/Resources/FAQs/Pages/Microchipping-of-animals-FAQ.aspx [https://perma.cc/NB6J-R3QB].

203. Cyrus Farivar, *Man Has NFC Chips Injected into His Hands to Store Cold Bitcoin Wallet*, ARS TECHNICA (Nov. 15, 2014, 11:00 AM), https://arstechnica.com/information-technology/2014/11/man-has-nfc-chips-injected-into-his-hands-to-store-cold-bitcoin-wallet/ [https://perma.cc/D49Q-ZCPN].

204. Grauer, *supra* note 200.

205. Farivar, *supra* note 203.

206. Associated Press, *supra* note 201.

207. CYBORGNEST, https://cyborgnest.net/ [https://perma.cc/3QP4-GKQC]. As of February

bodies[208] in various Internet-connected ways, such as vibrating whenever the wearer is facing north.[209] For example, one wearer uses an implant to inform her when a seismic movement occurs.[210] Another wearer—the first legally recognized "cyborg" per his U.K. passport—fused his implant to his brain to have it translate color into musical tones.[211] Informal "biohacking" communities and hackathons[212] are increasingly popular, and formalized conferences and workshops already exist.[213]

Also, as in every Internet context, marketing and "customer experience" data collection is pushing new technology adoption. Indeed, recent patent filings indicate this dynamic has already arrived to second-generation IoB.[214] For example, British Airways has filed a patent with the UK Intellectual Property Office seeking to patent a swallowable "ingestible sensor" to monitor customer experience on flights from the inside of customers' bodies.[215]

In particular, as the preceding examples illustrate, one of the business dynamics visible in the evolution of second-generation IoB technologies is the merger of first and second-generation medical IoB with other existing consumer technologies, creating new recreational (nonmedical) IoB.[216] For example, in medical contexts,

---

2017, around 1000 people had ordered a north-sensing kit. Adam Popescu, *This $425 DIY Implant Will Make You a Cyborg*, BLOOMBERG BUSINESSWEEK (Feb. 16, 2017, 10:30 AM), https://www.bloomberg.com/news/articles/2017-02-16/this-425-diy-implant-will-make-you-a-cyborg [https://perma.cc/R9XD-72AC].

208. Generally two small titanium barbells akin to a piercing are implanted in the wearer's chest. *Id.*

209. *Id.*

210. *Id.*

211. *Id.*

212. Nicole Kobie, *How to Hack Your Senses: From 'Seeing' Sound to 'Hair GPS*,*'* WIRED (July 5, 2016), http://www.wired.co.uk/article/how-to-hack-senses-see-sound [https://perma.cc/H3NF-R9ML].

213. *See, e.g.*, *Biohackers at DEFCON*, DEFCON BIOHACKING VILLAGE, https://www.defconbiohackingvillage.org/ [https://perma.cc/7FHW-RVEN]. A particularly engaged community exists in Brooklyn. *See Brooklyn Biohackers*, MEETUP, https://www.meetup.com/Brooklyn-Biohackers/?_cookie-check=4rhghGnRdc7nBd3x [https://perma.cc/S69D-24CK].

214. Eleazer Corpuz, *British Airways Plans to Monitor Its Passengers with a 'Digital Pill*,*'* FUTURISM (Nov. 30, 2016), https://futurism.com/british-airways-plans-to-monitor-its-passengers-with-a-digital-pill/ [https://perma.cc/98SM-ZPKT].

215. U.K. Patent Application No. 1600548.0, 2 1.34, Publication No. 2538339 (filed Mar. 24, 2014) (published Nov. 16, 2016) (British Airways PLC, applicant) (noting the sensor would communicate from the inside of the passenger's body).

216. *See id.*

ocular lens implants have long been used as a surgical correction for eyes damaged by cataracts.[217] Meanwhile, in recreational contexts, first-generation IoB gaming and other augmented reality devices initially involved glasses[218] and other headgear,[219] but then they started to include wearable IoB contact lenses.[220] Blending these two technology trends—one from medicine and one from consumer and enterprise technology—it perhaps should be unsurprising that augmented reality and other recreational visual products are now creeping inside the eyeball in injected form.[221] In other words, while these lenses were first used for medical reasons,[222] they are now also used for recreational[223] and military[224] purposes. It is

217. Millions of people receive ocular lens implants yearly as part of cataract surgeries. *See* Richard Lindstrom, *Thoughts on Cataract Surgery: 2015*, REV. OPHTHALMOLOGY (Mar. 9, 2015), https://www.reviewofophthalmology.com/article/thoughts-on--cataract-surgery-2015 [https://perma.cc/CDG2-YHQR].

218. *See* Dieter Bohn, *Intel Made Smart Glasses that Look Normal*, VERGE (Feb. 5, 2018, 8:00 AM), https://www.theverge.com/2018/2/5/16966530/intel-vaunt-smartglasses-announced-ar-video [https://perma.cc/9WK7-27Z8]; Jacob Kleinman, *Augmented Reality Glasses: What You Can Buy Now (or Soon)*, TOM'S GUIDE (Feb. 14, 2018, 8:00 AM), https://www.tomsguide.com/US/BEST-AR-GLASSES,REVIEW-2804.HTML [https://perma.cc/AA9D-RQVH].

219. *See* Lucas Matney, *RealWear Raises $17M as It Looks to Take a Simpler Approach to Enterprise AR Headgear*, TECHCRUNCH (Feb. 14, 2018), https://techcrunch.com/2018/02/14/realwear-raises-17m-as-itlooks-to-take-a-simpler-approach-to-enterprise-ar-headgear/ [https://perma.cc/J3UK-EVAE].

220. *See* Nick Statt, *Augmented-Reality Contact Lenses to Be Human-Ready at CES*, CNET (Jan. 3, 2014, 4:00 AM), https://www.cnet.com/news/augmented-reality-contact-lenses-to-be human-ready-at-ces/ [https://perma.cc/TQM9-TUH5].

221. For example, Google has patented an injectable implant that corrects and enhances vision and comes with an antenna for connecting to the Internet and recharging using special glasses. *See* Anthony Cuthbertson, *Google Patents a Cyborg Lens that Injects into Your Eyeball*, NEWSWEEK (May 5, 2016, 5:14 AM), http://www.newsweek.com/google-patent-cyborg-smart-lens-injecteyeballs-455824 [https://perma.cc/7CMY-3SL5].

222. *See* Alexandra Sifferlin, *Google Granted Patent for Smart Contact Lens*, TIME (Mar. 25, 2015), http://time.com/3758763/google-smart-contact-lens/ [https://perma.cc/2LY9-H866].

223. Sony has filed a patent on new contact lenses that can record video. *See* Clemence Michallon, *Sony Files to Patent New Contact Lenses that Can Record Video, Store It, Play It Back—and Adjust Zoom, Focus and Aperture Automatically*, DAILYMAIL (Apr. 30, 2016, 5:27 PM), http://www.dailymail.co.uk/sciencetech/article-3567402/Sony-patent-application-reveals-new-contact-lensesrecord-video-store-play-adjust-zoom-focus-apertureautomatically.html#ixzz48ngMvB00 [https://perma.cc/7GM3-5CHY].

224. Implanted augmented reality contact lenses might be useful in the creation of a generation of "super soldiers" according to some proponents of the technology. *See* Sarah Buhr, *Omega Opthalmics Is an Eye Implant Platform with the Power of Continuous AR*, TECHCRUNCH (Aug. 4, 2017), https://techcrunch.com/2017/08/04/ophthalmics-is-an-eye-implantwith-the-power-of-continuous-ar/ [https://perma.cc/4NPM-7CYJ].

this progressive creep that will also transform current brain prosthetics into the third generation of IoB—where body and mind meld with the Internet and remote computing, not only for medical purposes but also as a chosen aesthetic enhancement.

3. Third-Generation IoB: Body Melded

Third-generation IoB devices meld the human mind with external computers and the Internet.[225] As currently conceptualized, these devices primarily involve injected or implanted brain computer interfaces that act in a bidirectional read/write manner.[226] In other words, they functionally extend and externalize portions of the human mind.[227] Thus, one of the goals of third-generation IoB is the (optional) cognitive enhancement[228] of healthy, able-bodied humans with the help of brain-implanted computers and linkages.[229] As described by Elon Musk,[230] the founder of a company researching ways to connect computers directly to brains,[231] the goal is a "merger of biological intelligence and machine intelligence."[232] Entrepreneurs

225. *See* Olivia Solon, *Elon Musk Says Humans Must Become Cyborgs to Stay Relevant. Is He Right?*, GUARDIAN (Feb. 15, 2017, 3:00 AM), https://www.theguardian.com/technology/2017/feb/15/elon-musk-cyborgs-robots-artificial-intelligence-is-he-right [https://perma.cc/SA8J-H8MG].

226. *See id.*

227. *See* Sarah Marsh, *Neurotechnology, Elon Musk and the Goal of Human Enhancement*, GUARDIAN (Jan. 1, 2018, 4:00 AM), https://www.theguardian.com/technology/2018/jan/01/elon-musk-neurotechnology-human-enhancement-brain-computer-interfaces [https://perma.cc/ZV6T-PF9C].

228. The fear of AI takeover fuels discussion of enhanced brain capacity. *See* Christof Koch, *To Keep Up with AI, We'll Need High-Tech Brains*, WALL ST. J. (Oct. 27, 2017), https://www.wsj.com/articles/to-keep-up-with-ai-well-need-high-tech-brains-1509120930?mod=e2twd [https://perma.cc/647S-2LVN].

229. *See* Nick Statt, *Kernel Is Trying to Hack the Human Brain—But Neuroscience Has a Long Way to Go*, VERGE (Feb. 22, 2017, 12:36 PM), https://www.theverge.com/2017/2/22/14631122/kernel-neuroscience-bryan-johnson-human-intelligence-ai-startup [https://perma.cc/7DFC-PS2A].

230. *See* Kristin Houser, *Here's Everything You Need to Know About Elon Musk's Human/AI Brain Merge,* FUTURISM (Apr. 20, 2017), https://futurism.com/heres-everything-you-need-to-know-about-elon-musks-humanai-brain-merge/ [https://perma.cc/8PMV-9LA6].

231. Musk has voiced his concern that humans will be overtaken by artificial intelligence and turned into the metaphorical equivalent of a "house cat[ ]." Solon, *supra* note 225; *see also* Sebastian Anthony, *Humans Must Become Cyborgs to Survive, Says Elon Musk*, ARS TECHNICA (Feb. 14, 2017, 8:50 AM), https://arstechnica.com/information-technology/2017/02/humans-must-become-cyborgs-to-survive-says-elon-musk/ [https://perma.cc/FU8D-9YN2].

232. Solon, *supra* note 225.

building these third-generation IoB devices sometimes call them a "direct cortical interface,"[233] and they predict a coming "gold rush" in optional brain enhancement.[234] Indeed, some financial analysts forecast a $27 billion market for these devices by 2023.[235] Third-generation IoB devices are often not framed as a medical correction of a preexisting physical state.[236]

Despite Musk's recent assertions that third-generation IoB human testing will start in 2020,[237] perhaps reassuringly, current third-generation IoB devices are generally believed to be in relatively early stages of development.[238] While the goal of third-generation IoB includes brain enhancement and uploadable knowledge,[239] their current uses are, in fact, primarily in the context of treating medical conditions.[240] For example, brain prosthetic devices[241] with wireless components are currently being tested and prescribed for humans with Alzheimer's, Parkinson's, epilepsy, and other conditions.[242]

---

233. *See* Cade Metz, *Elon Musk Isn't the Only One Trying to Computerize Your Brain*, WIRED (Mar. 31, 2017, 7:00 AM), https://www.wired.com/2017/03/elon-musks-neural-lace-really-look-like/?mbid=social_twitter [https://perma.cc/V87V-YLEM].

234. *See* John H. Richardson, *Inside the Race to Hack the Human Brain*, WIRED (Nov. 16, 2017, 6:00 AM), https://www.wired.com/story/inside-the-race-to-build-a-brain-machine-interface/ [https://perma.cc/MHC7-P6XN].

235. *Id.*

236. *See id.*

237. Stephen Shankland, *Elon Musk Says Neuralink Plans 2020 Human Test of Brain-Computer Interface*, CNET (July 17, 2019), https://www.cnet.com/news/elon-musk-neuralink-works-monkeys-human-test-brain-computer-interface-in-2020/ [https://perma.cc/3DJT-SZH8].

238. *See* Christopher Mims, *A Hardware Update for the Human Brain*, WALL ST. J. (June 5, 2017), https://www.wsj.com/articles/a-hardware-update-for-the-human-brain-1496660400 [https://perma.cc/L2F3-34CC].

239. *See* Mark Molloy, *Scientists Discover How to 'Upload Knowledge to Your Brain,'* TELEGRAPH (Mar. 1, 2016, 7:45 PM), http://www.telegraph.co.uk/technology/2016/03/01/scientists-discover-how-to-download-knowledge-to-your-brain/ [https://perma.cc/7MLG-QPVU].

240. *See* Ian Sample, *Paraplegic Man Walks with Own Legs Again*, GUARDIAN (Sept. 23, 2015, 8:00 PM), https://www.theguardian.com/science/2015/sep/24/paraplegic-man-walks-with-own-legs-again [https://perma.cc/PRA4-WKK6].

241. *See* Jens Clausen et al., *Help, Hope, and Hype: Ethical Dimensions of Neuroprosthetics*, 356 SCI. 6345, 1338 (2017). Deep brain stimulation devices, by contrast, have generally not included external facing components but for doctor interfaces in proximity, presumably. *See* Tim Urban, *Neuralink and the Brain's Magical Future*, WAIT BUT WHY (Apr. 20, 2017), https://waitbutwhy.com/2017/04/neuralink.html [https://perma.cc/8PPA-QJGF].

242. *See* Robert Perkins, *Brain Prosthesis Aims to Provide Breakthrough for People Struggling with Memory Loss*, USC NEWS (Sept. 29, 2015), https://news.usc.edu/86658/new-device-aims-to-help-people-struggling-with-memory-loss/ [https://perma.cc/YH9G-GCJJ]. For example, memory prostheses have successfully replaced the Alzheimer's-damaged parts of a

Another possible medical application entails helping soldiers recover from postwar memory loss[243] and traumatic experiences.[244] But slippage into nonmedical uses of third-generation IoB is already visible. For example, third-generation IoB research also assists in the creation of cognitively enhanced super-soldiers as part of the U.S. Armed Forces.[245] As explained by DARPA Director Arati Prabhakar, "we can now see the future where we can free the brain from the limitations of the human body.... We can only imagine amazing good things and amazing potentially bad things that are on the other side of that door."[246]

Although we have not yet evolved an infrastructure and other technical capabilities[247] that can successfully support the "brain-cloud"[248] ideal of third-generation IoB, some experts estimate the arrival of third-generation IoB technology to be as little as a decade away.[249] A decade may seem a long time to technologists, but in terms of legal evolution, this time frame signals a need for expedited debate and legal preparation.[250]

While the potentially life-changing medical and lifestyle impact of a portion of these technologies is unquestionable, it is also the case that people will inevitably be hurt (and killed) by some of these

---

patient's hippocampus. *See* Eileen Toh, *USC Researchers Develop Brain Implant to Improve Memory*, DAILY TROJAN (Nov. 19, 2017), https://dailytrojan.com/2017/11/19/usc-researchers-develop-brain-implant-improve-memory/ [https://perma.cc/6LJ9-4ZW2].

243. *See* Perkins, *supra* note 242.

244. *See* Matt Burgess, *Scientists Use AI to 'Rewrite' Painful Memories in People's Brains*, WIRED (Nov. 21, 2016), http://www.wired.co.uk/article/brain-fear-decode-erase [https://perma.cc/5CDQ-PWE8].

245. The creation of super-soldiers is the alleged goal of a research program underway through DARPA. *See* Karla Lant, *DARPA Is Planning to Hack the Human Brain to Let Us "Upload" Skills*, FUTURISM (May 2, 2017), https://futurism.com/darpa-is-planning-to-hack-the-human-brain-to-let-us-upload-skills/ [https://perma.cc/4ZXS-XQEK].

246. Phillip, *supra* note 174.

247. *See* Houser, *supra* note 230 ("The company has to deal with the problems of biocompatibility, wirelessness, power, and ... bandwidth.").

248. For a discussion of the cloud, see generally Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 158 (2012) (discussing the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Judiciary House of Representative's ECPA Reform and the Revolution in Cloud Based Computing Hearing).

249. *See* Houser, *supra* note 230.

250. *See id.* ("The engineering is only half the battle, though. Like Musk mentioned, regulatory approval will be a big factor in the development and adoption of Neuralink's tech.").

IoB technologies.[251] Consequently, impacted plaintiffs will seek recourse through the courts.[252] In order to begin to craft a coherent and innovation-sensitive legal approach to address these IoB harms, let us first examine four lessons from our experiences with IoT.

B. The "Legacy Code" of IoT

Agent Smith: Never send a human to do a machine's job.[253]

As one Silicon Valley startup explains, the human body is "the next big innovation platform."[254] While this statement is accurate in heralding the arrival of IoB, it should also serve as a harbinger of looming harms and legal challenges. Because technology past is generally technology prologue, to anticipate the legal future of IoB, we can turn to an examination of the present state of IoT. Instructively, a series of serious IoT implementation problems have arisen as IoT has gained popularity. Parallel problems are already arising or are likely to arise in IoB.

