Journal of Business & Technology Law

Volume 16 | Issue 1 Article 5

Regulating the Cyberpunk Reality: Private Body Modification and the Dangers of 'Body Hacking'

Zachary Paul Birnbaum

Regulating the Cyberpunk Reality: Private Body Modification and the Dangers of 'Body Hacking'

ZACHARY PAUL BIRNBAUM*©

I. INTRODUCTION

Private Body Modification ("PBM"), and particularly cybernetic implants, have been contemplated in popular culture and science-fiction for the better part of a century.[1] Possibilities long thought remote and the product of overactive imaginations are now reality such as implanted digital access codes in employees' digits,[2] development of direct brain interfaces,[3] and various functional and cosmetic cybernetic implants.[4] However, Data Privacy protections have not advanced in tandem with these technologies. Neither the United States nor the European Union have adequately addressed the rising issue of PBMs: there is no federal Data Privacy standard in the United States[5] and; Europe's present regulatory framework and

* J.D. Candidate 2021, University of Maryland Francis King Carey School of Law. The author would like to thank his fellow editors at the Journal of Business & Technology Law for their support and dedication in refining his ideas into this paper. The author would also like to thank Prof. Rauschecker for his guidance, and most importantly his wife Libby Dorman, his parents Michel and Gina Birnbaum, and his in-laws Todd and Lisa Dorman for their unconditional love and support, and without whom none of this would have ever been possible.

1. *See* Ed Cumming, *William Gibson: the man who saw tomorrow*, THE GUARDIAN (July 28, 2014), https://www.theguardian.com/books/2014/jul/28/william-gibson-neuromancer-cyberpunk-books; Hari Kunzru, *Dune, 50 years on: how a science fiction novel changed the world*, THE GUARDIAN (July 3, 2015), https://www.theguardian.com/books/2015/jul/03/dune-50-years-on-science-fiction-novel-world; Sean Captain, *HBO's Westworld Creators Talk AI, Sentience, And Surveillance*, FAST COMPANY (Sep. 30, 2016), https://www.fastcompany.com/3063743/hbos-westworld-creators-talk-ai-sentience-and-surveillance.

2. Associated Press, *Cyborgs at work: Swedish employees getting implanted with microchips*, THE TELEGRAPH (Apr. 4, 2017), https://www.telegraph.co.uk/technology/2017/04/04/cyborgs-work-swedish-employees-getting-implanted-microchips/.

3. Tyler Lacoma, *Everything you need to know about Neuralink: Elon Musk's brainy new venture*, DIGITAL TRENDS (Nov. 7, 2017), https://www.digitaltrends.com/cool-tech/neuralink-elon-musk/.

4. Eyder Peralta, *'Body Hacking' Movement Rises Ahead of Moral Answers*, NPR (Feb. 27, 2016), https://www.npr.org/2016/02/27/468366630/-body-hacking-movement-rises-ahead-of-moral-answers; *see generally* Sigal Samuel, *How biohackers are trying to upgrade their brains, their bodies – and human nature*, VOX (Jun. 25, 2019), https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr.

5. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

scheme, the General Data Protection Regulation ("GDPR"), does not address PBMs.[6] Globally, Data Privacy protections are lacking.[7]

The advent of the new technology of cybernetic implants and 'body hacking'[8] dependent on personal data has exponentially increased the need for strong, comprehensive Data Privacy protections.[9] Without such protections, data and experiences accrued by the implants and other modifications will not belong to those equipped with the body modification.[10] This information will belong to the manufacturing corporation under licensing agreements, leading to individuals' data being used without direct consent.[11]

We are currently amid the Fourth Industrial Revolution.[12] The cybernetic revolution is poised to bring about the Fifth.[13] Before this revolution takes place, a privacy framework must be in place and is necessary for responsible uses of cybernetics in the non-military space.[14] Part II will address the history of cybernetic enhancements, from medical applications in subpart II.A[15] to the BodyNet in subpart II.B.[16] Part III will discuss the current status of private sector and individual Data Privacy protections.[17] Part IV will discuss possible models of regulation for data

6. Danny Palmer, *What is GDPR? Everything you need to know about the new general data protection regulations*, ZDNET (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/; *see infra* IV.B.

7. Guidehouse, *A Roadmap to Global Data Privacy Regulation*, GUIDEHOUSE (2019), https://guidehouse.com/-/media/www/site/insights/financial-services/2019/fs-data-privacy-overview.pdf.

8. Peralta, *supra* note 4.

9. *See infra* III.A.

10. *See infra* II.B.

11. *See infra* II.B; Daniel Oberhaus, *This DIY Implant Lets You Stream Movies From Inside Your Leg*, WIRED (Aug. 30, 2019), https://www.wired.com/story/this-diy-implant-lets-you-stream-movies-from-inside-your-leg/. It should further be noted that manufacturers might very well require the implant user consent to the use of their data prior to implantation in certain cases. However, under the future schemes considered in this paper, consent would not be required for implantation, and post-implant data use by someone other than the implantee would require direct consent from that individual. *See infra* IV.A; IV.B; IV.C.

12. *See* Kevin Redden, *Addressing Automation in the Twenty-First Century*, 14 J. BUS. & TECH. L. 499, 499 (2019); *see generally* Klaus Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, WORLD ECONOMIC FORUM (Jan. 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

13. Center for Strategic & International Studies, *Beyond Technology: The Fourth Industrial Revolution in the Developing World* May 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190520_Runde%20et%20al_FourthIndustrialRevolution_WEB.pdf.

14. While the military has had and will continue to have an outsized impact on development of cybernetic implant technology, their involvement, impact, and policy implications will not be discussed herein. *See* Matthew Gault, *Here's the Pentagon's Terrifying Plan for Cyborg Supersoldiers*, VICE (Dec. 9, 2019), https://www.vice.com/en_us/article/xwee47/heres-the-pentagons-terrifying-plan-for-cyborg-supersoldiers.

15. *See infra* II.A.

16. *See infra* II.B.

17. *See infra* III.A; III.B.

accrued through cybernetic implants in subparts IV.A, IV.B, and IV.C.[18] This part will conclude by advocating for a hybrid model[19] based on the computer network[20] and the GDPR models.[21] The advent of the Fifth Industrial Revolution without safeguards in place either significantly handicaps the technology or risks its abandonment until such protections are in place.[22] A new hybrid model of regulation must be implemented for the coming technology, current existing models and protections by themselves are insufficient.

II. HISTORY OF CYBERNETIC ENHANCEMENTS: FROM SCIENCE-FICTION TO REALITY

As previously mentioned, cybernetics have long had a cherished place in popular culture.[23] The public has always held a fascination with the ramifications of such technology.[24] A fascination that unfortunately has not translated to extensive legal frameworks related to their specific Data Privacy challenges.[25] This section will discuss the historical background of cybernetics, focusing particularly on the medical industry[26] and proceed into a discussion on the rising industry of private body modification, brought about by the Transhumanist movement.[27]

A. Medical Implants and Cyborgization

The medical industry has been at the forefront of the body modification industry.[28] While popular culture often depicts cybernetics as a near to far future technology and

18. *See infra* IV.A; IV.B; IV.C.

19. *See infra* IV.C.

20. *See infra* IV.A.

