UC Irvine Law Review

Volume 11 | Issue 4 Article 7

4-2021

# Emergent Medical Data: Health Information Inferred by Artificial Intelligence

Mason Marks

# Emergent Medical Data: Health Information Inferred by Artificial Intelligence

Mason Marks*

*Artificial intelligence (AI) can infer health data from people's behavior even when their behavior has no apparent connection to their health. AI can monitor one's location to track the spread of infectious disease, scrutinize retail purchases to identify pregnant customers, and analyze social media to predict who might attempt suicide. These feats are possible because, in modern societies, people continuously interact with internet-enabled software and devices. Smartphones, wearables, and online platforms monitor people's actions and produce digital traces, the electronic remnants of their behavior.*

*In their raw form, digital traces might not be very interesting or useful; one's location, retail purchases, and internet browsing habits are relatively mundane data points. However, AI can enhance the value of digital traces by transforming them into something more useful—emergent medical data (EMD). EMD is health information inferred by artificial intelligence from otherwise trivial digital traces.*

*This Article describes how EMD-based profiling is increasingly promoted as a solution to public health crises such as the COVID-19 pandemic, gun violence, and the opioid crisis. However, there is little evidence to show that EMD-based profiling works. Even worse, it can cause significant harm, and current privacy and data protection laws contain loopholes that allow public and private entities to mine EMD without people's knowledge or consent.*

*After describing the risks and benefits of EMD mining and profiling, the Article proposes six different ways of conceptualizing these practices. It concludes with preliminary recommendations for effective regulation. Potential options include banning or restricting the*

---

* Assistant Professor, Gonzaga University School of Law; Edmond J. Safra/Petrie-Flom Centers Fellow-in-Residence, Harvard University; Affiliated Fellow, Yale Law School Information Society Project; External Doctoral Researcher, Center for Law and Digital Technologies, Leiden Law School. Thank you to Hank Greely and the fellows of Stanford Law School's Center for Law and the Biosciences for their thoughtful comments. Thanks to Jack Balkin, Nikolas Guggenberger, and the fellows of the Yale Information Society Project for the opportunity to present the article at Yale Law School. I am grateful to Katherine Strandburg, I. Glenn Cohen, Ari Waldman, Bart Custers, Simone Van Der Hoff, Thomas Kadri, Ido Kilovaty, Tiffany Li, and the faculties of the University of Washington School of Law and Seattle University School of Law for many helpful conversations, comments, and suggestions.

*collection of digital traces, regulating EMD mining algorithms, and restricting how EMD can be used once it is produced.*

Introduction ..... 996
I. Emergent Medical Data ..... 1000
A. Understanding the Concept of EMD ..... 1000
B. Medical, Public Health, and Commercial Applications of EMD ..... 1013
1. Medical Research ..... 1013
2. Personalized Medicine ..... 1016
3. Monitoring and Promoting Public Health ..... 1020
4. Targeted Advertising and Vulnerability-Based Marketing ..... 1027
II. Conceptualizing EMD Mining ..... 1030
A. As Regulatory Arbitrage that Circumvents Privacy Laws ..... 1031
B. As a Breach of Contextual Integrity ..... 1037
C. As the Unlicensed Practice of Medicine ..... 1041
D. As the Operation of Unregulated Medical Devices ..... 1044
E. As Unregulated Health Research ..... 1046
F. As a Breach of Trust and Fiduciary Duties ..... 1050
III. Regulating Emergent Medical Data ..... 1051
A. Adapting Existing Laws to Regulate EMD ..... 1051
1. Expanding the Scope of HIPAA ..... 1052
2. Relying on Notice and Consent ..... 1053
B. Proposed Privacy and Data Protection Laws Do Not Go Far Enough ..... 1056
1. Protecting Personal Health Data Act ..... 1056
2. Smartwatch Data Act ..... 1057
3. Consumer Online Privacy Rights Act ..... 1058
C. Next Generation Data Protection for Minimizing EMD-Related Risks ..... 1061
1. Ban or Regulate the Collection of Digital Traces ..... 1062
2. Regulate EMD Mining Algorithms ..... 1063
3. Regulate how EMD Can Be Used ..... 1064
4. Require IRB Approval for EMD Mining Research ..... 1064
Conclusion ..... 1065

## INTRODUCTION

In the Algorithmic Age, artificial intelligence (AI) can infer health data from people's behavior even when that behavior has no apparent connection to their health. In 2002, Target analyzed the retail purchases of its customers to identify

those who were pregnant.[1] Though the company used advanced statistics instead of AI, its predictions were a sign of what was to come.[2] Since then, the fields of AI and predictive analytics have matured, and data scientists claim they can infer many conditions, including depression, pregnancy, infection, and diabetes, by analyzing online communications, shopping habits, and other routine behaviors.[3]

This Article introduces the concept of emergent medical data (EMD), which I define as health information inferred by AI from data points with no readily observable connections to one's health.[4] The Article explains how EMD is mined and why it should be considered a new type of health information distinct from traditional medical data (TMD). Unlike TMD, which is shared voluntarily in the context of research and healthcare delivery, and is subject to state and federal privacy laws, EMD is largely unregulated and is often collected surreptitiously without people's consent.[5]

The Article analyzes the ethical, legal, and social implications of EMD mining for medical and commercial purposes. In both contexts, EMD-based profiling is promoted as a solution to vexing public health problems, such as suicide, gun violence, the opioid epidemic, and infectious disease outbreaks. However, there is little evidence to show that it works.[6] Even worse, EMD-based profiling can cause significant harm, and privacy laws provide inadequate protection.[7]

---

1. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/UC8S-V5TP] (describing how Target used statistics to infer pregnancy from purchases involving unscented body lotion, mineral supplements, and cotton balls).