Four of these IoT implementation problems include the "Better with Bacon" problem of gratuitous Internet connectivity,[255] the "Magic Gadget" problem of failing to plan for failure,[256] the "Builder Bias" problem of shipping without securing,[257] and the "Mandatory Soup" problem of limited self-help, diminished market choice, and obsolescence through adhesion.[258] However, when these four problems manifest in IoB contexts, they will present one critical difference from their IoT incarnation: human bodies may be directly physically harmed.[259]

---

251. *See* Urban, *supra* note 241.
252. *See infra* Part I.C.2.
253. THE MATRIX, *supra* note 2.
254. *Nootrobox Is Hiring an Editor-in-Chief*, STARTUP.JOBS, https://startup.jobs/editor-in-chief-at-nootrobox [https://perma.cc/Q2Y6-P8FD].
255. *See infra* Part I.B.1.
256. *See infra* Part I.B.2.
257. *See infra* Part I.B.3.
258. *See infra* Part I.B.4.
259. *See* Urban, *supra* note 241.

1. The Better with Bacon Problem: Gratuitous Internet Connectivity

An April Fools' Day joke from 2013 touted the launch of the Toaster.io—a toaster connected to the Internet.[260] At the time, the idea of a toaster being connected to the Internet seemed ridiculous to an average consumer.[261] In hindsight, of course, the Internet of Things exploded shortly thereafter, and Toaster.io was merely a preview of actual products soon to arrive on the market.[262]

The seemingly unrelenting "cybering" of all the consumer things[263] that occurred in the IoT marketplace calls to mind an admonition from Professor Siva Vaidhyanathan. Professor Vaidhyanathan has argued that perfunctory innovation may be supplanting the idea of progress, stating that "[p]rogress is out-of-fashion."[264] He argued that "innovation differs from progress in many ways. Innovation lacks a normative claim of significant betterment. It emerges from many small moves ... [and] does not contain an implication of a grand path or a grand design of a knowable future."[265] Indeed, our model of "innovation" often appears to involve relentlessly connecting consumer products to the Internet, even when a product's functionality is not necessarily materially enhanced by the Internet connectivity.[266]

This argument lies at the heart of what might be called the "Better with Bacon" problem.[267] Just as some restaurants seem to

260. See Zack Whittaker, *The World's First Social Toaster*?, ZDNET (Apr. 1, 2013), https://www.zdnet.com/pictures/april-fools-2013-the-best-techy-pranks-of-the-day/3/ [https://perma.cc/SH33-RKB2].

261. *See id.*

262. *See* Roberto Baldwin, *The World Now Has a Smart Toaster*, ENGADGET (Jan. 4, 2017), https://www.engadget.com/2017/01/04/griffin-connects-your-toast-to-your-phone/ [https://perma.cc/598J-X9G4].

263. *See* Elizabeth Nolan Brown, *Meme Origins: "All the Things" Tic Spawned by Artist Allie Brosh*, BUSTLE (Aug. 30, 2013), https://www.bustle.com/articles/4393-meme-origins-all-the-things-tic-spawned-by-artist-allie-brosh [https://perma.cc/K8T7-P5X6].

264. Siva Vaidhyanathan, *The Golden Quarter*, AEON (May 13, 2015), https://aeon.co/users/siva-vaidhyanathan [https://perma.cc/6D39-HNB3].

265. *Id.*

266. For example, one might ask whether Internet connectivity meaningfully enhances the experience of a saw. Yet, saws are available in IoT form. *See Rotozip*, THE HOME DEPOT, https://www.homedepot.com/p/Rotozip-5-5-Amp-Corded-1-4-in-Rotary-RotoSaw-Spiral-Saw-Tool-Kit-with-5-Accessories-SS355-10/203408190 [https://perma.cc/873E-EWUB].

267. One common technology variant of the Better with Bacon problem might be the

erroneously believe that all meals are "better" with an ample sprinkling of (sometimes unexpected) bacon,[268] so too some technology producers and users believe that every gadget is "better" with gratuitous, even if functionally nonessential, Internet capabilities.[269] While for some diners surprise bacon presents an unexpected benefit, for vegetarian diners, surprise bacon may effectively undermine the entirety of the enterprise. And, just as surprise bacon bits are never calorie-free (and sometimes unwelcome), gratuitous technology "bacon" is also never costless. It always comes at the expense of security.

While an Internet-connected toaster that, for example, emblazons the morning weather onto toast[270] might seem like a harmless curiosity for a kitchen or corporate break room, its Internet connectivity adds attack surface and material risk for the security of a network as a whole.[271] For example, a vulnerability in an IoT toaster may be an entree for compromising a company's or a consumer's otherwise protected network.[272] Particularly in sensitive situations with national security or infrastructural implications, the IoT

---

addition of Bluetooth devices. Bluetooth has been amply demonstrated to create additional vulnerabilities in systems. Chris Merriman, *BlueBorne: Bluetooth Hack Doesn't Require Pairing with Victims Devices,* INQUIRER (Sept. 13, 2017), https://www.theinquirer.net/inquirer/news/3017247/new-bluetooth-hack-doesnt-require-pairing-with-victims-device [https://perma.cc/AE75-73QV].

268. *See, e.g.*, Mr. B, *Top 10 Most Popular Gifts for Serious Bacon Lovers!*, BACON TODAY (2015), https://bacontoday.com/top-10-most-popular-gifts-for-serious-bacon-lovers/ [https://perma.cc/X6L2-H3XC]. Bacon is a culinarily pleasing food for some diners. However, it does not carry equal utility in all implementation environments. Todd Van Luling & Renee Jacques, *The 17 Dumbest Things Vegetarians Have to Deal with,* HUFFPOST (Dec. 4, 2017, 9:59 AM), https://www.huffingtonpost.com/entry/vegetarians-dumbest-things_n_4177147.html [https://perma.cc/QMP6-B924].

269. An example of the phenomenon is the idea that all devices are better with Bluetooth. *But see* Merriman, *supra* note 267 (stating Bluetooth is a notoriously vulnerable technology).

270. *See* Abigail Williams, *This High-Tech Toaster Prints the Weather Report on Bread,* HUFFPOST (Aug. 16, 2016, 9:44 AM), https://www.huffingtonpost.com/entry/toaster-weather-forecast-toasteroid_n_57b30217e4b0a8e1502526a4 [https://perma.cc/VJ6E-FNGJ].

271. *See* Andrea M. Matwyshyn, *The Big Security Mistakes Companies Make When Buying Tech,* WALL ST. J. (Mar. 13, 2017), https://www.wsj.com/articles/the-big-security-mistakes-companies-make-when-buying-tech-1489372011 [https://perma.cc/U3HG-J6BP].

272. Indeed, Internet-connected ovens have already been known to suffer serious security vulnerabilities in their code. *See Security Flaw Could Have Let Hackers Turn on Smart Ovens*, PHYS.ORG (Oct. 26, 2017), https://phys.org/news/2017-10-flaw-hackers-smart-ovens.html [https://perma.cc/US9H-BHST].

whimsy-to-unreasonable security risk ratio should swiftly tilt the calculus in favor of choosing the non-IoT device.[273]

Again, IoT history offers a warning: in 2013, the technology press and the security research community accurately predicted that ransomware[274] would soon lock up computers at scale and that botnets would use IoT devices in denial of service attacks. Three years later, in 2016, a botnet of IoT devices committed a successful distributed denial of service attack against Twitter and Reddit, and entire hospital networks were crippled due to ransomware.[275] Today, security professionals are already warning that gratuitously connecting human bodies to the Internet will end even more poorly[276]—with botnets of bodyparts and human bodies immobilized by ransomware.[277] Yet, despite these credible and somber warnings, our overenthusiasm and magical thinking leads us to often gratuitously and unwisely connect devices to the Internet without fully considering the additional security risk. This blind overenthusiasm also begets our next problem—the "Magic Gadget" problem.

2. The Magic Gadget Problem: Failing to Anticipate Failure

In his book *Pinpoint*, author Greg Milner describes how, since the launch of the GPS system in 1980, humans have slid into overreliance and magical thinking about the trustworthiness of the

273. *See* Robert Cottrell, *Why You Should Be Afraid of a Smart Toaster*, BBC FUTURE (Feb. 16, 2015), http://www.bbc.com/future/story/20150216-be-afraid-of-the-smart-toaster [https://perma.cc/G7VE-N5WG].

274. *See* J.M. Porup, *Ransomware Is Coming to Medical Devices,* VICE MOTHERBOARD (Nov. 19, 2015, 6:00 AM), https://motherboard.vice.com/en_us/article/jpgxxk/ransomware-is-coming-to-medical-devices [https://perma.cc/7C4W-J3QN].

275. *See infra* notes 288-90, 297, 321-23 and accompanying text.

276. One security professional has warned of the same possibility with IoB heart defibrillators. Chris Wysopal (@WeldPond), TWITTER (Oct. 24, 2016, 11:56 PM), https://twitter.com/WeldPond/status/790809257448972288 [https://perma.cc/C5UN-LMHN] ("What's next in 2017? Heart defibrillators joining in IoT DDoS attacks?").

277. For example, one security professional warned of IoB breast pumps being compromised and used as part of a denial of service attack. *See* Alfredo Ortega (@ortegaalfredo), TWITTER (Jan. 5, 2017, 9:34 AM), https://twitter.com/ortegaalfredo/status/817031461878562816 [https://perma.cc/B6Y5-Y5SU] ("Botnets will get really weird this year."); *see also* Jeremiah Grossman (@jeremiahg), TWITTER (Oct. 19, 2016, 6:54 AM), https://twitter.com/jeremiahg/status/788739996739969024 [https://perma.cc/2XMC-8CJB] ("[B]ody implants are likely to be in our [near] future, so technically we're personally going to be IoT devices.").

technology.[278] While GPS has generally eased the struggles of mapping, in some cases, it has contributed to the untimely demise of its users—what he terms "death by GPS."[279] As users blindly trust the "magic" gadget in their hand, they sometimes disregard other superior sources of evidence in physical space,[280] even despite ample evidence that GPS can fail[281] or be manipulated by attackers.[282] This type of overly optimistic IoT thinking might be termed the "Magic Gadget" problem.

Turning to IoB, the adventures of Professor Mann offer a cautionary tale. Professor Steve Mann has experimented with IoB technology through an auto-recording augmented reality "glass eye" technology[283] that is permanently attached to his head.[284] In 2012, Mann's IoB device was implicated in a physical altercation in a Paris restaurant.[285] Allegedly, the restaurant employees decided to aggressively enforce a "no camera" policy and attempted to remove Professor Mann's glass eye by force from his head.[286] This unexpected physical disruption to Mann's IoB device allegedly rendered it inoperable, partially due to a secondary, moisture-related,

278. *See* GREG MILNER, PINPOINT: HOW GPS IS CHANGING TECHNOLOGY, CULTURE, AND OUR MINDS 112-15 (2016).

279. *Id.*

280. *See id.*

281. Kristen Lee, *These Are Your Worst GPS-Fail Stories*, JALOPNIK (Sept. 12, 2017, 10:55 AM), https://jalopnik.com/these-are-your-worst-gps-fail-stories-1803140713 [https://perma.cc/987G-MXEB].

282. Elias Groll, *Russia Is Tricking GPS to Protect Putin*, FOREIGN POL'Y (Apr. 3, 2019, 5:19 PM), https://foreignpolicy.com/2019/04/03/russia-is-tricking-gps-to-protect-putin/ [https://perma.cc/V5SC-KCMW].

283. *See EyeTap: The Eye Itself as Display and Camera*, EYETAP.ORG, http://www.eyetap.org/research/eyetap.html [https://perma.cc/W3NR-THAK]. This IoB device is used by Mann partially to improve his night vision using lasers. *See* Jake Edmiston, *No Shirt, No Shoes, No Cyborgs: Toronto Prof Says He Was Roughed up at Paris McDonald's Over No-Camera Policy*, NAT'L POST (July 19, 2012, 1:23 AM), http://news.nationalpost.com/news/canada/no-shirt-no-shoes-no-cyborgs-toronto-prof-says-he-was-roughed-up-at-paris-mcdonalds [https://perma.cc/SL5F-XEV6].

284. *See* Edminston, *supra* note 283.

285. *See* Katie Daubs, *Toronto 'Cyborg' Steve Mann Says He Was Assaulted in Paris McDonald's*, STAR (July 18, 2012), https://www.thestar.com/news/gta/2012/07/18/toronto_cyborg_steve_mann_says_he_was_assaulted_in_paris_mcdonalds.html [https://perma.cc/5YD7-65WC] (noting that before the incident, another employee had accepted Mann as a customer, sold him food, and reviewed his doctor's note).

286. *See* Edmiston, *supra* note 283.

hardware malfunction.[287] Professor Mann's experience offers us a reminder that catastrophic IoB failures will often happen unexpectedly and that they are not always within our control.

Yet, technology over-trust and the Magic Gadget problem often cause a failure to plan for even catastrophic failures. Indeed, a harbinger of these looming Magic Gadget problems in IoB might be found in the March 2016 ransomware attack that crippled the network of a Maryland hospital chain, impairing the patient care in 10 hospitals and 250 clinics.[288] With apparently no adequately robust crisis management system in place, employees described the attack as creating a "chaotic environment" and a "patient safety issue" that was potentially avoidable.[289] The hospitals had allegedly failed to patch vulnerabilities (that were well-known in the security community since 2007) despite direct prior warnings and the existence of techniques exploiting those unpatched vulnerabilities.[290] The Wannacry ransomware attack similarly paralyzed thousands of the U.K.'s National Health Service administrative computers,[291] potentially contributing to physical harm of patients who were waiting on emergency surgeries and consultations.[292]

But now consider a version of these ransomware scenarios in which the targeted devices are patients' IoB artificial pancreases

---

287. *Id.* ("Like I said, I had to go to the washroom.... But when he pushed me out the door, at some point my pants became a toilet.... Some of the critical items were affected (by water damage).").

288. *See* John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html [https://perma.cc/E7P2-6JEU].

289. *Id.*

290. *See* Sean Gallagher, *Maryland Hospital: Ransomware Success Wasn't IT Department's Fault*, ARS TECHNICA (Apr. 7, 2016, 10:12 AM), https://arstechnica.com/information-technology/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomware-attack/ [https://perma.cc/5643-HNA9].

291. For a discussion of Wannacry, see Josh Fruhlinger, *What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?*, CSO (Aug. 30, 2018, 6:52 AM), https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html [https://perma.cc/3U8S-96D5].

292. *See* Owen Hughes, *WannaCry Impact on NHS Considerably Larger than Previously Suggested*, DIGITALHEALTH (Oct. 27, 2017), https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/ [https://perma.cc/6Y8A-7A8Q] ("NHS England put the total number of cancelled appointments at some 19,494, which includes at least 139 patients who had 'an urgent referral for potential cancer cancelled.'").

instead of computer systems. Particularly, when we combine the Better with Bacon problem and the Magic Gadget problem with our next problem, the problem of Builder Bias, physical harm to IoB users becomes unfortunately entirely predictable and likely.[293]

3. The Builder Bias Problem: Shipping Without Securing

Consider the scenario in which a manufacturer with lax code-security practices has released a vulnerable IoB pancreas. The device's rampant security vulnerabilities allow for a remote attacker to disable it, demanding a "ransom" payment to turn it back on. Or imagine a botnet comprised of injected IoB eye lenses that cannot be easily removed. How would an average consumer respond when he learns that his eyeballs might be implicated in a distributed denial of service attack on a critical infrastructure target?

As a wisely programmed computer once announced in the movie *War Games*, "[t]he only winning [strategy] is not to play."[294] The only viable answer to these IoB security failure scenarios lies in avoiding the problem from the outset—devices must be as secure as possible at the point of shipping. Yet, the lessons of IoT caution us that many builders of IoB will fail to build in line with what the FTC calls security by design.[295] As builders rush to ship code to market, they often fail to prioritize the security and consumer safety of their code.[296] IoT product manufacturers, in particular, have sometimes perceived themselves to have little financial incentive to prioritize security or to disclose and correct flaws,[297] and security errors in their products have frequently gone undetected.[298] For example, IoT

293. Early adopter consumers seeking out "magic gadgets" may pay a heavier than anticipated price. *See* Charles Fain Lehman, *Experts Say Medical Care Next Big Threat,* FREEBEACON (Sept. 24, 2017, 5:00 AM), http://freebeacon.com/issues/experts-say-medical-care-next-big-cyber-threat/ [https://perma.cc/28RN-AQVP].

294. *See WarGames (War Games) Quotes*, ROTTENTOMATOES, https://www.rottentomatoes.com/m/wargames/quotes/ [https://perma.cc/Y8S3-MMC2].

295. START WITH SECURITY: A GUIDE FOR BUSINESS, U.S. FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business [https://perma.cc/6277-TPX3].

296. *See, e.g.*, Mike Lloyd, *The Internet of Things that Can Attack You,* FORBES (Feb. 17, 2017, 9:00 AM), https://www.forbes.com/sites/ciocentral/2017/02/17/the-internet-of-things-that-can-attack-you/171zb2dfedda [https://perma.cc/83W6-AX8R].

297. *See id.*

298. *See id.*

products are not always built to be updateable,[299] and attempts to report flaws by third parties sometimes result in receiving legal threats instead of thanks.[300] This failure of manufacturers to consider the implementation realities of security for fear it might delay shipping might be termed the problem of "Builder Bias."

Historically, IoB devices—just like IoT devices—have also been notoriously vulnerable to attacks by third parties due to imprudent security design choices such as hardcoded passwords.[301] In other words, the Builder Bias problem is already visible in IoB. For example, in 2012 when an episode of the television drama series Homeland included a plot twist where the sitting Vice President was murdered by a terrorist through a remote computer intrusion into his pacemaker,[302] the possibility of such a compromise was already well-recognized within the security research community.[303] In other words, the knowledge that IoB pacemakers could be remotely compromised by attackers existed years before the recent FDA IoB security recall.[304] Yet, despite this widespread knowledge, the medical device company that manufactured the pacemaker subject to the FDA security recall initially chose to deny the existence of a problem and to sue the security researcher who

299. *See* Jason Perlow, *All Your IoT Devices Are Doomed*, ZDNET (July 12, 2016), https://www.zdnet.com/article/all-your-iot-devices-are-doomed/ [https://perma.cc/TDT7-2WUL].