21. *See infra* IV.B; Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1, Art. 7, 10, and 17.

22. *See infra* IV.A; IV.B; IV.C.

23. *Supra* note 1.

24. Charles Towers-Clark, *Cyborgs Are Here And You'd Better Get Used To It*, FORBES (Oct. 1, 2018), https://www.forbes.com/sites/charlestowersclark/2018/10/01/cyborgs-are-here-and-youd-better-get-used-to-it/#423b555d746a.

25. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

26. *See infra* II.A.

27. *See infra* II.B.

28. *See* Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications*, BROOKINGS (Sep. 2014), https://www.brookings.edu/research/our-cyborg-future-law-and-policy-implications/; Arthur House, *The Real Cyborgs*, THE TELEGRAPH (Oct. 20, 2014), https://s.telegraph.co.uk/graphics/projects/the-future-is-android/.

challenge, the reality is that they have been in place in some form or another since the early 16th century.[29]

While the technology has come much farther and become much more sophisticated since the 1500s, similar ethical and privacy challenges abound.[30] Cybernetic enhancements are a far-ranging, all-encompassing industry that is not aided by being reduced to a singular approach and framework.[31] To illustrate this point are four different types of medical cybernetic advances:

1. Prosthetic Limbs

Prosthetics, such as the C-leg implant, introduced by German manufacturer Ottobock in 1997,[32] can involve microprocessors.[33] The C-leg functions by using the microprocessor to control the knee joint and its flexion to copy the natural motion of an organic limb.[34] Small valves are used through a hydraulic system to respond to small variations in the data collected by the device through sensors to change the pressure and assist in a more natural gait.[35]

From a cybernetic perspective, these types of implants do not seem to have Data Privacy implications. But, advancements in this type of technology such as WiFi powered limbs, or direct brain wave operated limbs, do.[36] In fact, several scholars,

29. William Park, *The geniuses who invented prosthetic limbs*, BBC (Nov. 2, 2015), https://www.bbc.com/future/article/20151030-the-geniuses-who-invented-prosthetic-limbs.

30. John Hewitt, *The Future of permanent, fully integrated prosthetic limbs and bionic implants*, EXTREMETECH (Sep. 16, 2014), https://www.extremetech.com/extreme/189746-the-future-of-permanent-fully-integrated-prosthetic-limbs-and-bionic-implants (discussing the difficulty in proper fitting of implants and the challenge of creating a strong implant to skin interface resistant to infection).

31. *See* Collin R. Bockman, *Cybernetic-Enhancement Technology and the Future of Disability Law*, 95 IOWA L. REV. 1315, 1323–1328 (2010); Leslie Wenning & Richard Cruz, *The Ethics of Artificial Vision Technology: An Early Step Towards an Ethics of Cybernetic Repair and Augmentation*, 5 COLUM. J. OF BIOETHICS 59, 60–63 (Fall 2006) (highlighting, on the one hand, different examples of medical cybernetic technology and its potential impact on disability laws and, on the other hand, ethical implications of cosmetic cybernetic technology).

32. MARKO B. POPOVIĆ, BIOMECHANICS AND ROBOTICS 231 (2013).

33. *Id.* at 232–233.

34. *Id.* at 232 (discussing the use of hydraulic cylinders and the microprocessor to mimic the flexing of a natural limb and joint).

35. *Id.*

36. *See* John Hewitt, *Green implants are coming, and paving the way for implantable WiFi devices*, EXTREMETECH (Dec. 16, 2014), https://www.extremetech.com/extreme/195674-green-implants-are-coming-and-are-paving-way-for-implantable-wifi-devices; Karla Lant, *New "Interscatter Communication" Could Let Your Implants Talk via Wi-Fi*, FUTURISM (Sep. 10, 2016), https://futurism.com/new-interscatter-communication-could-let-your-implants-talk-via-wi-fi; Luke Dormehl, *'Interscatter communication' could help your brain implant talk to your iPhone*, DIGITAL TRENDS (Aug. 18, 2016), https://www.digitaltrends.com/cool-tech/interscatter-communication/.

such as Weber Tobias,[37] have contemplated criminal implications of the hackability of such devices. Posing the question, "could someone overtake the [prosthetic] arm and make [it] do something [the individual] didn't want to do?"[38] These criminal implications of cybernetic hacking are pervasive across the multitude of devices involving this technology.[39]

2. Cochlear Implants

A cochlear implant is an electronic device implanted under a patient's skin to assist their hearing.[40] Much like the implants discussed above,[41] these devices can be hacked.[42] This has been established by a team of engineering students at Duke University who hacked cochlear implants to allow for customizable setting adjustments of the implants to boost effectiveness for individuals.[43]

While this team of engineers hacked benignly, the inverse possibility is possible by implication.[44] With the rise of deepfake video fabrications,[45] it does not take a strong imagination to consider that with lackluster data protections for these devices, a malicious actor could implant auditory hallucinations through this backdoor.[46] Once again, this dangerous possibility of hacking gives rise to criminal Data Privacy implications.[47]

37. Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms.

38. *Id.*

39. Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications*, BROOKINGS (Sep. 2014), https://www.brookings.edu/research/our-cyborg-future-law-and-policy-implications/.

40. COCHLEAR IMPLANTS, Nat'l Inst. on Deafness and Other Comm. Disorders (NIDCD), https://www.nidcd.nih.gov/health/cochlear-implants (2019).

41. *Supra* II.A.1.

42. *See* Nickolaus Hines, *Neural Implants Could Let Hackers Hijack Your Brain*, INVERSE (Aug. 5, 2016), https://www.inverse.com/article/19148-neural-implants-could-let-hackers-hijack-your-brain; Mary Beth Nierengarten, *Protecting Medical Devices against Cyberthreats*, ENTTODAY (Sep. 24, 2017), https://www.enttoday.org/article/protecting-medical-devices-cyberthreats/.

43. Ken Kingery, *Hacking into a Bionic Ear*, DUKE PRATT SCH. OF ENG'G (Aug. 23, 2016), https://pratt.duke.edu/about/news/hacking-bionic-ear.

44. *Id.*

45. CNN Business, *Deepfake videos: Inside the Pentagon's race against deepfakes*, CNN (Jan. 2019), https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

46. *See* Hines, *supra* note 42.

47. Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms; *see also* S. 1790, 116th Cong. (2019). This is the first federal legislation specifically geared towards the use of "deepfakes", a growing concern especially in the political space. This represents a growing awareness of the concerns expressed in this comment regarding the manipulation of sensory data. *See Id.;* Matthew F. Ferraro,

3. Pacemakers

Pacemakers are medical devices implanted in a patient's chest to assist in managing issues with heart rate through electrical pulses.[48] Hacks of these devices have already been acknowledged by the U.S. Department of Homeland Security in March 2019.[49] According to the agency, "[a]n attacker with adjacent short-range access to an affected product, in situations where the product's radio is turned on, can inject, replay, modify and/or intercept data within the telemetry communication."[50] Of further concern is that they also indicated that such attacks could be undertaken with little difficulty by low-level attackers.[51] The low level of sophistication required for such attacks reflects the consensus among cybersecurity professionals that these medical devices have historically lacked any data security.[52]

Without cybersecurity protections, conceivable scenarios could entail malicious actors "shutt[ing] off a defibrillator or command it to deliver a shock to the heart."[53] Protections for political, business, and intelligence leaders would need to be significantly revisited if assassination could be conducted in the privacy of one's office or home on unsuspecting persons with heart conditions.[54]

4. Direct Neural Implants

Direct neural implants and brain-computer interfaces are the latest advance in cybernetic enhancements.[55] Furthermore, as a category, they implicate the previous

Deepfake Legislation: A Nationwide Survey, WILMERHALE (Sep. 25, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20190925-deepfake-legislation-a-nationwide-survey.