300. Zack Whittaker, *Lawsuits Threaten Infosec Research—Just When We Need It Most*, ZDNET (Feb. 19, 2018, 1:00 PM), https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/ [https://perma.cc/B2B8-CNN7].

301. NCCIC, MEDICAL DEVICES HARD-CODED PASSWORDS, U.S DEP'T HOMELAND SEC. (Oct. 29, 2013), https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01 [https://perma.cc/BH42-MA77].

302. Barbara Chai, *'Homeland,' Season 2, Episode 10, 'Broken Hearts': TV Recap,* WALL ST. J. (Dec. 2, 2012, 11:00 PM), http://blogs.wsj.com/speakeasy/2012/12/02/homeland-season-2-episode-10-broken-hearts-tv-recap/ [https://perma.cc/5Pe5-48ZV]; *see also* Barnaby Jack, *"Broken Hearts": How Plausible Was the Homeland Pacemaker Hack?*, IOACTIVE (Feb. 26, 2013), https://ioactive.com/broken-hearts-how-plausible-was-the-homeland-pacemaker-hack/ [https://perma.cc/C59K-DQWJ].

303. *See* Tarun Wadhwa, *Yes, You Can Hack a Pacemaker (and Other Medical Devices Too)*, FORBES (Dec. 6, 2012, 8:31 AM), https://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/#6df879826853 [https://perma.cc/F92J-YL7P].

304. *See* Jeremy Kirk, *Pacemaker Hack Can Deliver Deadly 830-Volt Jolt*, COMPUTERWORLD (Oct. 17, 2012, 1:40 AM), https://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html [https://perma. cc/BX6W-WHLW].

identified the flaw in its product.[305] Further, based on security research and warnings issued by the FDA[306] and the Department of Homeland Security,[307] we know that a "[v]ast array of medical devices [are] vulnerable to serious" attacks due to unpatched vulnerabilities and products that ship vulnerable by default.[308] Apart from the predicted concerns of ransomware disabling IoB devices in extortion schemes and botnets of body parts attacking third parties,[309] the Builder Bias problem in IoB has already manifested itself by introducing novel national security risks. For example, inadequate security on the website of an IoB fitness tracking application recently disclosed the location of a previously unknown military base through leaked information about the presence of large numbers of human bodies attached to IoB devices.[310]

Brain interfaces in second- and third-generation IoB, in particular, present opportunities for malicious actors to potentially compromise bodies in order to obtain confidential information, such as passwords,[311] or—even more frighteningly—to corrupt the integrity or availability of the information residing in the brain hardware and, perhaps, even the functionality of the brain itself. Professor Jennifer Chandler and a team of coauthors raise concerns about the use of neuroprosthetic devices and the risk of "brainjacking"—the malicious manipulation of connected brain implants.[312] Similarly, Professors Tamara Bonaci, Ryan Calo, and Howard Jay Chizeck

---

305. *See* Charlie Osborne, *MedSec Sued over St. Jude Pacemaker Vulnerability Report*, ZDNET (Sept. 8, 2016, 8:30 AM), http://www.zdnet.com/article/medsec-sued-over-st-jude-pacemaker-vulnerability-report/ [https://perma.cc/FPF3-K38R].

306. *Cybersecurity*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medicaldevices/digitalhealth/cybersecurity [https://perma.cc/WR6W-WZEU].

307. *See* NCCIC, *supra* note 301.

308. *See* Dan Goodin, *Vast Array of Medical Devices Vulnerable to Serious Hacks, Feds Warn,* ARS TECHNICA (June 13, 2013, 4:54 PM), https://arstechnica.com/information-technology/2013/06/vast-array-of-medical-devices-vulnerable-to-serious-hacks-feds-warn/ [https://perma.cc/8BZP-3RX6].

309. *See supra* notes 273-76 and accompanying text.

310. *See* Richard Pérez-Peña & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say,* N.Y. TIMES (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/ strava-heat-map.html [https://perma.cc/54TC-6YRR].

311. *See* Tom Simonite, *Using Brainwaves to Guess Passwords*, MIT TECH. REV. (May 5, 2017), https://www.technologyreview.com/s/604293/using-brainwaves-to-guess-passwords/ [https://perma.cc/RYR9-4DLB].

312. Clausen et al., *supra* note 241.

warn of the risk of "brain malware"[313] and the need for an interdisciplinary approach to addressing the development of attacks on brain-computer interfaces.[314] Through the eyes of a security professional, these compromised brains are not an "if," they are a certainty—a "when."[315] While these concerns may still be a few years away; lessons from IoT security remind us that the pace and severity of attacks generally escalate and outstrip our preparedness to address them.[316]

The three prior problems introduced above—the Better with Bacon problem of gratuitous connectivity, the Magic Gadget problem of the failure to anticipate failure, and the Builder Bias problem of shipping without securing—all converge to exacerbate the fourth problem—the problem of "Mandatory Soup."

4. The Mandatory Soup Problem: Diminishing Market Choice and Obsolescence Through Adhesion

In the opening episode of *Battlestar Galactica*, a war rages in the galaxy.[317] All of the most advanced military spaceships have been compromised by the enemy because they have been networked together and, therefore, are vulnerable to remote attack by the enemy.[318] Only one ship remains viable—Galactica.[319] It had been "airgapped"[320]—intentionally kept off the grid and disconnected from

313. Victoria Turk, *How Hackers Could Get Inside Your Head with 'Brain Malware*,' VICE MOTHERBOARD (Aug. 3, 2016, 7:50 AM), https://motherboard.vice.com/en_us/article/ezp54e/how-hackers-could-get-inside-your-head-with-brain-malwareups [https://perma.cc/2Q3H-AN29].

314. Tamara Bonaci et al., *App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces*, IEEE TECH. & SOC'Y MAG., June 2015, at 2.

315. Greg Conti (@cyberbgone), TWITTER (Mar. 27, 2017, 4:35 PM), https://twitter.com/cyberbgone/status/846505878824128512 [https://perma.cc/2PCL-JE6S] ("An entire neural malware & anti-malware field is waiting to happen. Imagine #ransomware & the RSA vendor floor then.").

316. George Dvorsky, *How Will We Stop Hackers from Invading Our Brains Once We're Cyborgs?*, GIZMODO (June 29, 2017, 2:00 PM), https://gizmodo.com/how-will-we-stop-hackers-from-invading-our-brains-once-1796520628 [https://perma.cc/PUL8-PQY8].

317. *Battlestar Gallactica: Episode #1.1*, IMDB, http://www.imdb.com/title/tt1699275/plotsummary?ref_=tt_ov_pl [https://perma.cc/RJ45-2VUJ].

318. *Miniseries, Night 1*, FANDOM: BATTLESTAR GALACTICA WIKI, https://galactica.fandom.com/wiki/Miniseries,_Night_1 [https://perma.cc/DTW9-Q52W].

319. *Id.*

320. *See, e.g.*, Unknown Lamer, *Is Analog the Fix for Cyber Terrorism?,* SLASHDOT (Mar.

the other ships as an information security measure by its astute captain, Adama.[321] This plotline from a science fiction television show teaches us an often neglected but basic lesson about technology: the mere existence of a newer technology does not automatically make that new technology the better choice for a particular challenge.[322] This principle that the most connected device may not be the most appropriate device for a particular task might be termed the "Adama Principle."[323]

The Adama Principle is perhaps illustrated best by a famous IoB pacemaker story from 2007 involving former Vice President Dick Cheney. Six years before the compromised pacemaker episode on Homeland[324] aired, then-Vice President Dick Cheney was concerned that attackers would attempt to compromise his implanted defibrillator and kill him.[325] As a consequence, he asked his doctor to disable the device's wireless functionality.[326] But Cheney's leveraging of the Adama Principle is not the norm. Most consumers lack the necessary information regarding potential vulnerability of IoB to be able to make similarly informed choices about their bodies.[327]

Instead of the Adama Principle, what prevails in consumer markets is closer to what might be called the Mandatory Soup problem. Consider a guest at a set-menu wedding dinner. As hardworking servers distribute substantially identical meals to each diner, the opportunity for customization is minimal. As a consequence, a diner sometimes finds herself trapped behind a bowl of unwanted soup for

---

18, 2014, 12:01 AM), http://it.slashdot.org/story/14/03/18/021239/is-analog-the-fix-for-cyber-terrorism [https://perma.cc/6CV9-FZJ3].

321. *See Miniseries, Night 1*, *supra* note 318. Captain Adama knew that the enemy—the cylons—were masters at disabling battlestars by breaking into networks via wireless networks and then using them to disable the whole ship and as a consequence, he ordered that his ship never be networked. *See id.*

322. Michael C. Bodson, *The Latest, Shiniest New Technology Isn't Always the Best*, WORLD ECON. FORUM (Jan. 15, 2018), https://www.weforum.org/agenda/2018/01/why-the-latest-shiniest-tech-isn't-always-best/ [https://perma.cc/MPX7-4B7K].

323. For a different but related version of this idea, see Raza Panjwani (@occamsraza), TWITTER (June 27, 2018, 7:40 AM), https://twitter.com/occamsraza/status/1011982726113759232 [https://perma.cc/68D7-8GWV].

324. Chai, *supra* note 302.

325. Bob Fredericks, *Cheney Feared Terrorists Would 'Hack' Pacemaker*, N.Y. POST (Oct. 19, 2013, 4:11 AM), http://nypost.com/2013/10/19/cheney-feared-heart-gizmo-hack-attack/ [https://perma.cc/4G2Q-NUZK].

326. *Id.*

327. Horrigan, *supra* note 156.

a period of time. While other people may want the soup, she does not, and she experiences negative consequences because it has been foisted upon her. For example, the soup blocks her ability to use the plate beneath the bowl, and it inhibits her streamlined access to the wine in the middle of the table. It also places her at unnecessary risk of soup-related sartorial catastrophe.

The consumer marketplace is becoming flooded with a bevy of "Mandatory Soup" IoT products, often making less-connected versions of those same products nonexistent or hard to find.[328] Rather than maximizing competition on *degree* of connectedness as a differentiating factor within individual product lines, we instead see a progressively impoverished marketplace with consumer products tending to default in their evolution to the maximum degree of connectedness.[329] The Adama Principle of selecting the less connected option when appropriate becomes functionally impossible without extraordinary effort in this type of impoverished artificially constrained marketplace. For example, examining the new car market, finding a new car without multiple accompanying end user license agreements, always on location tracking, and several million lines of code is quickly becoming an impossible task.[330]

Indeed, not only is market choice becoming impoverished on the degree of product in connectedness, but the "real" price of competing goods with the same level of connectedness is becoming incomparable to an average consumer at the time of purchase. Material differences in future obsolescence and data stewardship are usually not disclosed at the time of purchase and not predictable for consumers.[331] Thus, the actual cost of product ownership across time for consumers of an IoT device is frequently not accurately calculable

328. *See* David Roe, *7 Big Problems with the Internet of Things*, CMS WIRE (Feb. 7, 2018), https://www.cmswire.com/cms/internet-of-things/7-big-problems-with-the-internet-of-things-024571.php [https://perma.cc/P6EB-KSYZ].

329. *See id.*

330. *See* Julie A. Steinberg, *Fifty Billion Connected Devices Bring Tort, Software Law Clash*, BLOOMBERG L. (Feb. 26, 2016), https://www.bna.com/fifty-billion-connected-n57982067832/ [https://perma.cc/N4QC-TE7W]. Cars are now functionally IoT devices on wheels—whether consumers desire this extreme connectivity and code-reliance or not. *See* Andrea M. Matwyshyn, *CYBER!*, 2017 BYU L. REV. 1109, 1141-42.

331. *See* David Gewirtz, *Revolv is Dead. Google Killed It. Long Live Innovation*, ZDNET (June 20, 2016, 3:19 PM), http://www.zdnet.com/article/revolv-is-dead-google-killed-it-long-live-innovation/ [https://perma.cc/X9GA-UHM4].

at the point of purchase.[332] A consumer might choose away from one particular product knowing that the expected life is five years shorter than that of another (superficially) competitively priced product. Thus, the Mandatory Soup problem exposes consumers to the undisclosed price terms of (planned and unplanned) unilateral manufacturer obsolescence determinations and data handling changes—rights reserved in the terms of the accompanying (and evolving) end-user license agreements (EULA).[333] This dynamic might be called "obsolescence through adhesion."[334]

IoT history again provides warnings about the hidden costs of Mandatory Soup and, in particular, obsolescence through adhesion. In 2014, Nest acquired an IoT start up called Revolv, a company that made a smart home hub intended to control devices such as lights, alarms, and doors.[335] Allegedly because of an "allocat[ion] [of] resources,"[336] Revolv announced that its service would shut down and customers' applications would no longer work.[337] In short, customers who had purchased the Revolv hub were informed, much to their surprise and dismay, that they would be left with a "bricked" device, regardless of what the company's promises or customers' reasonable expectations were at the time of purchase.[338] This Revolv

---

332. *See id.*

333. As such, it might be argued that in egregious cases, undisclosed hidden costs of planned obsolescence amount to an unfair trade practice under Section 5 of the Federal Trade Commission Act, warping competition in the marketplace of IoT products. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/44NZ-N37A].

334. "Obsolescence through adhesion" refers to the combination of technical and contract-based measures in technology products that functionally hide the actual cost of ownership and can discretionarily force a consumer to discontinue use of a particular product, attempting to nudge the consumer into a new purchase. *See* Andrea Matwyshyn (@amatwyshyn), TWITTER (Mar. 7, 2018, 10:39 AM), https://twitter.com/amatwyshyn/status/971424989063925760 [https://perma.cc/S2VP-YHX4].

335. Nick Statt, *Nest Is Permanently Disabling the Revolv Smart Home Hub*, VERGE (Apr. 4, 2016, 3:40 PM), https://www.theverge.com/2016/4/4/11362928/google-nest-revolv-shutdown-smart-home-products [https://perma.cc/Q9RU-b95W].

336. *Id.*

337. Alex Hern, *Revolv Devices Bricked as Google's Nest Shuts Down Smart Home Company*, GUARDIAN (Apr. 5, 2016, 5:04 AM), https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home [https://perma.cc/CQN8-YL3G].

338. Chris Hoffman, *What Does "Bricking" a Device Mean?*, HOW-TO GEEK (Sept. 26, 2016, 5:36 PM), https://www.howtogeek.com/126665/htg-explains-what-does-bricking-a-device-mean/ [https://perma.cc/L9P6-7GF3].

IoT incident highlights that consumers may not realize that IoT products are now functionally software products still tethered to the manufacturer through remote updates, despite their physicality.

Now, let us turn to the IoB context. Particularly when the obsolescence through adhesion dynamic relates to IoB security and future patches, consumers will find themselves in a dangerous lose-lose scenario that puts them at increased risk of physical harm.[339] Imagine that your eyeball-injected IoB contact lens provider informs you that (per the terms of the contract on which you clicked "yes" when you downloaded your lens software), it has decided that it will no longer support the version of the software your lenses run and that it will no longer push out security patches for your eyes. None of your options are good in this scenario. You can get your lenses removed, risking physical harm and absorbing the cost. You can keep your lenses, knowing they are no longer supported, which, in turn, exposes you to different physical risks through malfunction or security compromise. Alternatively, you can buy "upgraded" lenses, absorbing those associated risks and costs. In all cases, the IoB manufacturer has contractually and technically forced an "upgrade" onto the body of the consumer.

While each of these four problems—the Better with Bacon problem, the Magic Gadget problem, the Builder Bias problem, and the Mandatory Soup problem—is independently a point of concern, when taken together in the context of some second- and third-generation IoB, the risks they present transform into a significant threat in the aggregate—the threat of physical harm to human bodies.[340] Indeed, second-generation IoB presents obvious corporeal risks,[341] while third-generation IoB presents the risk not only of losing control over our own bodies but also our cognitive processing.[342] Put another way, third-generation IoB impacts our functional freedom of thought, and, as a consequence, it presents the threat of potentially losing control over the deliberative individual processes on which we implicitly rely not only for governance of our bodies but

339. Andrea M. Matwyshyn, *The 'Internet of Bodies' Is Here. Are Courts and Regulators Ready?*, WALL ST. J. (Nov. 12, 2018, 11:19 AM), https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566 [https:// perma.cc/XAD8-TJYM].

340. *See id.*

341. *See supra* Part I.A.2.

342. *See supra* Part I.A.3.

also for self-governance in a democratic society.[343] In light of the gravity of these risks, let us consider the current state of IoT and IoB regulation and the desirable directions for its evolution.

C. The Future of Corporate Software Liability and IoB

Morpheus: What is real? How do you define 'real'? If you're talking about what you can feel, what you can smell, what you can taste and see, then 'real' is simply electrical signals interpreted by your brain.[344]

At present, third-generation IoB's risks are (mostly) not yet upon us,[345] but the challenges presented by second-generation IoB are already present and escalating.[346] While last century's legal approaches to technology were animated by a principle of avoiding the imposition of software liability in the name of innovation,[347] IoB forces a recalibration of this default. As human bodies become regularly physically harmed by computer code, consumer and market trust in technology will wane without buttressed legal baselines of consumer protection.[348] Indeed, recent survey data warns that this consumer trust breakdown is already in progress: growing numbers of consumers are doubting whether the Internet has been a mostly positive development for society.[349]

Bolstering consumer trust in technology and constructing an innovation-sensitive legal framework for IoB begins with correcting the legacy problems of IoT identified in Part I.B—the residual deficits in consumer protection from IoT that are already transferring

343. *See infra* notes 565-70 and accompanying text.

344. *The Matrix*, *supra* note 2.

345. *See supra* notes 246-49 and accompanying text.

346. *See supra* Part I.A.2.

347. *See supra* notes 48-18 and accompanying text.

348. For one novel model of creating corporate duties of care in technology conduct, see Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186, 1209 (2016) (arguing "many online service providers and cloud companies ... should be seen as information fiduciaries toward their customers and end users" because by virtue of "their relationship with another," they have assumed "special duties with respect to the information they obtain in the course of the relationship").

349. *See* Pew Research Internet (@pewinternet), TWITTER (May 24, 2018, 7:32 AM), https://twitter.com/pewinternet/status/999659285406765057 [https://perma.cc/XA74-HHJ6].

into IoB. This correction requires improving consumer access to accurate information about the functionality, risks, and true costs of IoB products and services, as well as creating meaningful consumer recourse for physical harms occasioned by IoB. Evolution is needed, in particular, in the frameworks of certain regulatory agencies, tort, contract law, intellectual property, secured transactions, and bankruptcy.[350]

1. Regulatory Agencies

While first-generation IoB regulatory oversight has been primarily divided between the FDA and FTC,[351] next generations of IoB will likely require a greater level of regulatory involvement not only from those two agencies, but also the Consumer Product Safety Commission, the Consumer Financial Protection Bureau, and the Federal Communications Commission, among others.

a. FDA

Although most first-generation IoB devices were deemed to fall outside the FDA's definition of a medical device,[352] a portion of second- and third-generation IoB devices will be deemed medical devices falling squarely within the FDA's regulatory and oversight authority.[353] With the goal of improving the quality of the software embedded in medical devices, including IoB medical devices, the FDA has released two guidance documents on security. The first is entitled "Content of Premarket Submissions for Management of Cybersecurity and Medical Devices: Guidance for Industry and Food and Drug Administration Staff," dated October 2, 2014, and provides guidance on the types of security considerations medical device manufacturers should incorporate in developing (and disclosing substantiated information about) their devices,[354] as

350. *See* Matwyshyn, *supra* note 339 (exploring questions regarding the IoB in the realms of regulatory agencies, intellectual property, contracts, and bankruptcy).

351. *See id.*

352. *See supra* note 96 and accompanying text.

353. *See supra* notes 183, 239 and accompanying text.

354. U.S. FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES (2014). The guidance offers a useful preliminary

updated.[355] The second guidance is entitled "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff" issued on December 28, 2016, and creates ongoing duties of care to ensure the security of devices on the market.[356] These documents signal a shift in the agency toward greater scrutiny of IoB devices, particularly on security.

In addition to this guidance, at least three specific changes to the FDA's current approach would materially improve its preparation for the further arrival of IoB. First, the FDA should compel significantly more detailed premarket disclosures from companies with respect to IoB technologies. These disclosures should include representations regarding third-party code audit and testing, specifying any embedded code libraries, third-party hardware components, and comparable information.[357] In turn, the FDA should make this information available to the public and searchable. This additional information transparency will facilitate more informed decision-making by patients and medical professionals and allow for third-party researcher validation. The FDA should also continue to collaborate with the teams of security professionals that assisted it with its postmarket guidance[358] to craft this list of necessary informational disclosures. For companies relying on the 510(k) premarket approval streamlined process to release devices,[359] a duty of "security parity" should be required. Specifically, the FDA should

---

starting point for medical device manufacturers unfamiliar with the basics of security. *See id.* at 1-2. However, the guidance unfortunately does not provide rigorous disclosure requirements that would facilitate informed decision-making by consumers. *See id.* at 3-4. In particular, the guidance contains no discussion of third-party product audits or penetration testing of devices to assess the integrity, availability, and confidentiality of the code they contain. *See id.* at 4-5. Encryption of data is suggested only "where appropriate," demonstrating a restrained set of recommendations that are unlikely to cause dramatic improvements in the quality of medical device security. *See id.* at 5.

355. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, U.S. FOOD & DRUG ADMIN. (Oct. 2018), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices [https://perma.cc/3R2M-UFYJ].

356. U.S. FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES 4 (2016).

357. U.S. FOOD & DRUG ADMIN., *supra* note 355.

358. *See id.* at 7.

359. *See id.* at 2.

issue guidance stating that by relying on the 510(k) process, these companies will be deemed to implicitly attest that their current devices (and all code therein) are as safe as their prior devices introduce no new risks to safety. This code safety warranty extends to security.

Second, the FDA should correct the imperfections in its adverse event reporting structures and improve the public accessibility of verified adverse event information. FDA adverse event reporting structures as they currently exist are not optimally suited to address security incidents in next generation technologies such as IoB.[360] Despite the agency's receptivity to third-party reports,[361] there appears to be no obvious, publicized, formal channel through the website to accept adverse event reports from nonmedical professionals such as security researchers and others who have potentially identified the existence of life-threatening code flaws in medical devices.[362] Similarly, past historical approval recall and adverse event data should be made more usable for patients. It should also be expanded and re-analyzed to provide more specific descriptions of incidents where a "software design issue" impacted the functionality of the medical device.

Third, the FDA should mandate as a condition of either a new device approval or a 510(k) premarket approval that it or a patient (or a deceased patient's family or designee) be provided an opportunity to conduct an independent forensic analysis of an IoB device following an adverse incident. Manufacturers and insurers should be prohibited from exercising intellectual property and contract rights against patients to block the performance of forensic examinations of code in devices that potentially has led to human injury. Finally, the FDA should collaborate more formally and closely with the Federal Trade Commission to minimize potential regulatory gaps.

---

360. *See Reporting Serious Problems to FDA*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/Safety/MedWatch/HowToReport/default.htm [https://perma.cc/D8Y6-QPJU] (outlining FDA incident reporting procedures for consumers).

361. *See id.*

362. *See id.* (outlining voluntary reporting procedures for consumers and healthcare professionals, but not for nonmedical professionals). Recall information on medical devices with code flaws is also not easily findable for consumers who wish to determine the safety history of a particular medical device. *See supra* text accompanying notes 296-99.

b. FTC

As explained in prior sections, first-generation IoB devices were frequently deemed by the FDA[363] to constitute general wellness and healthy lifestyle devices rather than medical devices.[364] Consequently, their primary regulator became the FTC.[365] With medical devices, the FTC's enforcement is primarily limited to policing false, unfair, or deceptive health claims in advertisements and marketing.[366] However, for lifestyle products such as most first-generation IoB devices including fitness trackers, the FTC is the primary enforcement agency not only for advertising/marketing, but also unfair and deceptive practices.[367] In other words, whether the device is classified by the FDA as medical or "healthy lifestyle"/recreational directly impacts the FTC's jurisdictional reach.[368]

With second- and third-generation IoB devices, the FDA is again unlikely to decide that all of these devices are "medical devices," particularly where the device's stated primary use relates to optional self-augmentation for nonmedical reasons.[369] Despite the FDA's recent robust interest in security of medical devices, the FTC has historically taken the more aggressive posture in consumer protection and code quality, in particular with respect to data

363. The FDA is the primary regulatory agency overseeing approval and safety of medical devices. *See* U.S. FOOD & DRUG ADMIN., *supra* note 356.

364. The FDA describes its mission as one of protecting

> the public health by ensuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The agency also is responsible for the safety and security of our nation's food supply, cosmetics, dietary supplements, products that give off electronic radiation, and for regulating tobacco products.

FDA in Brief: FDA Issues Guidance to Help Animal Drug Manufacturers Meet Antimicrobial Sales Data Reporting Requirements, FOOD & DRUG ADMIN. (June 28, 2018), https://www.fda.gov/NewsEvents/Newsroom/FDAInBrief/ucm612145.htm [https://perma.cc/7XEF-VWXF].

365. The Federal Trade Commission describes itself as an agency charged with a "unique dual mission to protect consumers and promote competition." *What We Do*, U.S. FED. TRADE COMM'N, www.ftc.gov/about-ftc/what-we-do [https://perma.cc/GT5V-CVEA].

366. This is in addition to competition matters. *See Health Claims*, U.S. FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/advertising-and-marketing/health-cl [https://perma.cc/FEZ7-UJE7].

367. *See* 15 U.S.C. § 45 (2012).

368. *See supra* notes 185-94 and accompanying text.

369. For example, the British Airways "customer experience" pill ostensibly offers no medical benefit. *See supra* notes 215-16 and accompanying text.

security and consumer privacy.[370] For example, the FTC has engaged in approximately sixty enforcement actions to date[371] against companies for failing to use reasonable security practices[372] in their operations. Yet, the FTC is a much smaller agency than the FDA and currently lacks the bandwidth to monitor a future explosion of IoB devices (in addition to its current enforcement responsibilities) without additional resources.[373]

The FDA and FTC have not formally collaborated up to this point on IoB issues. Formalizing this collaboration into a targeted, joint effort presents the most logical starting point for more effective regulation of second and third-generation IoB. Specifically, the FTC should launch a new "technology practices" group, with a joint FTC-FDA cross-detailed team focused on IoB enforcement.[374] Because of the FDA's and FTC's distinct but complementary authority, this joint group would be able to engage in streamlined enforcement. Most importantly, the existence of the team and its coordination should prevent IoB products that harm consumers from falling through the definitional gaps of what does and does not constitute a "medical device." In particular, the new IoB team in the technology practices group should be granted rulemaking and fining authority by Congress,[375] and it should also use core FTC Act Section 5 authority to aggressively enforce the FTC Act's prohibition on

370. For a discussion of the FTC's security enforcement, see Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2267, 2269, 2276, 2282 (2015).

371. *See Cases Tagged with Data Security*, U.S. FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/terms/249 [https://perma.cc/7MCH-2DVS].

372. *See* START WITH SECURITY, *supra* note 295.

373. In the year 2018, FDA reported 17,468 employees, while the FTC reported 1114. *Compare* U.S. FOOD & DRUG ADMIN., DETAIL OF FULL-TIME EQUIVALENT EMPLOYMENT (FTE), https://www.fda.gov/downloads/aboutfda/reportsmanualsforms/reports/budgetreports/ucm566335.pdf [https://perma.cc/42QG-DST6], *with* U.S. FED. TRADE COMM'N, AGENCY FINANCIAL REPORT: FISCAL YEAR 2018 (2018), https://www.ftc.gov/system/files/documents/ reports/agency-financial-report-fy2018/ftc_agency_financial_ report_fy2018_1.pdf [https://perma.cc/NUM4-VP5Y].

374. This team should include cross-detailed investigators, technologists, and attorneys whose enforcement activity will focus on both the marketing practices and technological risks of IoB devices.

375. While the FTC could create this practice group using its current regulatory authority under Section 5 of the FTC Act and its other statutory authorities, a congressional authorization explicitly granting fining and rulemaking authority to a new practice group would nudge the group's creating with greater speed and agency confidence.

unfair and deceptive advertising claims about IoB.[376] In particular, with respect to "lifestyle" and recreational IoB, ensuring disclosure of the hidden consumer costs identified in earlier sections of this Article[377] aligns with the FTC's mission of consumer protection and preserving fair competition in the market.[378] Thus, the new technology practices group would both protect consumers from unfair and deceptive practices and encourage fair competition—the two cornerstones of the FTC's mission.[379]

c. CPSC

The Consumer Product Safety Commission (CPSC) offers an underexplored avenue of consumer protection in IoT and IoB. Any IoT device, such as a smart TV or an Internet-connected baby monitor, is also subject to any applicable safety requirements of CPSC.[380] However, the CPSC has only recently begun an inquiry regarding the safety of Internet of Things products[381] and has otherwise not yet engaged with rulemaking[382] in the areas of embedded device hardware and software safety in any IoB-specific context.[383] Consequently, the CPSC should organize a working group around issues of IoB hardware and software safety, culminating in

376. *See* 15 U.S.C. § 45 (2012).

377. *See supra* Part I.A.1.

378. *See What We Do*, *supra* note 365.

379. *See id.*

380. *See About CPSC*, U.S. CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/About-CPSC [https://perma.cc/MV54-N9Z4].

381. *See CPSC Conducting a Public Hearing on the "Internet of Things and Consumer Product Hazards,"* U.S. CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/Newsroom/Public-Calendar/2018-05-16-140000/cpsc-conducting-a-public-hearing-on-the-%E2%80%9Cinternet-of [https://perma.cc/Z28U-W6KV].

382. Elliot F. Kaye & Jonathan D. Midgett, *A Framework for Safety Across the Internet of Things*, U.S. PRODUCT SAFETY COMM'N. (Jan. 31, 2019), https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf?1KJ.t4Tn04v9OtEBr2s0wyLAP.KsuuQ3 [https://perma.cc/J4QF-BK8C].

383. A query for software on the CPSC website yielded zero results. *See Search Results*, U.S. CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/Newsroom/News-Releases?edit-field-nnr-date-value-value%5Bvalue%5D%5Bmonth%5D=&edit-field-nnr-date-value-value%5Bvalue%5D%5Byear%5D=&field_nnr_heading_value=software [https://perma.cc/8ZFC-Y4U2]. A query for hardware yielded one result from 1984 related to mechanical crib components, not computing hardware. *See CPSC Votes on Crib Hardware*, U.S. CONSUMER PROD. SAFETY COMM'N (Apr. 2, 1984), https://www.cpsc.gov/Newsroom/News-Releases/1984/CPSC-Votes-On-Crib-Hardware [https://perma.cc/H4U5-MNU2].

rulemaking that focuses on IoB consumer products.[384] It should also contribute a cross-detailed team to the FTC's new technology practices group.

d. CFPB

As companies experiment with "social credit" monitoring,[385] it is perhaps predictable that the current wide breadth of (sometimes inaccurate)[386] information included in U.S. credit reports and background checks will continue to expand. In particular, assessments of credit "risk" based on streams of data from IoB devices are likely to become incorporated. For these reasons, the Consumer Financial Protection Bureau's (CFPB) self-interpretation of its mission[387] and its express regulatory authorization[388] (as well as the definition of "credit report"[389]) should be extended to include all potentially "credit-impacting information," regardless of the identity of the corporate holder and not merely the historical categories of information held by traditional credit reporting agencies and financial institutions. With this expansion, the CFPB would be well-positioned to engage in enforcement actions where IoB data streams, particularly streams from second- and third-generation

384. For a discussion of the CPSC, see Anita Bernstein, *Implied Reverse Preemption*, 74 BROOK. L. REV. 669, 669 (2009).

385. For example, China uses a social credit score system. *See, e.g.*, Mara Hvistendahl, *Inside China's Vast New Experiment in Social Ranking*, WIRED (Dec. 14, 2017, 6:00 AM), https://www.wired.com/story/age-of-social-credit/ [https://perma.cc/ZSD8-ZGQW].

386. *See* U.S. FED. TRADE COMM'N, REPORT TO CONGRESS UNDER SECTION 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003, at 6 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/section-319-fair-accurate-credit-transactions-act-2003-sixth-interim-final-report-federal-trade/150121factareport.pdf [https://perma.cc/FNT6-MYA9].

387. The CFPB describes its mission as follows: "The CFPB implements and enforces federal consumer financial laws to ensure that all consumers have access to markets for consumer financial products and services that are fair, transparent, and competitive." *Rulemaking*, U.S. CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/policy-compliance/rulemaking/ [https://perma.cc/C6PJ-JWUK].

388. The Dodd-Frank Act created the CFPB, setting forth its mission as follows: "The Bureau shall seek to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive." 12 U.S.C. § 5511(a) (2012).

389. Fair Credit Reporting Act, 15 U.S.C. § 1681a(d) (2012).

IoB, impact the financial opportunities of consumers because of data repurposing and licensing.

e. FCC

Perhaps surprisingly, the Federal Communications Commission's (FCC)[390] and Congress's[391] ongoing net neutrality debate is important to IoB's future.[392] If consumers rely on life-enabling or hard-wired IoB technologies, poor Internet connectivity will have physical consequences.[393] Consider the next generation of neural-bypass technologies—technologies already FDA approved for testing—that allow paralyzed limbs to function with the assistance of a body-external computer and a chip implanted in the body.[394] These technologies will rely on software for their security and functionality, and all software requires patching and updating.[395] This means that at least some aspects of operation of these IoB devices are likely to rely on real-time Internet access and feedback.[396] Poor Internet access will, therefore, potentially mean increased risk of physical harm and limited functionality for these IoB bodies.[397]

The reasons for poor connectivity may be due to inadequate network infrastructure, but they may also be due to deliberate throttling decisions by an Internet provider for "network management" purposes or because the customer (the IoB company or the consumer) have purchased a lower "tier" of service.[398] Serious

390. *Restoring Internet Freedom*, U.S. FED. COMMC'NS COMM'N, https://www.fcc.gov/restoring-internet-freedom [https://perma.cc/MQ3K-SLE7].

391. James K. Willcox, *Net Neutrality Battles Move to the States, Congress, and the Courts*, CONSUMER REP. (Mar. 8, 2018), https://www.consumerreports.org/net-neutrality/net-neutrality-battles-move-to-states-congress-courts/ [https://perma.cc/SL6G-SVRY].

392. Supporters of net neutrality believe it is essential to next generation innovation. *See Principles to Preserve & Protect an Open Internet*, INTERNET ASS'N, https://internetassociation.org/reports/principles-to-preserve-protect-an-open-internet/ [https://perma.cc/GPR3-KYES].

393. Andrea M. Matwyshyn, *Unavailable*, 81 U. PITT. L. REV. (forthcoming 2019).

394. *See supra* notes 166-76 and accompanying text.

395. *See supra* Introduction.

396. *See, e.g.*, *supra* notes 16-20 and accompanying text.

397. *See, e.g.*, Urban, *supra* note 241.