48. PACEMAKERS, NIH Nat'l Heart, Lung, and Blood Inst., https://www.nhlbi.nih.gov/health-topics/pacemakers (2019).

49. Bob Curley, *Hackers Can Access Pacemakers, but Don't Panic Just Yet*, HEALTHLINE (Apr. 4, 2019), https://www.healthline.com/health-news/are-pacemakers-defibrillators-vulnerable-to-hackers; *see* Alex Hern, *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*, THE GUARDIAN (Aug. 31, 2017), https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update (acknowledging the hacking risks in pacemakers with over 500,000 compromised devices in 2017. Per DHS, this risk has increased exponentially and thus projections of current risk are likely much higher); *see also* Richard Yonck, *The next generation of hackers may target your medical implants*, SALON (Mar. 14, 2020), https://www.salon.com/2020/03/14/the-next-generation-of-hackers-may-target-your-medical-implants/ (further explaining current and future projected risk of medical device hacks).

50. Curley, *supra* note 49.

51. *Id.*

52. Mary Beth Nierengarten, *Protecting Medical Devices against Cyberthreats*, ENTTODAY (Sep. 24, 2017), https://www.enttoday.org/article/protecting-medical-devices-cyberthreats/.

53. Curley, *supra* note 49.

54. Hern, *supra* note 49.

55. Jerry J. Shih et al., *Brain-Computer Interfaces in Medicine*, 87(3) MAYO CLINIC PROC. 268, 268 (2012). The authors explain that a Brain-Computer Interface, or 'BCI', "is a computer-based system that acquires brain signals, analyzes them, and translates them into commands that are relayed to an output device to carry out a

three discussed devices.[56] Direct neural implants can be used to control anything from a prosthetic limb responding directly to brain impulses, to a pacemaker responding to minute electrical changes relayed by the heart to the brain.[57]

However, this development, from a security standpoint is among the most concerning.[58] Whereas other devices involve the localized limb/body specific networks,[59] a direct neural implant involves, by necessity, a total body network.[60] Consequently, a possibility exists where a hacker enters through a backdoor to the device and can access any area where the brain has a connection.[61] The rise of the deepfake industry makes this possible backdoor to the body's network even more concerning.[62] The possibility of direct neural implant hacks raises the risk of false memory implantation[63] or sensory hallucinations.[64] These serious risks underscore the need for strong, federalized, cybersecurity protections.[65]

desired action." *Id.* Training of both the user and the artificial intelligence powering the interface are needed for optimum use. *Id.*

56. Dom Galeon, *Experts: Artificial Intelligence Could Hijack Brain-Computer Interfaces*, FUTURISM (Nov. 20, 2017), https://futurism.com/experts-artificial-intelligence-hijack-brain-computer-interfaces.

57. *See* Shih at 272–274 (detailing current and possible future applications of brain-computer interfaces).

58. *See* Sergio López Bernal et al., Cybersecurity in Brain-Computer Interfaces: State-of-the-art, opportunities, and future challenges (2019) (on file with the University of Murcia) at 1, 10-22; Casey Newton, *Brain-computer interfaces are developing faster than the policy debate around them*, THE VERGE (July 31, 2019), https://www.theverge.com/interface/2019/7/31/20747916/facebook-brain-computer-interface-policy-neuralink.

59. *See supra* II.A.1; II.A.2; II.A.3.

60. *See* Shih at 268 (explaining that brain-computer interfaces, by virtue of being directly linked to the brain, possess direct connectivity to the central nervous system and, thus, the entire individual's body).

61. *See* Mary Beth Nierengarten, *Protecting Medical Devices against Cyberthreats*, ENTTODAY (Sep. 24, 2017), https://www.enttoday.org/article/protecting-medical-devices-cyberthreats/.

62. *See* CNN Business, *Deepfake videos: Inside the Pentagon's race against deepfakes*, CNN (Jan. 2019), https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

63. Philip Perry, *Scientists discover how to implant false memories*, BIG THINK (June 15, 2016), https://bigthink.com/philip-perry/scientists-have-discovered-how-to-implant-false-memories.

64. Nickolaus Hines, *Neural Implants Could Let Hackers Hijack Your Brain*, INVERSE (Aug. 5, 2016), https://www.inverse.com/article/19148-neural-implants-could-let-hackers-hijack-your-brain.

65. *Infra* III.B.

B. Private Body Modification: BodyNet and the Danger of Body Hacking

Private Body Modification is on the rise.[66] The transhumanist movement[67], pioneered by philosopher and journalist Zoltan Istvan,[68] has increased the popularity of cybernetic enhancement procedures.[69]

Procedures rapidly gaining in popularity include, but are not limited to, chips directly implanted under the skin that contain digital wallets,[70] access cards,[71] and other electronic personal identification.[72] Such implants naturally engender cybersecurity concerns as well as ethical ones.[73] For example, workplaces in Sweden have experimented with microchips embedded under the skin of their employees to remove the need for physical key cards, IDs, and the like.[74] It remains unknown whether these implanted microchips that would replace physical key cards will become mainstream or not.[75] It is crucial for policymakers and lawmakers to

66. Tim Adams, *When man meets metal: rise of the transhumans*, THE GUARDIAN (Oct. 29, 2017), https://www.theguardian.com/technology/2017/oct/29/transhuman-bodyhacking-transspecies-cyborg (highlighting the rise of the transhumanist movement and creation of various organizations to promote said movement).

67. Transhumanism is a philosophical movement having as central construct the belief that the marrying of technology to human biology will allow humanity to transcend current physical and mental limitations and provide the basis for future evolutionary progress. *See* Wesley J. Smith, *A Transhumanist Runs for President*, NATIONAL REVIEW (Feb. 22, 2020), https://www.nationalreview.com/2020/02/transhumanism-zoltan-istvan-technological-self-perfection-immortality/.

68. John Hewitt, *An interview with Zoltan Istvan, leader of the Transhumanist Party and 2016 presidential contender*, EXTREME TECH (Oct. 31, 2014), https://www.extremetech.com/extreme/192385-an-interview-with-zoltan-istvan-leader-of-the-transhumanist-party-and-2016-presidential-contender.

69. Fraser Gillan, *The transhumanists who are 'upgrading' their bodies*, BBC NEWS (Oct. 6, 2019), https://www.bbc.com/news/uk-scotland-49893869 (discussing the increase in popularity of bio-hacking and implanting cybernetic devices in one's own body).

70. Steven Melendez, *Under My Skin: The New Frontier Of Digital Implants*, FAST COMPANY (June 11, 2016), https://www.fastcompany.com/3059769/ive-got-you-under-my-skin-the-new-frontier-of-digital-implants.

71. Maddy Savage, *Thousands Of Swedes Are Inserting Microchips Under Their Skin*, NPR (Oct. 22, 2018), https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin.

72. Haley Weiss, *Why You're Probably Getting a Microchip Implant Someday*, THE ATLANTIC (Sep. 21, 2018), https://www.theatlantic.com/technology/archive/2018/09/how-i-learned-to-stop-worrying-and-love-the-microchip/570946/. Such implants give rise to the concept of the 'BodyNet'. In other words, a technology network operating at and within the human body. This network is solely contained and operational within the body but may interface with other networks at certain access points (such as a key card panel in the case of access card implants). *See Id.*

73. *See* Alex Pearlman, *The Ethics of Experimentation: Ethical Cybernetic Enhancements*, MEDIUM (June 19, 2017), https://medium.com/@lexikon1/the-ethics-of-experimentation-ethical-cybernetic-enhancements-48f9ad991769; Andy Miah, *The Ethics of Human Enhancement*, MIT TECHNOLOGY REVIEW (Sep. 8, 2016), https://www.technologyreview.com/s/602342/the-ethics-of-human-enhancement/.

74. Savage, *supra* note 71.

75. Weiss, *supra* note 72.

understand the ramifications of technological body modification prior to enacting any regulatory or statutory schemes designed to protect consumers as society proceeds into the unknowns of the Fifth Industrial Revolution[76] and the world envisioned by transhumanism.[77] Moreover, this procedure is not the sole province of Europe, where they possess the slight benefit of the GDPR,[78] American-based companies have toyed with similar implanted microchips for their employees.[79] There is a stark difference, societally, between these implantations that occur in Europe and the implantations that occur in the United States: the lack of comprehensive federal cybersecurity protections within the United States and the high widespread variability of such protections among the States unlike Europe.[80]

In addition, while implanting microchips in employees may invoke strong ethical concerns and ramifications, other implants such as digital wallets raise more conventional security risks.[81] There have been several prominent hacks of personal information over the last decade that have had dire economic consequences.[82] Yet these relatively frequent hacks, directed to arguably less vital but more digitally secured domains than the self and human body, do not seem to have dissuaded the

76. The Fifth Industrial Revolution, as contemplated here, stands for an envisioned era of commonplace bio-hacking that will follow the Fourth Industrial Revolution of wide-spread automation and artificial intelligence. *See generally* Klaus Schwab, *The Fourth Industrial Revolution: what it means, how to respond*, WORLD ECONOMIC FORUM (Jan. 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

77. Sarwant Singh, *Transhumanism And The Future of Humanity: 7 Ways The World Will Change by 2030*, FORBES (Nov. 20, 2017), https://www.forbes.com/sites/sarwantsingh/2017/11/20/transhumanism-and-the-future-of-humanity-seven-ways-the-world-will-change-by-2030/#645dd0d07d79.

78. The slight benefit referenced here refers to the existence of a common cybersecurity and data privacy scheme across the European Union which provides a degree of protection and certainty regarding compliance to European-facing individuals and entities. This contrasts with the United States where there is no federal regulatory scheme. *See* Danny Palmer, *What is GDPR? Everything you need to know about the new general data protection regulations*, ZDNET (May 17, 2019), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/; Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

79. Merrit Kennedy, *Wisconsin Company Offers to Implant Chips in its Employees*, NPR (July 25, 2017), https://www.npr.org/sections/thetwo-way/2017/07/25/539265157/wisconsin-company-plans-to-start-implanting-chips-in-its-employees.

80. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

81. Emily Stewart, *If bitcoin is so safe, why does it keep getting hacked?*, VOX (May 9, 2019), https://www.vox.com/recode/2019/5/8/18537073/binance-hack-bitcoin-stolen-blockchain-security-safu. The conventional digital wallet hacking considerations invoke here are equally pertinent for implantable digital wallets. *Id.*

82. *See* Victoria Cavaliere & Brian Fung, *Equifax exposed 150 million Americans' personal data. Now it will pay up to $700 million*, CNN BUSINESS (July 22, 2019), https://www.cnn.com/2019/07/22/tech/equifax-hack-ftc/index.html; Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (illustrating different examples of significant hacks in recent years).

rising industry of the digital wallet and associated cybernetic enhancement industry.[83]

Digital wallets, implanted under the skin of an individual, invoke the need for data protections.[84] However, who would bear responsibility for this data and its protection is unknown or ambiguous. On the one hand, financial institutions, presumably owning the account associated with the wallet, could take responsibility for protecting the digital wallet as a device and its accompanying data.[85] On the other hand, implanted individuals could bear the responsibility for securing their own data as well through the purchase of network and device protection, like firewalls and general anti-hacking software, for their own body and implanted technology located therein.[86] Currently, no conclusive answers nor federal guidelines exist to guide law and policymakers when making decisions regarding data security and privacy frameworks, particularly where new and emerging technologies are concerned.[87] Underscoring this lack of guidance, the GDPR does not contemplate cybernetics in its regulatory scope, thereby providing little instructional assistance.[88]

Lastly, as somewhat discussed previously,[89] law and policymakers must attempt to foresee the criminal implications of an event where body essential functions are hacked and compromised.[90] Suppose a direct neural implant or brain-computer interface is hacked by malicious actors and this interface links to a prosthetic. In a scenario where these malicious actors seize control of the limb to perform a violent

83. Michael Moeser, *5 trends driving growth of digital wallets*, PaymentsSource (June 24, 2019), https://www.paymentssource.com/list/5-trends-driving-growth-of-digital-wallets.

84. Digital wallets, by virtue of being an outgrowth of banking, invoke high levels of data security and protection as monetary security is paramount to the individual and the society to which said individual belongs to. *See* Stewart, *supra* note 81.

85. *See Id.* Should the responsibility for the data lie with the financial institution, regulation would operate like it currently does for banking applications and non-implantable wallets.

86. If the answer to this question is yes, then the framework would operate like current cyber insurance. *See* Abha Bhattarai, *Cyber-insurance becomes popular among smaller, mid-size businesses*, THE WASHINGTON POST (Oct. 12, 2014), https://www.washingtonpost.com/business/capitalbusiness/cyber-insurance-becomes-popular-among-smaller-mid-size-businesses/2014/10/11/257e0d28-4e48-11e4-aa5e-7153e466a02d_story.html.

87. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

88. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1. The regulation clearly sets out its scope as applying "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system", none of which implicates the particular mechanisms of cybernetic implants. *Id.*

89. *Supra* II.A.

90. *Id.*

crime, there are no conclusive answers regarding who bears ultimate responsibility.[91] The responsibility could lie with the individual that physically accomplished the crime, in other words the implantee,[92] or it could lie with the malicious actors, the implantors, which may give rise to attribution issues.[93] Or, would the company, which may not have diligently reinforced its interface's security protocols, bear ultimate fault.[94] The law and general scholarship provide little clarity on the subject, but, as society approaches a present where 'cyborgization'[95] and potential omnipresence of cybernetic enhancements are a reality, law and policymakers need to be able to contemplate the extensive ramifications that such technology could have.[96] Data protections must be strongly reinforced and regulatory clarity and scheme must be in place at the federal level.[97]

III. PRIVATE SECTOR USE OF DATA: THE REGULATORY WILD-WEST

A. Inadequate Personal Data Protection

Data Privacy laws in the United States are sector-specific in nature and primarily state-based.[98] These laws are solely focused on particular challenges and risks faced by individual sectors and industry, and do not take a 'big picture' view in their regulatory approaches.[99] While this comment advocates for a cybernetic-focused approach when it comes to regulating their Data Privacy challenges,[100] it also advocates a 'big picture' one as cybernetic enhancement technology encompasses a wide variety of applications across numerous industries, each with their own particularities.[101]

The lack of comprehensive federal Data Privacy law is concerning in of itself, but particularly so when considering cybernetic enhancement technology.[102] A citizen in

91. *See* Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms (discussing this exact dilemma in discussion with Weber Tobias).