398. Major Internet service providers have been accused of throttling access. *See* Jon Brodkin, *Verizon Throttled Fire Department's "Unlimited" Data During Calif. Wildfire*, ARS TECHNICA (Aug. 21, 2018, 3:49 PM), https://arstechnica.com/tech-policy/2018/08/verizon-throttled-fire-departments-unlimited-data-during-calif-wildfire/ [https://perma.cc/735C-7Y69].

physical security consequences are possible, particularly in security emergencies.[399] For example, imagine the WannaCry attack scenario, but instead of hospital administrative computers, the malware exploits an unpatched vulnerability in IoB medical devices. Imagine an emergency patch becomes available, but it is too large to push to some users because of the bandwidth limitations of their tier of Internet service. Unpatched, vulnerable code in an Internet of Bodies device means that an attacker may be able to take control of or harm the connected body part through that device.

For reasons of security, a robust market in Internet of Bodies products will not blossom without reliable and abundant, high-quality (and affordable) Internet access.[400] These Internet infrastructure and market conditions are a prerequisite for the functionality, security, and adoption of IoB devices.[401]

In addition to these regulatory questions, IoB security failures and data breaches will lead to additional regulatory consequences under existing data protection statutes on the federal, state,[402] and international levels.[403] But, there are also less obvious legal and security questions involving tort, contract, intellectual property, and secured transactions and bankruptcy law.

2. Tort

In what might be considered a type of technology performance art, a technology writer recently connected a shock-delivering IoB bracelet he was wearing to Twitter and informed his followers that

399. *See id.*

400. For a discussion of the importance of reliable and redundant Internet access to the adoption of IoB, see Matwyshyn, *supra* note 393.

401. *Id.*

402. After a data breach or a deficiency in reasonable security practices, these expected legal consequences include FTC or FDA scrutiny, a class action tort suit, and state-level breach notification duties. *See* Jeff John Roberts, *A Surprise in the Equifax Breach: Victims Likely to Get Paid*, FORTUNE (Oct. 10, 2017), http://fortune.com/2017/10/10/equifax-class-action/ [https://perma.cc/EH7T-LET3]. For public companies, consequences may include SEC enforcement actions. *See Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, U.S. SEC. & EXCH. COMM'N (Feb. 21, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf [https://perma.cc/2R65-HQZR].

403. *See, e.g.*, *General Data Protection Regulation*, EUROPEAN UNION, https://gdpr-info.eu/ [https://perma.cc/E4KZ-QXDT].

they had the ability to zap him remotely.[404] Although the product in question, an IoB bracelet that pairs with mobile phones and intentionally shocks the wearer, was presumably not designed with third-party Internet zapping in mind, the company's CEO appeared to validate this particular personalization and other repurposed uses.[405] The writer's experiment and the CEO's response raise interesting, unsettled questions regarding the relationship among code, tort, security, and IoB product testing and design. In the situation where a device, such as this one, malfunctions and causes bodily injury, courts will struggle with fact-intensive legal inquiries in IoB.

As Professor Mark Geistfeld has explained in the IoT context of connected cars:

> The potential for legal error is ... compounded by the need for courts to resolve this issue for each body of state tort law. As compared to a relatively "easy" problem, courts across the country are more likely to adopt different rules for solving a difficult tort issue, creating substantial variability within the national market.[406]

A similar dynamic is likely to present itself in the context of IoB.

Indeed, journalists have long warned that current medical devices regularly demonstrate lack of care in their manufacture and testing upon closer examination.[407] These concerns become amplified in the context of IoB. In addition to the software-interrupted surgery discussed in Part I and the medical disruptions caused by

---

404. Jack Morse, *Some Guy Connected an Electroshock Bracelet to Twitter and Let the World Have at Him*, MASHABLE (Aug. 24, 2017), https://mashable.com/2017/08/24/twitter-shock-bracelet/#YM8xWToDyEqW [https://perma.cc/GF8H-939T].

405. *See id.* ("'I think the public experiment is very cool, and we LOVE the ability to "touch" across the Internet—including vibration patterns, sound, and zap,' Maneesh Sethi wrote over email. 'Of course, it's all configurable to what you want.'").

406. Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CALIF. L. REV. 1611, 1618-19 (2017). Professor Geistfeld further explains that courts "will presumably correct mistakes over time, but the prospect of initial legal error and widespread disagreement creates an additional source of uncertainty for manufacturers trying to assess their potential liability in the national market." *Id.* at 1619.

407. *See Are Implanted Medical Devices Creating a 'Danger Within Us'?*, NPR (Jan. 17, 2018, 3:10 PM), https://www.npr.org/2018/01/17/578562873/are-implanted-medical-devices-creating-a-danger-within-us [https://perma.cc/9P6Q-CQXA].

ransomware in Part II, software errors have already been implicated in deadly medical failures.[408] However, the nonmedical uses of IoB are also likely to sometimes result in unfortunate outcomes with bodily injury. The regulatory gaps described previously[409] mean that some IoB products will potentially be subject to no preemptive regulatory scrutiny before entering the market. This legal environment also makes it more likely that plaintiffs will turn to tort law to address the failures in these products that cause physical harms to human bodies.

Because, to date, a majority of IoT consumer harms have related to privacy and security,[410] private litigants have faced challenges in demonstrating actual economic losses in the eyes of some courts.[411] However, the obstacles of demonstrating actual economic loss become substantially more straightforward when the connected "thing" is a human body: the "blue screen of death"[412] can become, quite literally, a blue screen of death or the cause of extreme physical harm for an IoB-connected human. In other words, the economic loss will often be more easily quantifiable and economically demonstrable in IoB contexts than was possible in prior generations of software cases. Because of courts' familiarity with providing recourse for bodily injury in tort, these IoB cases are likely to result in new doctrinal lines of software liability.

Instead, the tort arguments are likely to shift toward various possible calculations of damages amounts and to what extent any liability protection exists for the device manufacturers—akin to traditional medical device harm cases.[413] These determinations will

---

408. *See* Adam Fabio, *Killed by a Machine: The Therac-25,* HACKADAY (Oct. 26, 2015), https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/ [https://perma.cc/9598-8J92].

409. *See supra* text accompanying notes 345-49.

410. *See* Jenni Ryall, *How Your Smart Device Caused the Internet to Crash and Burn*, MASHABLE (Oct. 21, 2016), https://mashable.com/2016/10/21/dyn-attack-iot-device/ [https://perma.cc/MJ24-DGPD].

411. Edward R. McNicholas & Grady Nye, *D.C. Circuit Widens the Split on Standing in Data Breach Cases After* Spokeo, SIDLEY AUSTIN LLP (Aug. 8, 2017), https://datamatters.sidley.com/d-c-circuit-widens-split-standing-data-breach-cases-spokeo/#page=1 [https://perma.cc/RDU9-BJ3G].

412. Chris Hoffman, *Everything You Need to Know About the Blue Screen of Death*, HOW-TO GEEK (Nov. 12, 2018, 11:05 AM), http://www.howtogeek.com/163452/everything-you-need-to-know-about-the-blue-screen-of-death/ [https://perma.cc/8SD6-UMHA].

413. Manufacturers may also attempt to identify the cause of the harm as a deficit of care

examine whether the devices are "medical" in the eyes of the FDA, the relationship of contract waivers of liability, what constitutes defective design, and the well-trod debates in tort law over the appropriate calculations of pain and suffering. The often predictable failures of code and hardware visible in the Internet of Things will morph into the often unpredictable and idiosyncratic failures of devices and software intersecting with various idiosyncrasies of the "hardware" of human bodies.

Specifically, suits seeking recourse for harms arising from IoB will encounter the "legacy code" of tort law—doctrines of product liability and its subfield of medical device liability in particular. Some will succeed even in the IoB medical device context tort liability is likely in some cases. Historically, courts have not uniformly protected manufacturers from tort liability in health device cases, particularly for devices that are not deemed to be Class III medical devices.[414] For IoB manufacturers, a lower FDA class categorization for their medical IoB device may seem attractive because it means getting to market faster. However, that lower categorization may also mean greater risk of tort liability, including for security harms.[415]

The case law litigating disputes around pacemakers and cochlear implants, two of the earliest IoB devices,[416] may act as a harbinger of how we might expect tort claims for IoB harms to play out in the courts. Tort claims for pacemaker harms have generally involved eight kinds of claims: failure to warn,[417] breach of warranty,[418]

---

on the part of a medical professional or other "installer" of an IoB device, another familiar analysis for courts from past generations of medical device cases.

414. *See, e.g.*, Paul H. Sunshine, *The Preemptive Scope of the Medical Device Amendments of 1976*, 50 FOOD & DRUG L.J. 191, 209 n.135 (1995) ("A determination that a device belongs in class III, as opposed to classes I or II, completely shields the manufacturer of such device from state tort liability. Courts generally have been deferential to FDA reclassifications.").

415. *See id.*

416. Pacemakers and cochlear implants are now calibrated while attached to the body by physicians through the use of software. *See, e.g.*, Jeff Lagasse, *Cochlear Limited Launches FDA-Cleared, Apple-Compatible Cochlear Implant*, MOBIHEALTHNEWS, https://www.mobihealthnews.com/content/cochlear-limited-launches-fda-cleared-apple-compatible-cochlear-implant [https://perma.cc/M6EN-3ZXX].

417. *See, e.g.*, Lohr v. Medtronic, Inc., 56 F.3d 1335, 1350-52 (11th Cir. 1995) (holding that the plaintiffs' failure to warn claim was preempted).

418. *See, e.g.*, Talbott v. C.R. Bard, Inc., 63 F.3d 25, 31 (1st Cir. 1995) (holding plaintiffs' breach of warranty claim was preempted).

design defect,[419] negligence,[420] fraud,[421] misrepresentation,[422] RICO,[423] and unfair state trade practices.[424] Cases demonstrate that courts are not always quick to dismiss, and some claims for failure to warn[425] and breach of warranty[426] have resulted in plaintiff success. One material obstacle for plaintiffs is the possible preemption of their claims by federal law under the Medical Device Amendments[427] to the Food, Drug, and Cosmetic Act;[428] however, courts have ruled both in favor of federal preemption[429] and against preemption[430] in pacemaker cases. Cardiac pacemakers have also been held to be unavoidably unsafe products within the meaning of comment k to Section 402A of the Second Restatement of Torts,[431] which adds to plaintiffs' difficulty in establishing claims. Yet, this determination has not dispositively prevented recovery in all

419. *Lohr*, 56 F.3d at 1347.

420. *Id.*

421. *See, e.g.*, Woods v. Gliatech, Inc., 218 F. Supp. 2d 802, 810-11 (W.D. Va. 2002) (holding that the Medical Device Amendments did not preempt the plaintiff's negligence, fraud, and failure to warn claims against the manufacturer of a device used in surgical back procedures).

422. *See, e.g.*, Kemp v. Medtronic, Inc., 231 F.3d 216, 232-36 (6th Cir. 2000) (discussing plaintiffs' fraudulent misrepresentation claim against pacemaker manufacturer).

423. *See, e.g.*, *In re* Cordis Corp. Pacemaker Prod. Liab. Litig., No. MDL 850, C-3-86-543, 1992 WL 754061, at *3 (S.D. Ohio Dec. 23, 1992); *see also* Int'l Bhd. of Teamsters v. Philip Morris, Inc., 196 F.3d 818, 823 (7th Cir. 1999) ("[G]etting a product that causes deferred injury and medical expenses, causes a loss of one's money, which is 'property.'").

424. *See, e.g.*, Martin v. Medtronic, Inc., 254 F.3d 573, 575 (5th Cir. 2001).

425. *See, e.g.*, *Woods*, 218 F. Supp. 2d at 810-11 (holding that the Medical Device Amendments did not preempt the plaintiff's failure to warn claims against the manufacturer of a device used in surgical back procedures).

426. *See, e.g.*, Fogal v. Steinfeld, 620 N.Y.S.2d 875, 883 (Sup. Ct. 1994) (ruling defective design, breach of warranty, and failure to warn claims against pacemaker manufacturer were not preempted).

427. 21 U.S.C. § 360(c)-(k) (2012).

428. §§ 301-399.

429. *See, e.g.*, R.F. and R.F. v. Abbott Labs., 745 A.2d 1174, 1192 (N.J. 2000) (holding that the FDCA preempted the plaintiff's negligent design and strict liability claims).

430. *See, e.g.*, Medtronic, Inc. v. Lohr, 518 U.S. 470, 502 (1996) (holding that the FDA's shortened approval process for devices that are substantially similar to those already on the market does not trigger preemption of state common law claims under section 360k(a)—the Medical Device Amendments' preemption provision).

431. RESTATEMENT (SECOND) OF TORTS § 402A cmt. k (AM. LAW INST. 1965) ("There are some products which, in the present state of human knowledge, are quite incapable of being made safe for their intended and ordinary use.... Such a product, properly prepared, and accompanied by proper directions and warning, is not defective, nor is it unreasonably dangerous.") (emphasis omitted).

cases.[432] Cochlear implants cases have similarly resulted in rulings divided on the preemption issue,[433] with some claims in negligence,[434] breach of warranty,[435] fraud and negligent misrepresentation,[436] and common law strict liability[437] surviving preemption analysis. Therefore, it is fair to say that courts have not adopted a uniform position on pacemaker and cochlear implant manufacturer liability in tort and that the inquiries are particularly fact-intensive.

IoB device cases are likely to further feed this doctrinal complexity in tort cases, leading to years of uncertainty in IoB tort litigation. While this result may seem inefficient, it is not necessarily a bad outcome. By contrast, if courts took a legal shortcut and adopted a position that the mere presence of software should dispositively trigger liability limitation, the consequences would be undesirable for IoB consumer protection. Meanwhile, the inverse, in an unnuanced form, might damage IoB medical innovation.

3. Contract

Professor Margaret Radin has argued that contract law, particularly through the use of boilerplate terms, has facilitated the convergence of machine and text, leading to an undesirable imbalance that places consumers at risk in their technology transactions.[438] The contract law imbalances that Professor Radin has highlighted become exacerbated when the technologies at issue are attached to and embedded in human bodies with IoB.

---

432. *See, e.g.*, *Lohr*, 518 U.S. at 494 (holding that plaintiff's negligent design claims under Florida law were not preempted).

433. *See* Purcel v. Advanced Bionics Corp., No. 3:07-CV-1777-M, 2008 WL 3874713, at *5 (N.D. Tex. Aug. 13, 2008) (surviving preemption challenge).

434. *See, e.g.*, *id.* at *2 (refraining from even considering if negligence claim was preempted).

435. *See, e.g.*, *id.* at *2-5.

436. *See, e.g.*, *id.* at *2 (refraining from even considering if fraud claim was preempted).

437. *See, e.g.*, *id.* at *2-5.

438. MARGARET RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 9, 15-18 (2013) (arguing that normative and democratic degradation is resulting from the standardization dynamics in current digital contracting); *see* Margaret Jane Radin, *Online Standardization and the Integration of Text and Machine*, 70 FORDHAM L. REV. 1125, 1125 (2002) (arguing that "blurring is helping to break down the distinction between technological standards and legal standards").

a. EULAs

IoB companies primarily rely on contracts—such as EULA and privacy policies—to obtain the rights to monitor, aggregate, and share users' body data, as well as to retain rights in the software. Learning again from IoT history, we find a collision of contract law from sales of physical goods, on the one hand, with norms of the world of software contracts, on the other.[439]

Traditionally, under the approach set forth in the individual state versions of Uniform Commercial Code (UCC) Article 2, when purchasing a physical good, a consumer usually retains certain rights of recourse regardless of what any agreement accompanying the physical good may stipulate.[440] New products are generally not sold on an as-is/where-is basis.[441] However, historically, that minimum guaranteed level of functionality/fitness, merchantability, and consumer recourse has not been the default with respect to software products.[442] Indeed, most end-user license agreements stipulate that the code is provided as-is/where-is and that consumer remedies, including any remedies under UCC Article 2, do not apply.[443] IoT has added complexity not only with respect to consent in contract

439. This crash will particularly impact warranties implied by law and recourse/enforceability of limitations of liability.

440. *See, e.g.*, U.C.C. § 2-315 (AM. LAW INST. & NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 2017) ("Implied Warranty: Fitness for Particular Purpose. Where the seller at the time of contracting has reason to know any particular purpose for which the goods are required and that the buyer is relying on the seller's skill or judgment to select or furnish suitable goods, there is, unless excluded or modified under the next section an implied warranty that the goods shall be fit for such purpose.").

441. For a discussion of implied warranties, see, for example, Stacy-Ann Elvy, *Hybrid Transactions and the INTERNET of Things: Goods, Services, or Software?*, 74 WASH. & LEE L. REV. 77, 87 (2017) (arguing that "[t]he application of Article 2, along with its implied warranties to transactions involving IOT products, may encourage IOT companies to effectively address ... security concerns."); Matwyshyn, *supra* note 330, at 1183 (arguing for implied warranties of security modeled on UCC Article 2 and landlord-tenant law).

442. For a discussion of software liability see, for example, Peter A. Alces & Aaron S. Book, *When Y2K Causes "Economic Loss" to "Other Property,"* 84 MINN. L. REV. 1, 5 (1999) (assessing "[w]hether the strict products liability law provides the basis to award a commercial entity damages for the 'economic loss' caused by the Millennium Bug").