92. *See id.*

93. *Id.*

94. *Id.*

95. Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications*, BROOKINGS (Sep. 2014), https://www.brookings.edu/research/our-cyborg-future-law-and-policy-implications/.

96. *Infra* III.B.

97. *Id.*

98. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

99. *Id.*

100. *Infra* III.B.

101. *Infra* IV.C.

102. *Infra* III.B.

Florida[103] will be subject to an entirely different set of protections and remedies than a citizen in California.[104] Additionally, if the Data Privacy breach occurs across different states then protections and remedies will be severely lacking, not to mention that even where there may be protections, these may not be clear and may not have been subject to rigorous judicial interpretation yet.[105] Moreover, States do not even focus on similar lenses when addressing Data Privacy.[106] For example, in Maryland, the approach to cybersecurity and Data Privacy is focused on enacting minimum security standards, this reflects a proactive pre-incident approach.[107] On the other hand, Florida's Data Privacy laws are focused on the nature of the privacy of the data itself.[108] This means that Florida's legal frameworks are designed primarily around the recovery and post-securitization of data in the event of a breach.[109] Consequently, it is much more reactive and focused on the exposure of weaknesses by a breach.[110] No state currently has a multi-faceted scheme that incorporates both styles of legal mechanisms.[111]

In the fast-approaching world of cybernetic enhancement technology, the need for robust, clear, comprehensive Data Privacy law will never be stronger.[112] Cybernetic enhancement technology, at its core, implicates the self.[113] It is essentially wearable technology,[114] using the Internet of Things,[115] melded to one's own body and therefore, eventually, an intricate part of the self and one's identity.[116] It is hard to

103. CYBERSECURITY LEGISLATION 2019, Nat'l Conf. of State Legislatures (2019), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx.

104. *Id.*

105. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

106. *Id.*

107. CYBERSECURITY LEGISLATION 2019, *Maryland*.

108. CYBERSECURITY LEGISLATION 2019, *Florida*.

109. *Id.*

110. *Id.*

111. *See generally* CYBERSECURITY LEGISLATION 2019.

112. *Infra* III.B.

113. Cybernetic enhancements, being an integral part of the individual's autonomy, by nature involve the sense of identity of the individual and are, thus, intensely personal. *See* Alex Pearlman, *The Ethics of Experimentation: Ethical Cybernetic Enhancements*, MEDIUM (June 19, 2017), https://medium.com/@lexikon1/the-ethics-of-experimentation-ethical-cybernetic-enhancements-48f9ad991769.

114. Much of the particularities and implications of bio-hacking and cybernetic implants are present in current wearable technology like smart watches and smart eyewear. *See* Steve Ranger, *What is the IoT? Everything you need to know about the Internet of Things right now,* ZDNET (Feb. 3, 2020), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

115. *Id.* The Internet of Things is used to refer to the interconnected systems of devices that collect and share data through the internet. *Id.*

116. *Supra* note 113.

nearly impossible to predict how law and policymakers would treat cybernetic enhancements when individuals believe that these enhancements are part of their body.[117] The treatment of such unique issues could entail property rights or it could invoke First Amendment rights.[118] State privacy laws are currently designed to be intentionally vague.[119] For instance, State laws mandating minimum security standards frequently center around the following language: "reasonable security procedures and practices must be implemented."[120] However, there is lack of clarity surrounding what may be considered reasonable.[121] More importantly, such statutory language, when litigated, is then interpreted by non-experts in cybersecurity which leads to further lack of clarity and potentially more confusion, and even nonsensical resolutions to potential issues.[122]

At present, the wild-west state of Data Privacy regulatory frameworks within the United States is an untenable position.[123] A robust, comprehensive federal Data Privacy framework must be in place in the near future.[124] More specifically on the issue of cybernetic enhancement, the enactment of such a scheme is not enough.[125] For cybernetic enhancement and their more pointed challenges regarding Data Privacy, a complementary specific approach must also be enacted accompanying

117. *Id.*

118. Courts have generally treated clothing as being protected by the First Amendment. Cybernetic enhancements, under the thought of being wearable technology, could also be treated under a similar concept. Presumably the treatment of cybernetic enhancements in this way would protect the data at the individual level. *See* Shira Stein, *As a high school student during the Vietnam War, she wore her protest on her sleeve*, THE WASHINGTON POST (Dec. 15, 2017), https://www.washingtonpost.com/local/public-safety/as-a-high-school-student-during-the-vietnam-war-she-wore-her-protest-on-her-sleeve/2017/12/14/ad4ffbfa-e10f-11e7-bbd0-9dfb2e37492a_story.html; Robert Barnes, *Supreme Court sides with 'subversive' clothing designer in First Amendment case*, THE WASHINGTON POST (June 24, 2019), https://www.washingtonpost.com/politics/courts_law/supreme-court-sides-with-apparel-maker-who-said-government-violated-first-amendment-by-denying-subversive-clothing-line-trademark/2019/06/24/717eb058-968a-11e9-916d-9c61607d8190_story.html.

119. *See* CYBERSECURITY LEGISLATION 2019, Nat'l Conf. of State Legislatures (2019), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx (highlighting several state examples. Enacted legislation must be intentionally vague in order to encompass the widest berth of possible emerging issues and remain efficiently responsive).

120. DATA SECURITY LAWS – PRIVATE SECTOR, Nat'l Conf. of State Legislatures (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx (listing at least 25 states incorporating variants of that language into their respective statutes).

121. *The February 2016 California Attorney General's Data Breach Report Sets a Standard for "Reasonable Security" – What does This Mean for Cybersecurity Litigation?*, AMERICAN BAR ASSOCIATION (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/04_klein/.

122. *Id.*

123. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

124. *Infra* III.B (discussing what ought to be addressed in a federal cybernetic framework).

125. *Id.*

such a federal framework.[126] Cybernetic enhancement technology must be regulated based on a hybrid formula built on the computer network formula and the more personal GDPR model.[127]

B. The Need for a Federal National Cybernetic Law

As discussed, the United States does not, as of this moment, possess any federal privacy framework.[128] All Data Privacy laws in the United States are sector-specific, State-law.[129] A comprehensive robust and clear federal Data Privacy law must be enacted.[130] However, for cybernetics, the issue and need go deeper.[131] For cybernetic enhancement technology itself, a complementary just as robust and just as clear cybernetic-specific set of laws must also be enacted.[132]

It is clear that privacy threats are constant and, that regardless of technology or industry, the federal laws must anticipate future threats.[133] This constant is never clearer than when considering the cybernetic issue.[134] The possibility and likelihood of abuse and breaches of personal data within this field are massive.[135] If a cybernetic-equipped individual is considered a licensee,[136] then this abuse of personal data would not even solely be within the realm of hackers and other various malicious actors, but also the province of the ultimate owner: a corporate entity.[137] In addition, for cybernetics, more traditional threats such as hacking and general

126. *Id.*

127. *Infra* IV.C.

128. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

129. *Id.*

130. *See id.* (demonstrating that this view is supported by the GAO).

131. *Id.* The issue and need go deeper where cybernetics are concerned as no real regulation, state or federal, is currently in place within the United States. *Id.*

132. *Supra* II.B.

133. *Id.*

134. *Id.*

135. *See* Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms; Nickolaus Hines, *Neural Implants Could Let Hackers Hijack Your Brain*, INVERSE (Aug. 5, 2016), https://www.inverse.com/article/19148-neural-implants-could-let-hackers-hijack-your-brain; Alex Hern, *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*, THE GUARDIAN (Aug. 31, 2017), https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update (demonstrating examples of the threat of cybernetic implant hacks).

136. The licensee theory stems from the idea that the device is the ultimate property of the corporate owner giving the implantee a more limited set of data rights. This theory is considered here to illustrate the need for comprehensive federal privacy legislation and complementary cybernetic ones. *See* Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/; *supra* note 85.

137. *See supra* note 85.

compromise of personal information must also be considered.[138] As a result, it is essential, through this clear need, to have a specific federal cybernetic Data Privacy framework built upon a comprehensive robust federal Data Privacy regulatory scheme.[139]

A federal privacy framework is necessary to ensure uniformity of purpose, protection, and remedy across the nation.[140] A cybernetic-specific add-on scheme would strengthen protections and validate decisions by individuals to equip cybernetic enhancement technology to themselves knowing their data is secured.[141] Furthermore, with unity of laws and schemes, a global framework could then be built around the United States framework and the European GDPR framework that would further maximize data security and allow flexibility for advances in technology among the cybersecurity industry, specifically that of cybernetics.[142] Future needs and technology can seldom be anticipated, but marrying two schemes, such as those contemplated, ensures a greater flexibility and a stronger responsiveness to unanticipated future needs without the need or challenge of constructing an entirely new legal framework and legal devices to address these future threats.[143]

138. *See* Emily Stewart, *If bitcoin is so safe, why does it keep getting hacked?*, VOX (May 9, 2019), https://www.vox.com/recode/2019/5/8/18537073/binance-hack-bitcoin-stolen-blockchain-security-safu; Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms.

139. *Infra* IV.C.

140. Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/.

141. The lack of strong data security is one of the main concerns of bio-hackers. Should data be more robust and secured, it is highly likely that a strong increase in the availability of the technology and a more widespread practice of cybernetic device implantation would be observed. *See generally* Sigal Samuel, *How biohackers are trying to upgrade their brains, their bodies – and human nature*, VOX (Jun. 25, 2019), https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr.

142. A global complementary scheme would assist in securing data against malicious actors and allow a robust cybersecurity framework to be built according to the peculiarities of the area seeking to be regulated. In other words, by building the framework as a complementary global engine, the scheme would have more ease regulating the fundamentally decentralized internet and digital realm. *See* Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1.

143. *Id.* (showing that by being complementary and built to regulate a decentralized industry, the framework would be more responsive to future, unanticipated threats as the scheme could be continuously built upon).

IV. MODELS OF REGULATION FOR CYBERNETIC ENHANCEMENTS

Data Privacy models are based around who bears ultimate responsibility in the event of security lapses.[144] For the traditional computer network model, the responsibility lies with the cyber network owner.[145] Whereas, the newly established European GDPR model puts more emphasis on the direct owner of the data (i.e. the individual).[146] For cybernetic enhancement technology, neither approach is sufficient to address the inherent challenges of the technology.[147] Instead, this comment advocates for a new approach, designed to incorporate elements of both models to withstand the possible risks present and future of such an industry.[148] Under this hybrid model, securitization of data and ownership would be shared and, thus, result in a novel scheme.[149]

A. The Computer Network Model

The Computer Network Model is considered the traditional approach to cybersecurity legislation and protective schemes.[150] Since the advent of the Internet and personal computers, and associated challenges, this is the scheme that has been enacted to ensure protection.[151]

Under this model, responsibility for securing networks and data lies with the ultimate network or server owner.[152] For example, when the Office of Personnel Management ("OPM") was breached[153] and the data of numerous government

144. *Id.* Frequently, this lies with the server owner, individual, or sometimes insurance company that insured the network. *See Id.*

145. *Infra* IV.A; *see* Jayne Ponder, *GAO Report Calls for Federal Privacy Law*, INSIDE PRIVACY (Feb. 24, 2019), https://www.insideprivacy.com/data-privacy/gao-report-calls-for-federal-privacy-law/; DATA SECURITY LAWS – PRIVATE SECTOR, Nat'l Conf. of State Legislatures (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx. The computer network model, where responsibility lies with the server owner is that more commonly used in non-European jurisdictions. *Id.*

146. *Infra* IV.B; Tony Pepper, *Whose data is it anyway? GDPR and the problem of data ownership*, ITPROPORTAL (Aug. 6, 2019), https://www.itproportal.com/features/whose-data-is-it-anyway-gdpr-and-the-problem-of-data-ownership/.

147. *Infra* IV.C.

148. *Id.*

149. *Id.*

150. Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms.

151. *Id.*

152. DATA SECURITY LAWS – PRIVATE SECTOR, Nat'l Conf. of State Legislatures (May 29, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

153. Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

employees was unlawfully accessed, the responsibility for the lack of securitization lay with the government, the owner of the server housing the data.[154] Such a model is inadequate to address cybernetics.[155]

Under this model, the regulation of cybernetic enhancements naturally supposes a linked cybernetic implant network.[156] This network would need to be common to all similar implants.[157] However, the key limitation would be that, since under the Computer Network Model responsibilities lies with the network owner, the implants and, consequently, the network would also have to belong to a single corporate entity that could be regulated, an arrangement that may encourage undesirable monopolistic behavior.[158]

Such a model for cybernetic enhancements is inadequate due to there being a myriad of possible implants that may incorporate this technology.[159] Furthermore, it is highly unlikely that a particular implant would solely be the province of a singular corporate entity.[160] Similarly, due to the security risk presented by the Internet itself,[161] it is not even certain that all implants would have a common network instead of a private network that may be housed under different entities.[162] Consequently, basing legislation around such a model for cybernetics would leave too many security holes and would be unlikely to maximize protections.[163]

B. The European Data Privacy Regulatory Model

The European Data Privacy Regulatory Model is based around a multi-faceted approach where ultimate responsibility for different facets of Data Privacy does not necessarily lie with a corporate network owner.[164]

154. *Id.*

155. *Infra* IV.C.

156. *Id.* If the network were unlinked, regulation would be unenforceable as there would be no common network owner. Under this supposition, government ownership of the ultimate network is most likely implicated. *Id.*

157. *Id.*

158. *See Id.*

159. *Infra* II.A.