443. For example, the EULA for one of Ford's software products embedded in cars includes extensive limitations of liability and disclaimers of warranties and imposes an "obligation to drive responsibly" on drivers. FORD, END USER LICENSE AGREEMENT, https://www.ford.com/resources/ford/general/pdf/sync3eulareformatted.pdf [https://perma.cc/B472-C4VX].

formation,[444] but also with respect to breach[445] and damages analysis.[446] Similarly, IoT has also caused us, yet again, to engage with many of the issues discussed decades ago during the debate over the drafting of UCC Article 2B for software transactions. But, now these questions also directly implicate aspects of the functionality in the context of a UCC Article 2 consumer good.[447] It also wades us knee-deep into the doctrinal weaknesses of the *ProCD, Inc. v. Zeidenberg*[448] line of cases.[449]

Despite the practical reality that users rarely read or comprehend lengthy user contracts (even Chief Justice John Roberts has admitted to not always reading them),[450] courts have been slow to limit their enforceability.[451] Meanwhile, companies' aggressive contracting practices raise progressively more troubling questions. For

444. For a discussion of consent in IoT, see, for example, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 95 (2014).

445. *See, e.g.*, Stacy-Ann Elvy, *Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond*, 44 HOFSTRA L. REV. 839, 864 (2016) (discussing IoT, robotic agents, and that "a principal may be subject to liability to the agent for breach of contract").

446. Elvy, *supra* note 441, at 148 (arguing that viewing IoT transactions as hybrid "could present insurmountable problems of proof in determining how to apply different rules of damages"). Courts look at a number of factors in determining the severity of breaches, including the extent to which money can make the plaintiff whole. *See* Elvy, *supra* note 445, at 864 (discussing the complexity of IoT device breach of contract).

447. UCC Article 2B became the Uniform Computer Information Transactions Act (UCITA) and the Uniform Electronic Transactions Act (UETA); UCITA was adopted in only two states, but UETA was widely adopted. *See generally* Richard E. Speidel, *Revising UCC Article 2: A View from the Trenches*, 52 HASTINGS L.J. 607 (2001). For a discussion of the UCC Article 2B revision process, see *id.* at 607 (explaining that there "was plenty of trouble in the Article 2 process").

448. 86 F.3d 1447 (7th Cir. 1996).

449. In particular, courts have not yet grappled with the question of "returnability" or rejection of nonconforming or defective software when it has been embedded into the ecosystem of your body and potentially caused harm. For a discussion of the shortcomings of *ProCD*, see, for example, Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 550-54 (2007).

450. Mike Masnick, *Supreme Court Chief Justice Admits He Doesn't Read Online EULAs or Other 'Fine Print*,' TECH DIRT (Oct. 22, 2010, 9:48 AM), https://www.techdirt.com/articles/20101021/02145811519/supreme-court-chief-justice-admits-he-doesn-t-read-online-eulas-or-other-fine-print.shtml [https://perma.cc/UZ7R-3HNE].

451. Cases enforcing end user license agreements also frequently uphold prohibitions against class actions. *See, e.g.*, Cullinane v. Uber Tech., Inc., No. 14-14750-DPW, 2016 WL 3751652, at *9 (D. Mass. July 11, 2016) (upholding the Uber EULA and its class action prohibition). *But see* Meyer v. Kalanick, 200 F. Supp. 3d 408, 422 (S.D.N.Y. 2016) (finding no consumer consent to the Uber EULA at the point of alleged formation).

example, some IoT companies have allegedly threatened to deactivate or "brick" devices unless a consumer assents to contract changes relating to data privacy and information sharing.[452] In IoB contexts, that potentially bricked device may be embedded in a body, and may control physical functionality of that body. In such cases, judges are likely to struggle with denying recourse to harmed plaintiffs,[453] at least in equity[454] if not in contract.

Doctrinal approaches to addressing these harms may hinge upon a reinvigoration of formation doctrines around voidability of agreements for formation defects such as coercion/duress and undue influence, as well as strengthening the enforcement doctrines around procedurally and substantively unconscionable terms.[455] However, IoT and IoB contracting contexts impact not only state contract law but also "contract-adjacent," product-specific state consumer protections laws,[456] as well as the practical impact of state data breach notification laws.[457] These state-specific consumer protection regimes present an accessible starting point for buttressing consumer protection. States can strengthen disclosure obligations not only around the occurrence of data breaches but also pre-breach at point of product purchase, in particular creating implied warranties of

---

452. For a recent controversy, see Zack Whittaker, *Sonos Says Users Must Accept New Privacy Policy or Devices May "Cease to Function,"* ZDNET (Aug. 21, 2017, 11:00 PM), http://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/ [https://perma.cc/7SVE-JCBR].

453. Courts have struggled with the quantification of privacy harms. Bruce E. Boyden, *Can a Computer Intercept Your Mail?*, 34 CARDOZO L. REV. 669, 713 (2012) (discussing the difficulties of calculating privacy harms under the Wiretap Act).

454. For a discussion of equity first principles, see C.C. Langdell, *A Brief Survey of Equity Jurisdiction*, 1 HARV. L. REV. 355, 358 (1888).

455. *See* Matwyshyn, *supra* note 449, at 554-55, 554 n.119.

456. Andrea M. Matwyshyn, *Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*, 84 CHI.-KENT L. REV. 713, 727 (2010) ("In addition to the FTC Act, many states have consumer fraud laws, known as the "Little FTC Acts," that often authorize private citizens to recover damages and attorney fees for loss resulting from the merchant's deceptive practice. The remedies under state and local consumer fraud laws are often stronger than those under similar federal statutes; they also apply to more seller practices than do federal laws.").

457. Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI. & TECH. L. 450, 487 (2018) (arguing in favor of creating "uniformity in data breach notification and the option of a single point of public filing, while respecting states' rights to vary regarding enforcement").

security and privacy in every EULA,[458] and statutorily deeming of certain types of consumer recourse and liability to be nonwaivable.

b. Criminal Law and the Third-Party Doctrine

Questions of the relationship between IoB EULAs and the human body become particularly critical in criminal law contexts.[459] Again, prosecutorial use of the third-party doctrine and IoT data streams present an instructive model.[460] But the direct interaction of IoB and criminal contexts has also already begun: a recent criminal prosecution for insurance fraud expressly relied on IoB-derived evidence. The case illustrates one aspect of the doctrinal and constitutional questions under the Fourth and Fifth Amendments involving IoB:[461] in 2017, in an Ohio prosecution of a defendant accused of aggravated arson, the court admitted IoB pacemaker data obtained from the defendant's pacemaker company.[462] This case also serves as a reminder that the Supreme Court has already identified the need for evolution of the third-party doctrine in light of the changing nature of technology.[463]

Thus, complex questions lie at the intersection of consensual IoB data sharing and criminal law. Is the data cocreated by the defendant's body? Is an IoB device that simply extrudes a feed of physical evidence akin to a fingerprint that can be compelled by police

458. For a discussion of the potential effectiveness of implied warranties of security and privacy in state contract law, see, for example, Matwyshyn, *supra* note 330, at 1183 & n.495.

459. For a discussion of evolving criminal law standards in technological context, see Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 127 (2018).

460. *See, e.g.*, Colin Dwyer, *Arkansas Prosecutors Drop Murder Case that Hinged on Evidence from Amazon Echo,* NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo [https://perma.cc/V4RH-ZGFW].

461. *See, e.g.*, *Judge Rules Pacemaker Data Admissible in Court*, BBC NEWS (July 13, 2017), http://www.bbc.com/news/technology-40592520 [https://perma.cc/2RF4-D6 CS]; Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You.*, CHI. TRIB. (Oct. 9, 2017, 7:48 PM), http://www.chicagotribune.com/news/nationworld/ct-fitbit-key-fob-pacemaker-crime-20171009-story.html [https://perma.cc/K3QX-CHZX].

462. *Judge Rules Pacemaker Data Admissible in Court*, *supra* note 461. The defendant faced aggravated arson charges. *Id.* He claimed that "he was woken by a fire at home, packed a case, broke a window and threw out the bag. A cardiologist told police his explanation was 'highly improbable' based on his heart rate and cardiac rhythms at the time." *Id.*

463. United States v. Jones, 565 U.S. 400, 417-18 (2012) (Sotomayor, J., concurring).

without constitutional concerns?[464] Or, perhaps, this live data feed is better considered testimonial evidence subject to a higher level of judicial scrutiny, particularly if the IoB device in question is a third-generation IoB device directly connected to a human brain (and, therefore, raising obvious freedom of thought-autonomy concerns)?[465] Is the real-time location acquisition of the IoB device akin to location data collected from a tracking device attached to the underside of a suspect's car[466] or historical cell-site location?[467] These questions of criminal law will be more thoroughly addressed in a subsequent article.

4. Intellectual Property

Perhaps one of the most formidable and undertheorized obstacles to IoB consumer protection will arise with respect to enforcement of intellectual property rights by third parties in second- and third-generation IoB bodies.[468]

a. Patent

The Internet of Bodies sets up a collision between users' physical security/bodily integrity on the one hand and patent law on the other. Indeed, the current wave of software patent litigation is unlikely to spare IoB devices. In particular, patent assertion entities[469] are likely to begin eyeing IoB patents for acquisition.[470]

---

464. *See* Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 366-76 (2012).

465. *Id.* at 371-75.

466. *See* Stephanie K. Pell, Jones*ing for a Privacy Mandate, Getting a Technology Fix-Doctrine to Follow*, 14 N.C. J.L. & TECH. 489, 496-97 (2013).

467. *See Fourth Amendment—Third-Party Doctrine—Fourth Circuit Holds that Government Acquisition of Historical Cell-Site Location Information Is Not a Search.*—United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc)*, 130 HARV. L. REV. 1273, 1273-76 (2017).

468. *See* Jeanne C. Fromer, *The Compatibility of Patent Law and the Internet*, 78 FORDHAM L. REV. 2783, 2783 (2010) ("[H]ow, if at all, patent law and the Internet's values are compatible is undertheorized.").

469. Indeed, a portion of Internet of Bodies patents will likely end up in the portfolios of patent assertion entities—follow-on owners of patents sometimes known as "patent trolls" that make a business out of maximal patent-rights enforcement. *See* Mark A. Lemley & A. Douglas Melamed, *Missing the Forest for the Trolls*, 113 COLUM. L. REV. 2117, 2118-20 (2013).

470. IoB patents potentially provide greater leverage for patent assertion entities to extract settlements out of alleged infringers, as the public relations consequences and consumer trust outcomes might be more negative for the alleged infringer than in a usual technology

For example, consider second-generation IoB such as an eyeball-injectable, "smart" contact lens, a concept already patented by major technology companies.[471] Imagine that an injected contact lens maker is sued by a patent assertion entity alleging that the code that operates the lens infringes a patent it holds. While some IoB manufacturer defendants might be able to afford to settle, many would not; neither could they afford protracted litigation. But even assuming the defendant litigates, a court may decide that the technology is infringing, in which case, the manufacturer may not be allowed to—or financially able to—continue providing its services. Consumers with the allegedly infringing lens already injected into their eyeballs would lose twice in this scenario: once because they purchased and injected the lenses (in reliance upon a now discontinued service) and a second time because their eyes now have injected lenses in them that no longer function (which means that the consumer faces costs and physical risks of lens removal). Unlike any other recreational products implicated by patent judgments that consumers might have previously experienced, an infringing second- or third-generation IoB device will involve potentially removing hardware from the inside of their bodies.

Indeed, IoB patent questions will intersect with doctrinally complex "legacy" questions in patent law, and preservation of bodily security and autonomy may present the next frontier for patent law reform.[472] IoB will catalyze the need for resolution of prior open questions in patent law, in particular the deeply uncertain legal status of software patentability (despite multiple attempts at clarification)[473] and the patentability of follow-on discoveries from

---

patent situation. *See id.* at 2126-27.

471. *See supra* notes 217-24 and accompanying text.

472. In particular the debate over patentability of living things, exhaustion, and accidental infringement has caused much law review discussion. *See, e.g.*, Daryl Lim, *Self-Replicating Technologies and the Challenge for the Patent and Antitrust Laws*, 32 CARDOZO ARTS & ENT. L.J. 131, 133-37 (2013) (discussing Bowman v. Monsanto Co., 133 S. Ct. 1761 (2013)); Evan H. Tallmadge, *Patenting Natural Products After* Myriad, 30 HARV. J.L. & TECH. 569, 573-75 (2017) (discussing Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107 (2013)).

473. For a discussion of software patentability see, for example, Lemley & Melamed, *supra* note 469, at 2119-20 (explaining that although patent trolls "now [are] a majority of all patent assertions in the country and ... win both larger judgments and larger settlements than do ... [firms] that practice patents ... despite complaints that they often assert weak patents," there are also more complex patent dynamics at work); Greg R. Vetter, *Patent Law's*

human bodies.[474] Yet, the extent to which intellectual property holders should hold sole control over the disposition of an IoB device once implanted in a body is relatively new territory for courts. A harbinger for concern is again visible in IoT contexts, where courts have sometimes sided with patent holders, forcing companies to disable allegedly infringing functionality.[475] If courts analyze IoB patents in similar ways, they will increasingly be forced to choose whether to cause the bricking of body parts or brain functionality, to direct the specific performance of invasive surgery to remove allegedly infringing intellectual property from IoB bodies, or, instead, to construct some sort of approach that acts as a compulsory patent licensing regime for IoB devices.[476]

The most aggressive courts might even consider some IoB consumers to constitute patent infringers themselves. As Professor Gaia Bernstein warns, consumer "[e]nd users are likely to become even more prevalent in patent litigation" and they are "at a significant disadvantage in patent disputes," particularly when patent assertion entities are influencing the patent landscape.[477] Meanwhile, Professors Julie Cohen and Mark Lemley warn that patent law might be used as a sword not only in stopping infringing use but also potentially in stopping reverse engineering, a process that will frequently be used to assess IoB safety by both security experts and consumers.[478]

Unpredictability Doctrine and the Software Arts, 76 MO. L. REV. 763, 766-67 (2011) (arguing that "the progression of software technology since the time of the precedent influencing enablement for software patents suggests a failure by the law to recognize the changes in the technology").

474. *See* Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 480-82, 493-94 (Cal. 1990), *cert. denied*, 499 U.S. 936 (1991).

475. These holders have included patent assertion entities. John O'Brien, *Use Your Phone to Schedule Your Comcast DVR? Not Anymore, After Ruling in Patent Dispute,* FORBES (Nov. 22, 2017, 10:16 AM), https://www.forbes.com/sites/legalnewsline/2017/11/22/use-your-phone-to-schedule-your-comcast-dvr-not-anymore-after-ruling-in-patent-dispute/#2a076b886141 [https://perma.cc/B6PG-J5M8].

476. Courts have also sometimes been unforgiving when companies attempt to design around an injunction. *See, e.g.*, Bernard H. Chao, *After* eBay, Inc. v. MercExchange*: The Changing Landscape for Patent Remedies*, 9 MINN. J.L. SCI. & TECH. 543, 562-64 (2008); Conrad Gosen, Note, TiVo, Inc. v. EchoStar Corp.*: Providing Clarity to Contempt Proceedings in Patent Cases*, 27 BERKELEY TECH. L.J. 273, 273 (2012).

477. Gaia Bernstein, *The Rise of the End User in Patent Litigation*, 55 B.C. L. REV. 1443, 1446 (2014).

478. Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software*

In particular, the history of medical procedure patent litigation provides a cautionary tale of how patent litigation might harm the security and autonomy of IoB bodies. In the 1990s, a doctor was sued by a patent holder for performing an allegedly infringing but medically necessary procedure on a patient.[479] After public outcry, in 1997, Congress statutorily limited the ability of medical procedure patent holders to recover patent damages related to a medical practitioner's performance of a medical activity.[480] Similar congressional intervention may lie in the Internet of Bodies' future, rebalancing patent rights and bodily security.

b. Copyright

In contrast to patent law, legal debates around IoT and security have already crafted a new balance between consumer protection of IoB bodies and copyright. In 2015, the Copyright Office and Librarian of Congress granted an exemption to Section 1201 of the Digital Millennium Copyright Act (DMCA) that expressly allows security analysis of code in IoT devices and, consequently, IoB devices.[481] As long as this exemption continues to remain in effect[482] (or, preferably, if Congress follows the suggestion of the Copyright Office and amends the DMCA to make the exemption permanent)[483] most consumer protection research on IoB devices will not face dispositive obstacles from copyright.[484] Yet, these policy battles have

---

Industry, 89 CALIF. L. REV. 3, 56 (2001) ("Because software must be reverse engineered to be understood, the patent law's failure to provide a reverse engineering privilege may pose unique difficulties for software research.").

479. Julianne Befeler, *Seeking a Better Prescription for Physicians: Patent Eligibility for Diagnostic Methods in a Post*-Bilski *and* Prometheus *Era*, 35 SETON HALL LEGIS. J. 484, 510 (2011) (noting that Congress's initial refusal was overcome by "public outrage over a surgical patent lawsuit" that "sparked reform").

480. 35 U.S.C. § 287 (2000).

481. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944 (Oct. 28, 2015) (codified at 37 C.F.R. pt. 201).

482. The exemption stipulates that those devices must not be, for example, already attached to a human body and not in operation. *Id.* at 65956. Therefore, some analysis of IoB devices may fall outside the protected scope of DMCA security research conduct. *See id.*

483. The Copyright Office has encouraged Congress to amend the DMCA and adopt a permanent version of this exemption. U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17, 73-74 (June 2017), https://www.copyright.gov/policy/1201/section-1201-full-report.pdf [https://perma.cc/29SE-DLLL].

484. Until the granting of this exemption, however, merely testing the functionality of code

also demonstrated that medical device companies and other manufacturers of IoT and IoB products have traditionally taken an aggressively copyright-maximalist stance.[485] However, presuming that the DMCA Section 1201 security research issue is at least temporarily addressed, the primary remaining copyright issue pertains to the copyrightability of databases of personally identifiable information extracted from IoB devices.