160. *Id.* If an implant has multiple uses and/or functions, different ultimate owners might be involved depending on the functions and data necessary. *Id.*

161. Julia Alexander, *The Prosthetic DEKA Arm Is Hackable and a Legal Mess*, VICE (June 3, 2014), https://www.vice.com/en_us/article/ezvvvz/the-deka-arm-is-hackable-and-that-might-open-up-a-legal-can-of-worms.

162. *See Infra* II.A. In other words, multiple complementary intranets serving common functions of independent, distinct implants. *Id.*

163. *Infra* IV.C.

164. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such

The GDPR entails different responsibilities regarding data collection and its purpose and data retention, and incorporates a "Right to be Forgotten" among its data erasure regulation.[165] For cybernetic enhancements, these different segmented responsibilities and "Right to be Forgotten" would represent strong founding principles, but without complementary measures the GDPR and, importantly, these specific components, would be inadequate for a full regulatory scheme for cybernetic enhancement technology.[166]

Under this type of model, cybernetic enhancement technology would be regulated in different segmented parts.[167] Regulation would be based on the segment, and based on that segment, ultimate responsibility for the data would be established.[168] Subsection 1 of this section will discuss the advantages and disadvantages of the GDPR Data Collection and Purpose component as applied to cybernetic enhancements.[169] Subsection 2 of this section will discuss the same pertaining to the Data Retention component.[170] Lastly, subsection 3 will discuss the "Right to be Forgotten" and Data Erasure and why, while it should be a primordial tenet of a future cybernetic enhancement regulatory scheme, it is inadequate without complementary cybernetic-specific measures.[171]

1. Data Collection and Purpose

Under the GDPR Model, Data Collection and its purpose would be a primordial segment around which regulation could be based.[172] That is to say that collection for different types of purposes would be regulated differently.[173]

With this model of regulation, public health and benefit would be highly considered among applicable regulations.[174] If the cybernetic enhancement

Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1; *see infra* note 210.

165. Kristof Van Quathem et al., *GDPR's right to be forgotten limited to EU websites*, INSIDE PRIVACY (Sep. 25, 2019), https://www.insideprivacy.com/eu-data-protection/gdprs-right-to-be-forgotten-limited-to-eu-websites/.

166. *Infra* IV.C.

167. *Infra* IV.B.1; IV.B.2; IV.B.3 (the segmented parts referred to are the three core functions of data collection, retention, and deletion).

168. *Id.*

169. *Infra* IV.B.1.

170. *Infra* IV.B.2.

171. *Infra* IV.B.3.

172. Robin Kurzer, *The story of data, Part 3: Who owns it?*, MARTECH TODAY (May 22, 2018), https://martechtoday.com/the-story-of-data-part-3-who-owns-it-215922.

173. *Id.*

174. Elisabethann Wright, *Digital health: Understanding the new responsibilities facing life sciences companies related to collecting and processing personal health data under the GDPR*, HOGAN LOVELLS PUBLICATIONS (July 12, 2018), https://www.hoganlovells.com/en/publications/understanding-the-new-

technology is used for a primary health purpose and data is collected to that end, then that data's ownership may ultimately lie with the corporate implant owner and not the equipped individual.[175] The public health purpose of the data collection would implicate the need to have access to the data for research and health maximization purposes, a greater good approach, which means that the data is more easily obtained.[176] Conversely, because it is more easily accessed, it is more easily breached.[177] This type of data would need to be secured strongly against outward invasion, yet internally porous enough to allow lawful examination of the information.[178] More importantly, under this scheme, the data, personal as it may be, would not belong to the individual from whom it had been obtained.[179] Thus, responsibility in the event of breaches and lack of security would lie with the corporate entity most benefiting from the unfettered access to this data.[180]

On the other hand, if the cybernetic enhancement has a primary cosmetic or quality of life purpose, for example better eyesight, then this data may actually belong to the equipped individual.[181] The data collected and absorbed through this use would not possess a strong public health benefit, therefore under the GDPR model, this data would primarily belong to the equipped individual.[182] That is to say, and reinforce that once sale and implantation occurs, the data ceases to be within the realm of the corporate entity that originally owned the implant.[183]

responsibilities-facing-life-sciences-companies-related-to-collecting-and-processing-personal-health-data-under-the-gdpr.

175. *See supra* IV.C. In this view, the stronger the public health benefit procured by the data, the weaker the personal data protections of said collected data. *Id.*

176. *Id.*

177. *See* Lily Hay Newman, *A Zoom Flaw Gives Hackers Easy Access to Your Webcam*, WIRED (July 9, 2019), https://www.wired.com/story/zoom-bug-webcam-hackers/. The more accessible the information, the more easily accessible it is for everyone, including malicious actors. *Id.*

178. Such a scheme would resemble national hospital networks and the data they secure within. However, these networks are still breached frequently. *See* Jessica Kim Cohen, *Healthcare data breaches reach record high in April*, MODERN HEALTHCARE (May 10, 2019), https://www.modernhealthcare.com/cybersecurity/healthcare-data-breaches-reach-record-high-april.

179. *Supra* note 175.

180. *Id.* Putting it another way, either the government or the research entity using the data for public health/benefit purposes. *Id.*

181. *See Id.*

182. *Id.* As articulated in note 173, the weaker the public health purpose, the stronger the private data protections. Thus, when the enhancement and data are collected primarily for cosmetic or quality of life purposes, the data would likely lie with the implantee. *Id.*

183. *Id.* That is to say, once sale and implantation occurs, full property rights over the data are conferred to the implantee. *Id.*

The limitation of such a model is clear: a purpose-focused approach and inquiry does not provide enough clarity.[184] For cybernetic enhancement technology there are a multitude of purposes to which the technology may be put to use.[185] More importantly, a single cybernetic enhancement may have a variety of non-clearly delineated purposes.[186] Such a scenario would result in an intense fact-specific inquiry to establish responsibility that may result in inconsistent resolutions across different litigation.[187] Further, inconsistent resolutions would lead to uncertainty among consumers, which would correspondingly weaken the industry and result in less benefit derived from the technology.[188]

2. Data Retention

Data Retention under the GDPR model is focused on length.[189] For example, a corporate entity, such as Google, has the ability and right to retain an individual's data for a limited amount of time, at which point the data is no longer kept and is effectively 'returned' to the individual.[190]

For cybernetic enhancement technology, this is insufficient.[191] Due to the technology's very nature as heavily involved in the self and one's possible identity, data collected, and therefore retained from such technology, is inherently personal.[192] Under this model, having intensely personal data retained by impersonal corporate actors can feel almost like a violation, particularly when such data is health-related.[193] Uncertainties of this model could include whether the retained data could be sold to a third party during the limited proscribed period or whether entities, such as insurance companies, could be owner and retainer of the data.[194]

184. *Id.* This model would necessitate a fact-specific inquiry that might result in contradictory or ambiguous results. This lack of clarity would then implicitly weaken the protections present in the model. *Id.*

185. *Supra* II.A.

186. *Supra* II.A.4 (discussing that a single brain-computer interface may have several, distinct, and non-overlapping functions).

187. *Supra* note 184.

188. *Id.*

189. William Long & Vishnu Shankar, *The impact of the GDPR on the retention of personal data*, IAPP (Sep. 2016), https://iapp.org/media/pdf/resource_center/GDPR-retention-sidley-september-2016-1516.pdf.