The extent of copyrightability of databases has presented division in the legal scholarship.[486] Professor James Boyle has argued that "in copyright law—to a greater extent than in most other fields of legal doctrine—there is a routine *and acknowledged* breakdown of the simplifying assumptions of the discourse, so that mundane issues force lawyers, judges, and policymakers to return to first principles."[487] Indeed, the challenges IoB introduce will force a return to a first principles analysis, particularly with respect to questions of database copyright and body-internal data streams.[488]

Professor Boyle also argues that by disaggregating an idea from its expression, it becomes possible—at least in theory—to both give

---

in IoB devices for patient safety potentially subjected patients and researchers to copyright sanction. *See* Jay Radcliffe, Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, https://cdn.loc.gov/copyright1201/2015/comments-020615/InitialComments_ShortForm_Radcliffe_Class25.pdf [https://perma.cc/AN8M-UDLC] (explaining that as much as 40 percent of code in medical devices remains untested by security experts due to fear of copyright law consequences).

485. *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Round 2 of Comments (Opposition Comments)*, U.S. COPYRIGHT OFFICE, https://www.copyright.gov/1201/2018/comments-021218/ [https://perma.cc/W57S-BXZ9]; *see, e.g.*, Shaye Mandle, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, https://www.copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf [https://perma.cc/QBH8-H2R3].

486. For a discussion of the debate over copyrightability of databases, see, for example, Daniel J. Gervais, *The Protection of Databases*, 82 CHI.-KENT L. REV. 1109, 1157 (2007) ("[S]ome forms of restriction sought by database owners almost as knee-jerk attachment to 'property' may not, in the end, be in their own interest."); James Gibson, *Re-Reifying Data*, 80 NOTRE DAME L. REV. 163, 167 (2004) ("The most controversial aspect of the pro-expansionists' reaction to the digital dilemma, however, has been a combination of the technological and the legislative—an approach one might call 'technolegical,' as it involves the *legis*lative regulation of *techno*logical behavior in the market for information goods."); Jacqueline Lipton, *Balancing Private Rights and Public Policies: Reconceptualizing Property in Databases*, 18 BERKELEY TECH. L.J. 773, 775-82 (2003) (arguing that creating private property rights in databases will not inevitably lead to commercial and social problems).

487. JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 19 (1996).

488. *See id.*

the idea to the public while offering rights over the expression to the writer.[489] Yet, when the "writer" in question is your Internet-connected pancreas mediated by software written by a third party, courts will perceive themselves to be faced with hard choices in the attribution of rights in the databases created from IoB streams of extracted data, as well as rights in the information from their subsequent analysis.[490] In the context of IoB, the issues are further complicated through the interaction with the law of secured transactions and bankruptcy. However, as a starting point, judicial determinations of copyright impacting IoB should follow the model of the Copyright Office in the granting of the DMCA consumer products security research exemption: they should consider consumer protection concerns as a counterweight to maximalist copyright interpretation.[491] These topics, along with their corollary issues from secured transactions and bankruptcy, are the subject for a companion essay to this Article.

5. Secured Transactions and Bankruptcy

Imagine the situation where a bankruptcy court debates the sale of contract rights and databases in the bankruptcy estate of, for example, the company that provided your IoB injected contact lenses or your brain prosthetic device.[492] There would be no shortage of prospective purchasers for these assets. For example, insurance providers might be interested in purchasing IoB contract rights in order to monitor consumer behavior in real time to better predict

489. *Id.* at 18-19.

490. *See id.*

491. As Professor Boyle has argued, "[t]o say that a particular advantage may not be exploited in one area does not commit us to the view that it may not be exploited in another." *Id.* at 85.

492. For a company without many physical assets, the most valuable asset that the company would offer in bankruptcy to satisfy its creditors would be its contractual relationships with its users and its extensive database of personally identifiable consumer information. *See* Katherine J. Clayton, Comment, *Liquidating a Technology Company in Bankruptcy*, 4 N.C. J.L. & TECH. 169, 170-71 (2002). Although various consumers will have implemented dramatically different preferences with respect to privacy settings, a court is unlikely to be interested in interpreting privacy preferences with that degree of granularity. *See supra* notes 122-53 and accompanying text.

risk and premiums—perhaps parallel to the way that some insurers now monitor driving behavior with IoT devices installed in cars.[493]

It is unlikely that the drafters of the Bankruptcy Code imagined that debtor estates could directly impact physical security and integrity of consumers' bodies, but contract rights of remote access into devices and rights of real-time monitoring of IoB devices raise precisely these concerns. Bankruptcy statutes currently allow courts to approve the transfer of personally identifiable consumer information in a manner consistent with the debtor's privacy policy.[494] Alternatively, the court may choose to appoint a "privacy ombudsman," but this ombudsman is not necessarily a consumer advocate.[495] While creditor rights are key to funding innovation, this protection cannot and should not come at the expense of consumer protection, bodily safety, and autonomy.[496] Although the FTC has occasionally intervened in bankruptcies with sensitive databases, as it did in the *ToySmart*,[497] *Borders*,[498] *XY Magazine*,[499] and *ConnectEDU*[500]

493. Cherise Threewitt & John M. Vincent, *How Do Those Car Insurance Tracking Devices Work?*, U.S. NEWS & WORLD REP. (Feb. 26, 2018), https://cars.usnews.com/cars-trucks/car-insurance/how-do-those-car-insurance-tracking-devices-work [https://perma.cc/V959-TWY6].

494. Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), Pub. L. No. 109-8, 119 Stat. 23, 73-74 (2005).

495. In particular, courts sometimes refuse to appoint ombudsmen, and the law fails to offer any guidance with respect to derivative or "tethered" consumer databases of body-connected information. *See id.*

496. Even assuming that the dignitary arguments around crafting a private space of breathing room do not prove convincing, selling off databases of consumer information offers an unsustainable stream of assets. *See* Clayton, *supra* note 492. Because information is valued based on its scarcity, after a certain number of bankruptcies that implicate consumer databases, the market will become saturated with information about particular consumers. *See id.*

497. Press Release, U.S. Fed. Trade Comm'n, FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), https://www.ftc.gov/ news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding [https://perma.cc/BAY4-QNEK].

498. Press Release, U.S. Fed. Trade Comm'n, FTC Seeks Protection for Personal Customer Information in Borders Bankruptcy Proceeding (Sept. 21, 2011), https://www.ftc.gov/news-events/press-releases/2011/09/ftc-seeks-protection-personal-customer-information-borders [https://perma.cc/YE3D-WENN].

499. Letter from David C. Vladeck, Dir. Bureau Consumer Prot., U.S. Fed. Trade Comm'n, to Peter Larson & Martin E. Shmagin (July 1, 2010), https://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf [https://perma.cc/R35Q-WUTL].

500. Press Release, U.S. Fed. Trade Comm'n, FTC Seeks Protection for Students' Personal

bankruptcies, agency resource constraints mean that FTC intervention will not be possible in every IoB situation.[501] Indeed, these concerns with IoB bankruptcies have already begun. For example, a first-generation IoB fitness company recently filed for liquidation of its assets.[502]

A first step toward recalibrating this balance in bankruptcy involves amending the definitions of UCC Article 9 to expressly exclude databases of raw IoB-collected data from their scope.[503] A second step may include amending the responsibilities of the bankruptcy trustee, charging the trustee with weighing consumer protection concerns on par with those of secured creditors, and essentially creating the equivalent of an automatically perfecting "phantom"[504] security interest for consumers in their IoB information.[505] Consequently, the privacy ombudsman and the FTC become merely a check and balance on the bankruptcy trustee in the handling of consumer protection, rather than the primary method of consumer protection intervention.[506] A third step might involve amending the Bankruptcy Act to require explicit reaffirmation of consumer consent to each transfer of functional control over IoB contract rights with a consumer right to termination that includes information deletion and discontinuation of body tracking.[507]

Information in Education Technology Company ConnectEdu's Bankruptcy Proceeding (May 23, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-seeks-protection-students-personal-information-education [https://perma.cc/ZP5X-PRVS].

501. *See supra* note 373 and accompanying text.

502. Steve Kovach, *Fitness-Tracking Company Jawbone, Once Worth $3 Billion, Is Shutting Down and Liquidating Its Assets*, BUS. INSIDER (July 6, 2017, 6:54 PM), http://www.businessinsider.com/jawbone-shutting-down-liquidating-assets-2017-7 [https://perma.cc/GA9J-SPUZ].

503. For a discussion of Article 9's scope, see, for example, Xuan-Thao N. Nguyen, *Collateralizing Privacy*, 78 TUL. L. REV. 553, 574-77 (2004).

504. The idea of a phantom interest arises from the securities context. For a discussion of phantom interests, see, for example, Note, *Phantom Stock Plans*, 76 HARV. L. REV. 619, 619, 622-23 (1963).

505. The idea of automatic perfection is not novel. Secured transactions law addresses purchase-money security interests in consumer goods in this manner. By removing the filing requirement, the consumer's interests can be protected without imposing any logistical burden on consumers. For a discussion of PMSI, see, for example, Alan M. Christenfeld & Aleksandra Kopec, *Purchase-Money Security Interests*, 41 U.C.C. L.J. 291, 292-94 (2009).

506. Professor Xuan-Thao Nguyen has argued in favor of altering the regime of financing statements. Nguyen, *supra* note 503, at 585-87.

507. Peppet, *supra* note 444, at 160-64.

While each of these proposed regulatory and legal approaches will construct a more trusted set of consumer baselines for second-generation IoB, the legal challenges presented by third-generation IoB run deeper. They force us to revisit the unsettled questions of an individual's interests in her own body and the deeper question of whether the human body is a construct to be preserved or replaced in an age of technological innovation.

II. KANTIAN HEAUTONOMY

Neo: Why do my eyes hurt?
Morpheus: You've never used them before.[508]

The prior Parts introduced IoB and explained how legacy problems from IoT threaten the confidentiality, integrity, and availability of human bodies.[509] However, the basic legal inquiry of the extent to which a person is entitled to an inalienable legal default of control over her own body underpins their legal analysis. In other words, while the technologies of IoB are new, questions of control over the human body are not new to legal scholarship and jurists. Nevertheless, in a world of IoB, our traditional propertized debates over body "ownership" and, more importantly, the underlying framework of Kantian autonomy will no longer cleanly fit the technical realities shaping our legal conversations. As concrete physical harms to human bodies and minds caused by IoB begin to emerge, this mismatch of past legal discourse with the reality of harm will become obvious, particularly in our discussions of the desirability and regulation of third-generation IoB.

A. Why Autonomy Fails with IoB

In an iconic article setting forth the dominant analytic paradigms for the human body, Professor/Judge Guido Calabresi asked a seemingly simple question: do we own our bodies?[510] As his scholarly discussion unfolded, Calabresi took his readers on an

508. THE MATRIX, *supra* note 2.

509. *See supra* Part I.B.

510. Guido Calabresi, *An Introduction to Legal Thought: Four Approaches to Law and to the Allocation of Body Parts*, 55 STAN. L. REV. 2113, 2113-14 (2003).

intellectual journey using this question of body "ownership" to highlight the existence of four distinct analytical approaches used by legal scholars—doctrinalism, functionalism, legal process, and law and status—and posited how each would answer the question of whether humans own their own bodies.[511]

Calabresi offers a valuable articulation of body "ownership" interests that particular scholars are likely to consider—autonomy, insights from other disciplines, institutional capacity, and exploitation risks.[512] Yet, his underlying question of body "ownership" assumes a legal inquiry framed through the lens of property law.[513] This underlying assumption is worthy of reexamination.

1. Owned Bodies Versus Pwned[514] *Bodies*

Professor Radhika Rao explains that case law frames "property" as a "bundle of rights."[515] "The 'bundle of rights' which has been associated with property includes the rights to possess, to use, to exclude, to profit, and to dispose."[516] Yet, none of these rights exist in the traditional sense in a second- and third-generation IoB body.

Subject to a license agreement in connection with the code inside an IoB device, a user of an IoB device may never fully "possess" the device.[517] The right to use the device is contingent for its user, subject to unilateral alteration or degradation choices by a remote third party—the obsolescence by adhesion dynamic discussed in Section I.B.[518] As explained in the prior discussion of hidden price terms, use may be arbitrarily terminated in the discretion of the device manufacturer in many cases.[519] Exclusion is similarly not entirely possible: manufacturers of IoB devices view the data stream arising from the device[520] as potentially the most lucrative source of revenue

511. *Id.* at 2132-33, 2137, 2144, 2146.

512. *Id.* at 2132-33, 2137, 2144, 2146-47.

513. *Id.* at 2151.

514. *What Does 'Pwn' Mean? And How Do You Say It?*, MERRIAM-WEBSTER, https://www.merriam-webster.com/words-at-play/pwn-what-it-means-and-how-you-say-it [https://perma.cc/XV9U-P87Q].

515. Radhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 406 (2000).

516. *Id.* at 405-06 (quoting Brotherton v. Cleveland, 923 F.2d 447, 481 (6th Cir. 1991)).

517. AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP 57-64 (2016).

518. For a recent controversy, see Whittaker, *supra* note 452.

519. *See supra* Part I.B.4.

520. For example, Professor Devin Desai has previously examined the tensions between

and will harvest it as long as the device is in use, regardless of the desires of the user.[521] Through repackaging and selling (access to) this information to "trusted partners" (whose identities are rarely disclosed to the human attached to the IoB device), exclusion of others by the consumer is functionally impossible as long as the IoB device is in use.[522] Similarly, if the device is a medically prescribed IoB device such as a pacemaker, discontinuation of use is not a real option. Most consumers are not Vice President Cheney—they lack the bargaining power to demand alteration of technical functionality.[523] Disposition presents a similar problem: once the information streams generated by the IoB device are collected, the manufacturer has no incentive to dispose of them, and the IoB user cannot legally demand that the collected data be deleted under current U.S. law in almost all cases.[524] Further, the legal status of these data streams is unclear as a protectable user interest.[525] Even in purely physical body disposition situations, scholars highlight that the common law has always been divided and contradictory.[526] Indeed, as Professor Kara Swanson has explained, particularly on the point of finding property interests in body products such as blood, eggs, and semen, courts have demonstrated confusion and have been inconsistent in their findings.[527] Partially due to this doctrinal confusion, the Supreme Court tends to frame discussions of the body in ways that consciously avoid the body-propertization conversation.[528]

---

property and privacy with respect to implantable devices. *See* Devin Desai, *Privacy? Property?: Reflections on the Implications of a Post-Human World*, 18 KAN. J.L. & PUB. POL'Y 174, 176 (2009) ("For the purposes of this essay, however, I will focus on one key aspect of the investigation: how the advent of machine enhanced humans requires us to look at the relationship between property and privacy.").

521. For a discussion of data valuation from a corporate perspective, see, for example, Andrea M. Matwyshyn, *Privacy, the Hacker Way*, 87 S. CAL. L. REV. 1, 22-23 (2013).

522. Desai, *supra* note 520, at 179-80.

523. Dick Cheney's ability to obtain technical changes to his pacemaker was an unusual occurrence. Dan Kloeffler & Alexis Shaw, *Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger.'* ABC NEWS (Oct. 19, 2013, 10:27 AM), https://abcnews.go.com/US/vice-president-dick-cheney-feared-pacemaker-hacking/story?id=20621434 [https://perma.cc/KY3V-5TG2].

524. *See* Matwyshyn, *supra* note 521, at 2-3.

525. *See id.*

526. Rao, *supra* note 515, at 405-09.

527. *See generally* KARA W. SWANSON, BANKING ON THE BODY: THE MARKET IN BLOOD, MILK, AND SPERM IN MODERN AMERICA (2014).

528. *See* Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 487-89 (Cal. 1990). *See gen-*

But perhaps the most fundamental incompatibility between a world of IoB bodies and property frameworks arises because of security issues.[529] Property paradigms *assume* the knowability of the bundle of rights and risks that are being traded and that those bundles can be meaningfully constrained through the legal act of alienation or license.[530] The security realities of IoB devices render this knowability functionally impossible—a third-party attacker may stealthily usurp both parties' control over an IoB device.[531] Further, IoB security issues will always simultaneously be public safety and public health issues as well as private interests. The problem of "reciprocal security vulnerability"—the fact that private and public security concerns are inextricably entwined[532]—again renders property paradigms a poor fit for IoB bodies.

But why then are so many legal scholars drawn to this suboptimally fitting intellectual frame of property law? The answer may lie in part in their search for the strongest possible doctrinal hook for notions of bodily autonomy.[533] Indeed, an analysis of IoB's impact on autonomy yields yet another layer of concerns for freedom of thought, freedom of speech, and the future of deliberative democracy.

2. Autonomy Versus Heautonomy

As explained by Professor Robert Merges, "[p]roperty theorists identify autonomy[534] as perhaps the chief value inculcated by

---

erally SWANSON, *supra* note 527.

529. *See supra* Part I.B.3.

530. Rao, *supra* note 515, at 405-06.

531. *See supra* Part I.B.3.

532. For a discussion of the problem of reciprocal security vulnerability, see Matwyshyn, *supra* note 330, at 1121-25.

533. As explained by Professor Margaret Radin,

> Conservatives rely on an absolute conception of property as sacred to personal autonomy. Communitarians believe that changing conceptions of property reflect and shape the changing nature of persons and communities. Welfare rights liberals find entitlement to a minimal level of resources necessary to the dignity of persons even when the entitlement must curtail the property rights of others.

Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 957-58 (1982). Another reason may arise in their falling victim to the "economic value fatalism" which asserts that in order to protect something, one must propertize it. Matwyshyn, *supra* note 521, at 14-15.