190. *Id.* ("[B]usinesses must affirmatively delete or return personal data – or retain data such that it is not 'personal' – if retaining such data is not essential for the purposes for which the data was collected.").

191. *Infra* IV.C.

192. *Supra* note 113.

193. *See supra* notes 175; 177; 178.

194. *Id.* Such a possibility is an alarming one to consider from a medical and health perspective. With the multitude of data sets that cybernetic enhancements could collect, insurance companies could minutely tailor plans and premium costs to individuals using factors and data that the individuals themselves might not even be aware of. In turn, this would essentially render insurance companies akin to casinos where the odds are always in favor of the house. *Id.*

The possibility of such a scheme raises many questions, and these questions point to the difficulty of embracing such a model for this type of technology.[195] Personal data, being so intricate to one's sense of self, necessitates a level of protection and securitization above that provided by an impersonal corporate entity, even if such data is only retained for a limited amount of time.[196] The nature of the data invites abuse.[197] The data cannot possess maximized protection and safety unless it is solely retained by the individual.[198]

3. Right to be Forgotten and Data Erasure

The GDPR model allows for individuals to request corporate entities to permanently delete their data, and thus be "forgotten" by the corporate entity.[199] This component of the GDPR Data Privacy regulatory scheme ought to be a core feature of any federal Data Privacy framework and more precisely a federal cybernetic-focused legislation.[200]

In the case of cybernetic enhancement technology, this feature would allow for a far more advanced measure of comfort among consumers than if data disposal was the sole province of a corporate entity for the reasons discussed in the previous sub-section.[201] Under this model, more responsibility would be placed with the individual.[202] This extended measure of control would then ensure that, should consumers have concerns about particular aspects of their data being present on an impersonal server, they could request to have it disposed of with all haste.[203] Such a measure would be key in the event that the individual's data is mandated to be present on an impersonal server but a breach occurs resulting in the individual's concern regarding misappropriation of their data to be heightened.[204] This measure of the

195. *Id.* Particularly the possibility that data connected to one's identity and sense of self could no longer be one's own property if the greater good demanded it be made publicly available. *Id.*

196. *See* Long & Shankar *supra* note 190.

197. *Id.* Depending on the scrutiny and the burden of proof given to a case involving a claimed public benefit, weaker claims may survive, and the individual may sacrifice their legal rights to their data for the greater good. *Id.*

198. *Infra* IV.C.

199. Kristof Van Quathem et al., *GDPR's right to be forgotten limited to EU websites*, INSIDE PRIVACY (Sep. 25, 2019), https://www.insideprivacy.com/eu-data-protection/gdprs-right-to-be-forgotten-limited-to-eu-websites/.

200. *See Id.* This would enable implantees/equipped individuals to request, within a proscribed period of time, that data related to their cybernetic implant be erased and that sole control of said data is within their hands. *Id.*

201. *See supra* IV.B.1; IV.B.2.

202. *Infra* IV.C.

203. Kristof Van Quathem et al., *GDPR's right to be forgotten limited to EU websites*, INSIDE PRIVACY (Sep. 25, 2019), https://www.insideprivacy.com/eu-data-protection/gdprs-right-to-be-forgotten-limited-to-eu-websites/.

204. *Supra* note 178 (stating that medical data is the focal point in terms of concern should a breach occur).

model strongly aids in marrying the public interest of mostly unfettered access to an individual's data that has public health benefits and the interests of the individual that wishes to keep their personal data strongly secured.[205] Among the cybernetic enhancement industry, this should be a central tenet.[206]

C. The Hybrid Cybernetic Model

The Hybrid Cybernetic Model advocated for in this comment seeks to incorporate elements of both systems and models of regulation.[207] The proposed model seeks to specifically meld the overall network security aspect of the Computer Network Model[208] with the more specific aspects of the GDPR model, particularly the "Right to be Forgotten."[209] Correspondingly, cybernetic enhancements must be regulated at the network and implant and individual level.[210]

Under the Hybrid Cybernetic Model, the unique nature and standpoint of cybernetic enhancement technology would be recognized where regulation is concerned.[211] The nature of such technology demands that the several networks on which these implants will operate need to be secured.[212] Furthermore, the devices themselves need to have strong security protocols in place to ensure that individual devices not be breached notwithstanding a lack of network breach.[213] Like the Computer Network Model, these 'big picture' notions need to be the responsibility of the network owner and device manufacturer, in most cases these two entities being one and the same.[214] The requirement of strong device-based security protocols, and the responsibility for such protocols lying with the network owners and device manufacturers, will ensure that sophisticated actors can secure the networks and devices to the highest potential degree and allow individuals to fully benefit from

205. *Supra* note 175 (finding a compromise between the public health benefit procured and the interests of the individual in having their private data secured).

206. *Infra* IV.C.

207. *Supra* IV.A; IV.B.

208. *Supra* IV.A.

209. *Supra* IV.B.3.

210. *Id.* In other words, regulation should occur separately regarding the network (where responsibility is incumbent upon the corporate owner), the implant itself (where responsibility for security features would be incumbent upon the merchant/retailer who may or may not be the network owner), and the individual who would be responsible for insuring his data and acting reasonably in securing his data from malicious actors. *Id.*

211. *Id.*

212. *Supra* IV.A; *see* notes 156; 162.

213. *Id.* Meaning that, if malicious actors attempt to bypass hacking the network and instead attempt to breach individual devices, strong security protocols must be in place to thwart all but the most sophisticated attacks. *Id.*

214. *Supra* IV.A.

these without fear of their data being compromised by low-level actors due to a lack of expertise when it came to securing the network.[215]

Where the data itself is concerned however, aspects of the GDPR must be more fully embraced.[216] While security of the devices and network must by necessary expertise belong to the corporate entities building the networks and manufacturing the devices, the data must be the sole responsibility of individuals.[217] Under this Hybrid Cybernetic Model, individuals implanted with cybernetic enhancements must have sole undivided control of their own data, management and collection of such data (although it may be facilitated by corporate entities), and the disposal thereof.[218] The data erasure and "Right to be Forgotten" concepts of the GDPR must be fully embraced in any cybernetic enhancement regulatory framing due to the intensely personal nature of the data.[219] The unfiltered control of the data by the individual while the network and device on which the data operates is fully secured by an expert corporate entity marries the best aspects of both models and is uniquely suited to the particular nature of the technology.[220]

For cybernetic enhancement technology, a similar model to this advocated for Hybrid Cybernetic Model must be embraced to encapsulate the unique nature of the risks, challenges, and nature of the technology itself.[221]

V. CONCLUSION

Technology's exponential advance and comparative lackluster movement in Data Privacy laws and regulations have resulted in a crossroads for society. Without implementation of a Federal Data Privacy framework, followed by a specific complementary hybrid cybernetic scheme, Data Privacy will remain at the mercy of private actors. Within the next 10 to 15 years as personal body modification technology becomes more common, a lack of privacy laws will naturally mean and prove an obstacle and limit to these technologies.

215. *Id.* This will aid in marrying the expertise of industry operatives and the interests of private individuals in the securitization of their own data. *Id.*

216. *Supra* IV.B.

217. *Supra* IV.B.3.

218. *Supra* IV.B.

219. *Supra* IV.B.3; *see* note 113.

220. *Supra* note 210.

221. *Id.*