534. *See generally* Bruce J. Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. REV. 1705, 1707-15 (1992) (examining justifications for valuing autonomy).

individual ownership rights."[535] This concept of autonomy is often framed in reference to the work of Immanuel Kant.[536] Legal scholars often define Kantian notions of autonomy in reliance on his work in *Groundwork of The Metaphysics of Morals*[537] and Kant's frame in the first two Critiques—the *Critique of Pure Reason*[538] and *Critique of Practical Reason*.[539] In *Metaphysic of Ethics*, Kant explains that "the concept of freedom is the key that explains the autonomy of the will."[540] With this direct textual connection to a discussion of governance and notions of freedom, legal and philosophical scholarship has understandably focused heavily on Kantian autonomy and how it intersects with law.[541] This Kantian notion of autonomy has permeated not only property law but legal scholarship generally.[542]

Pierre Bourdieu and other noted scholars[543] have amply critiqued Kant's work, and legal scholars have framed the Kantian person as "simply an abstract autonomous entity capable of holding rights, a device for abstracting universal principles and hence by definition devoid of individuating characteristics."[544] However, when exploring Kant's later writings and the corresponding explanatory work of

---

535. Robert P. Merges, *To Waive and Waive Not: Property and Flexibility in the Digital Era*, 34 COLUM. J.L. & ARTS 113, 117 (2011).

536. For a discussion of Kantian autonomy see, for example, J.M. Finnis, *Legal Enforcement of "Duties to Oneself": Kant v. Neo-Kantians*, 87 COLUM. L. REV. 433, 434 (1987).

537. Immanuel Kant, *Groundwork of The Metaphysics of Morals*, *in* PRACTICAL PHILOSOPHY 37 (Mary J. Gregor ed., 1999).

538. IMMANUEL KANT, CRITIQUE OF PURE REASON 464-66 (Norman Kemp Smith trans., 1964).

539. IMMANUEL KANT, CRITIQUE OF PRACTICAL REASON 29-32 (Werner S. Pluhar trans., Hackett Publ'g Co., Inc. ed. 2002) (1788).

540. Kant, *supra* note 537, at 94. Kant continues,

> *Will* is a kind of causality belonging to living beings in so far as they are rational, and *freedom* would be this property of such causality that it can be efficient, independently on foreign causes *determining* it; just as *physical necessity* is the property that the causality of all irrational beings has of being determined to activity by the influence of foreign causes.

Id.

541. For a discussion of Kant's vision of the relationship of morality to law, see generally George P. Fletcher, *Law and Morality: A Kantian Perspective*, 87 COLUM. L. REV. 533 (1987).

542. Kantian autonomy has also been an animating argument of First Amendment scholarship. For a discussion of First Amendment scholarship on Kantian autonomy, see generally Christina E. Wells, *Reinvigorating Autonomy: Freedom and Responsibility in the Supreme Court's First Amendment Jurisprudence*, 32 HARV. C.R.-C.L. L. REV. 159 (1997).

543. Koenraad Geldof, *Authority, Reading, Reflexivity: Pierre Bourdieu and the Aesthetic Judgment of Kant*, 27 DIACRITICS 20, 24-26 (1997).

544. Radin, *supra* note 533, at 971.

philosophers, the theoretical underpinnings of Kantian autonomy become more complex than many legal scholars might perhaps expect.

Kant's framing of the *precedential conditions* for autonomy help to highlight the overarching legal and democratic concerns introduced by IoB. Specifically, the key precedential condition for Kantian autonomy is what Kant calls *heautonomy*. Heautonomy has been unexplored[545] by legal scholars in the law review literature.[546] The *Third Critique of Judgment*, where the term appears,[547] may appear initially to offer a less apposite text for law than his other work as it addressed the process of "common sense" judgment of the aesthetic and teleology.[548] Nevertheless, it is here in the *Third Critique* that Kant offers a more complex picture of autonomy's prerequisites.[549] And for purposes of an analysis of IoB, because Kant clearly intended this discussion of heautonomy to impact analyses of both "aesthetics and teleology" specifically,[550] the concept is particularly well-suited. As prior Parts have argued, IoB is not only medical; it also includes voluntary technological self-augmentations[551] done for aesthetic reasons.[552] For these reasons, the concerns embodied in Kantian heautonomy offer an important warning and a good fit for a legal critique of IoB.

---

545. The reason for this deficit of exploration may arise from philosophy's more limited engagement with the source of the discussion—Kant's *Third Critique of Judgement*. *Kant's Third Critique of Judgment* has been extensively referenced in art criticism theory despite its comparatively less popular status in legal and philosophy circles. *See, e.g.*, Diarmuid Costello, *Greenberg's Kant and the Fate of Aesthetics in Contemporary Art Theory*, 65 J. AESTHETICS & ART CRITICISM 217, 221, 225-26 (2007).

546. A search in Westlaw on heautonomy yields four results—an introduction to a symposium and three articles written by philosophers. Westlaw Search for Heautonomy, WESTLAW, https://1.next.westlaw.com [https://perma.cc/RCG6-REV4] (typing "heautonomy" in search bar, then pressing the search button). Based on these results, it appears no legal scholar has ever engaged deeply with the philosophical construct of heautonomy. *See id.*

547. Heautonomy only appears in the *Third Critique of Judgment* and only in the introduction. Juliet Floyd, *Heautonomy: Kant on Reflective Judgment and Systematicity*, *in* KANT'S AESTHETICS 193 (1998).

548. *Id.*

549. *See id.*

550. *Id.* at 195.

551. *See* discussion of Professor Mann, *supra* Part I.B.2.

552. As the introductory material on one IoB self-augmentation website describes it, "[t]he reason is simple. Adding more senses will make you smarter and result in a richer life experience." *The North Sense*, CYBORGNEST, https://cyborgnest.net [https://perma.cc/9CZD-4A7B].

In his introduction to the *Third Critique of Judgment*, Kant explains the critical nature of the distinction between autonomy and heautonomy: "The Judgment has therefore also in itself a principle *a priori* of the possibility of nature, but only in a subjective aspect; by which it prescribes, not to nature (autonomy), but to itself (heautonomy) a law for its reflection upon nature."[553] The distinction between Kantian autonomy and Kantian heautonomy has been described thus—autonomy refers to "acting freely according to one's form,"[554] but in contrast, heautonomy refers to "being the source of the form according to which one acts ... literally self self-governing."[555] While autonomy is the third-party viewable manifestation of freedom, heautonomy is the internal manifestation of freedom—the capacity of reflective judgment and self-self-governance, uncorrupted by involuntary inputs and unsurveilled.[556] Heautonomy is the "self-applicability of judgment's a priori principle."[557] It is this process of heautonomy[558] which, for Kant, underpins any externally visible exercise of freedom through subsequent autonomy.[559] In other words, it might be said that for Kant, autonomy is the intersection of the human in context of the rest of the world, while heautonomy is the internal ability of the human to process inputs and set the rules over the self in preparation for these autonomous interactions—a private deliberation.[560] Heautonomy is thus an independent process that occurs in a metaphorical hermetically sealed self, free from pushed influence of third parties.[561] Autonomy exercise follows, contingent upon the outcomes of these heautonomous

553. IMMANUEL KANT, THE CRITIQUE OF JUDGMENT 25 (J.H. Bernard trans., 2000).

554. Lydia L. Moland, *Friedrich Schiller*, STAN. ENCYCLOPEDIA OF PHIL. (Apr. 2017), https://plato.stanford.edu/entries/schiller/ [https://perma.cc/LMC9-Y9CL]. Schiller also uses the term "heautonomy," but uses it to describe the regulative character of aesthetic, not teleological judgment, which materially differs from Kant's usage. Sabine Roehr, *Freedom and Autonomy in Schiller,* 64 J. HIST. IDEAS 120, 120 (2003) ("What is perfect can possess autonomy, in so far as its form is determined purely through its concept; but only beauty possesses heautonomy, because only in beauty is the form determined by the inner nature." (footnote omitted)).

555. Moland, *supra* note 554.

556. *See id.*

557. Floyd, *supra* note 547, at 195.

558. Some philosophy scholars have noted that heautonomy might have been a good model for what Kant initially calls autonomy. PAUL GUYER, KANT 173 (2006).

559. KANT, *supra* note 553.

560. *Id.*

561. *See id.*

deliberations.[562] Consequently, heautonomy is a necessary precursor to any successful exercise of autonomy.[563]

Kant's underlying model for his discussion of heautonomy has been analyzed by philosophers to be "a legal one."[564] Thus, applying the lens of Kantian heautonomy crystallizes that the greatest threat presented by some second- and, in particular, third-generation IoB: the undermining of a human's ability for self-self-governance and, consequently, the undermining of the implicit prerequisites of deliberative democracy. In the world where third parties have a live feed into your senses and your brain, the possibility of truly detached, deliberative internal processes begins to disappear. Every thought and involuntary action could become a "broadcast" by our bodies, sometimes to our detriment. But even more importantly, in a world where we know that IoB devices will end up regularly compromised, the human's own body—as controlled by a remote third-party attacker—may undermine the very inputs and processing upon which heautonomy relies. In other words, some second and third-generation IoB—brain prosthetics and digital cortex interfaces, in particular—create the opportunity (and likely the inevitability) of third-party attacker corruption of human bodies and minds. Consider, for example, a data breach of third-generation IoB devices—a literal brain dump with sensitive information that could victimize impacted consumers on a new level of severity. When we build technologies that allow for owning and pwning[565] of (parts of)

---

562. *See id.*

563. *See id.*

564. One of the most thorough philosophy analyses of heautonomy is offered by Professor Juliet Floyd. Floyd explains that Kant calls this capacity for reflexive judgment "*facultas diiudicandi*" and that Kant

> claims that the capacity to exercise it is really the same as the capacity for making *adjudications* ... of cases in terms of rules. A judge is obliged to render a verdict by applying the rule(s) of law to a particular case. And whenever alternative, conflicting rulings seem plausible, a (good) judge does not make a determination "mechanically" for it is not (good) enough simply to *quote* the law. An *argument* must be given ... whether the case does or does not fall under the auspice of a given rule. In difficult (legal) cases, deliberation is required in order that a determination be made in a non-arbitrary manner.... As Kant writes, by means of the exercise of reflective judgment we "*make the universal concept specific* by indicating the diversity that falls under it, just as teachers of law ... talk about the specification of certain raw material."

Floyd, *supra* note 547, at 199.

565. *See supra* note 513.

human bodies—regardless of whether those rights of access are controlled by the public or the private sector—we risk undermining the process of "self-self-governance" that Kant highlighted as essential to autonomy and freedom.[566]

In this way, third-generation IoB, in particular, has the potential to corrupt the security not only of our bodies and our minds but also the security of the social structures of governance upon which democratic institutions rely. These heautonomous processes have always been the "secret sauce" for enabling robust First Amendment debate and deliberative democratic process. Thus, IoB introduces the technological viability of functionally damaging or perhaps even eliminating what Professor Neil Richards has called "intellectual privacy"[567] and what First Amendment theorists consider to fall within protections for a necessary freedom of thought.[568] In a world where our bodies and minds are connected to a single interconnected technological network, we begin to blur the lines between the freedom of thought, i.e. the physiological and heautonomous event of having a thought internally, and the act of broadcasting curated thoughts through the freedom of speech, i.e. the external autonomous manifestation that follows (or doesn't follow) a thought. This is the distinction between heautonomy and autonomy that IoB potentially threatens.[569] For these reasons, our animating legal principle for IoB should reflect a focus on creating legal structures capable of safeguarding heautonomy and the freedoms that emanate from it.

These legal and ethical choices about the commodifiability, disposition, and disposability of IoB bodies and their impact on

---

566. Moland, *supra* note 554.

567. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 6 (2015) ("Intellectual privacy ... shields the freedom of thought ... and the confidentiality of communications.").

568. Martin H. Redish & Kevin Finnerty, *What Did You Learn in School Today? Free Speech, Values Inculcation, and the Democratic-Educational Paradox*, 88 CORNELL L. REV. 62, 75 (2002) ("Freedom of thought must be protected, because absent free thought the concept of free expression is rendered incoherent[.]").

569. For example, notions of contractual and informed medical consent are already straining as currently implemented. *See, e.g.*, Radhika Rao, *Informed Consent, Body Property, and Self-Sovereignty*, 44 J.L. MED. & ETHICS 437, 438 (2016) (arguing that the "true challenge of informed consent is that this venerable doctrine often functions as a charade, a collective fiction which thinly masks the uncomfortable fact that the subjects of human research are not actually afforded full information").

heautonomy force us to ask a deeply uncomfortable question about our legal baseline assumption: Is the human body an existential construct to be protected and preserved or is it merely an outdated "operating system" or "platform"[570] awaiting an "upgrade"[571] from new technologies? Our answer to this question regarding the value of the human body as a construct will dispositively influence our IoB legal frameworks across areas of law. Therefore, for better or worse, legal scholars and policymakers must confront this somewhat forbidding (and foreboding) question.

B. Humanity—Bug or Feature?

Morpheus: Throughout human history, we have been dependent on machines to survive. Fate, it seems, is not without a sense of irony.[572]

At a recent conference, Professor Judith Rauhofer commented with a thought-provoking question: Will the Internet of Bodies really move society toward communities of autonomous, free-thinking cyborgs?[573] Or, instead, asked Professor Rauhofer, will IoB result in the slow decline of humanity into The Borg?[574] Much like Professor Rauhofer's question, the preceding Parts of this Article leave open a set of significant, unanswered, and uncomfortable social and legal questions. Perhaps the most basic of these open questions asks, "if the technological and legal changes that IoB will introduce are so transformational, does that impact the baselines of what we view as a 'correct' human?" The perhaps unsettling answer is that indeed it may.[575]

While both my own prior scholarship[576] and the work of other scholars[577] have considered some aspects of human-machine

570. Dmitry Paranyushkin, *Body/Mind Operating Systems*, POLYSINGULARITY (Aug. 17, 2016), http://polysingularity.com/ bodymind-operating-systems/ [https://perma.cc/GJ69-FC6Y].

571. *Id.*

572. THE MATRIX, *supra* note 2.

573. CPDPConferences, *CPDP 2018: The Internet of (Vulnerable) Bodies*, YOUTUBE (Feb. 6, 2018), https://youtu.be/10Rlk8uj-lo?t=32m0s [https://perma.cc/F8HP-9ASB].

574. *Id.*

575. I have argued that. *See* Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks*, 11 MINN. J.L. SCI. & TECH. 573, 573 (2010).

576. *Id.*

577. For example, Professor Paul Schwartz has called for a ban on data trade through the use of implantable chips, arguing that "[t]he privacy consequences of implantable chips will

convergence and its regulatory impact, the law review literature has done so in only a limited manner to date.[578] We currently lack a robust legal framework within which to consider social transformations, technological drift, and the human body.

Although the first generation of IoB has only sporadically tested our social norms of "acceptable" and "desirable" optional self-augmentation, nonmedical second- and third-generation IoB will likely do so with uncomfortable regularity. These body-internal and body-melded IoB devices will catalyze a need to craft a shared legal vision for the future of the human body in relation to technology. A spectrum of at least five options for this evolution exist—what we might call a "spectrum of technohumanity."[579] Where we stop on this spectrum will reflect our position on whether the human body is a feature or a bug—whether the human body is a focal point for legal preservation in current form or whether it is merely an antediluvian carbon-based operating system that we need to "upgrade."[580]

Different benchmarks along the scale of technohumanity will result in materially different innovation governance models and legal prescriptions. Yet, perhaps the most difficult question of all for law asks how we govern a society in which we do not all agree on the "correct" benchmark on the scale of technohumanity. For this inquiry on social governance and IoB, we can perhaps glean insights from the work of Bruno Latour. Latour's arguments and their implications for law and social governance will be considered at greater length in the companion essay to this Article, *The Internet of Latour's Things*.[581]

---

be considerable, and no information privacy law at present regulates the terms of such data collection." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2062 (2004); *see also* BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY (2018) (arguing that humans are being trained to behave like machines); Jannice Käll, *A Posthuman Data Subject? The Right to Be Forgotten and Beyond*, 18 GERMAN L.J. 1145, 1152 (2017).

578. The legal literature has not yet explicitly grappled with the issues presented by third-generation IoB to the First Amendment and deliberative democracy in particular.

579. The spectrum ranges from a model of the mechanically extended human, on the one side, to a model of AI simulation theory on the other. *See* Andrea M. Matwyshyn, The Internet of Latour's Things (unpublished manuscript) (on file with author).

580. Paranyushkin, *supra* note 570.

581. *See* Andrea M. Matwyshyn, The Internet of Latour's Things (unpublished manuscript) (on file with author).

CONCLUSION: THE (CYBER)PANCREAS AND THE PANOPTICON

Cypher: You know, I know this steak doesn't exist. I know that when I put it in my mouth, the Matrix is telling my brain that it is juicy and delicious. After nine years, you know what I realize?
[Takes a bite of steak]
Cypher: Ignorance is bliss.[582]

"This is going to be a thing in the future—people just kind of sitting around and staring at blank walls."
—Mark Zuckerberg[583]

This Article has introduced the ongoing progression of the Internet of Things into the Internet of Bodies—a network of human bodies whose confidentiality, integrity, and availability rely at least in part on the Internet and related technologies. First-generation body external IoB devices are already ubiquitous, and second generation body internal devices are arriving presently. Third-generation body-melded IoB devices are currently in development with maturity perhaps less than a decade away.

This Article has argued that IoB devices will suffer from the same categories of security flaws that are currently visible in IoT. However, unlike IoT, IoB technologies will directly, physically harm human bodies and necessitate the evolution of the way that scholars and jurists think about code and the body. A legal paradigm focused on safeguarding Kantian heautonomy as a guiding baseline principle will help mitigate the risk that IoB may corrupt not only individual human bodies but also our body politic.

"*I don't know the future. I didn't come here to tell you how this is going to end. I came here to tell you how it's going to begin.*"
—Neo[584]

---

582. THE MATRIX, *supra* note 2.

583. Zuckerberg, *supra* note 124 (explaining a new Facebook application that allows people to use their phones or other devices to "see" art on blank walls).

584. THE MATRIX, *supra* note 2.