2. *Id.*

3. *See* Raina M. Merchant, David A. Asch, Patrick Crutchley, Lyle H. Ungar, Sharath C. Guntuku, Johannes C. Eichstaedt, Shawndra Hill, Kevin Padrez, Robert J. Smith & H. Andrew Schwartz, *Evaluating the Predictability of Medical Conditions from Social Media Posts*, PLOS ONE, June 17, 2019, at 1.

4. Mason Marks, *The Right Question to Ask About Google's Project Nightingale*, SLATE (Nov. 20, 2019, 10:47 AM) [hereinafter Marks, *Project Nightingale*], https://slate.com/technology/2019/11/google-ascension-project-nightingale-emergent-medical-data.html [https://perma.cc/XX3V-V99V] ("Companies love EMD because it allows them to transform mundane nonmedical data into sensitive health information."); Mason Marks, *Tech Companies' Dangerous Practice: Using Artificial Intelligence to Mine Hidden Health Data*, STAT (Sept. 17, 2019) [hereinafter Marks, *Hidden Health Data*], https://www.statnews.com/2019/09/17/digital-traces-tech-companies-artificial-intelligence/ [https://perma.cc/J8V4-W9BS] ("Tech companies feed our digital traces into machine learning algorithms and, like modern day alchemists turning lead into gold, transform seemingly mundane information into sensitive and valuable health data."); Mason Marks, *Emergent Medical Data*, HARV. L. PETRIE-FLOM CTR.: BILL OF HEALTH (Oct. 11, 2017) [hereinafter Marks, *Emergent Medical Data*], https://blog.petrieflom.law.harvard.edu/2017/10/11/emergent-medical-data/ [https://perma.cc/6B5R-X5JL] (defining emergent medical data).

5. Marks, *Emergent Medical Data*, *supra* note 4.

6. Mason Marks, *Artificial Intelligence-Based Suicide Prediction*, 21 YALE J.L. & TECH. (SPECIAL ISSUE) 98, 111–20 (2019) (describing the use of AI to predict suicide with prior testing for safety and efficacy).

7. *Id.*

Mining for EMD is possible because modern societies are awash in data.[8] According to some estimates, humans generated more data in the past few years than in all preceding centuries of human history combined.[9] Most of this information is generated through people's daily interactions with technology because nearly everything people do is monitored by internet-enabled software and devices. Smartphones, wearables, surveillance cameras, social media platforms, and voice-activated digital assistants are now common in homes, schools, workplaces, and public spaces.[10] The architecture of these devices and the software platforms they connect with are increasingly designed for user surveillance, and continuous daily exposure to them produces millions of digital traces, the electronic remnants of users' interactions with technology.[11]

---

8. *See* Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 12–14 (2018) (describing how retailers like Walmart collect vast troves of data from millions of consumers often without their knowledge or consent); *see also* Bernard Marr, *Really Big Data at Walmart: Real-Time Insights from Their 40+ Petabyte Data Cloud*, FORBES (Jan. 23, 2017, 2:06 AM), https://www.forbes.com/sites/bernardmarr/2017/01/23/really-big-data-at-walmart-real-time-insights-from-their-40-petabyte-data-cloud/#51be272c6c10 [https://perma.cc/7XWW-VK2A] (reporting that Walmart, the world's largest brick-and-mortar retailer, collects an estimated 2.5 petabytes of customer data per hour, which is 167 times the data held by the U.S. Library of Congress).

9. *See* MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did Up to 2003*, TECHCRUNCH (Aug. 4, 2010, 4:58 PM), https://techcrunch.com/2010/08/04/schmidt-data/ [https://perma.cc/2W5U-3PLX]; *see also* Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015, 2:19 AM), https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#7a08c56717b1 [https://perma.cc/S5B3-4779].

10. *See* Don Reisinger, *The Future Is Now: A Decade of Change in Consumer Electronics*, FORTUNE (Dec. 19, 2019, 11:00 AM), https://fortune.com/2019/12/19/2010s-retail-consumer-electronics/ [https://perma.cc/NAY5-C39T] ("In just the third quarter of 2019, 84.5 million wearables shipped worldwide . . . ."); AJ Dellinger, *Gifting a Smart Speaker This Holiday? Only One Passes Privacy Tests*, FORBES (Nov. 30, 2019, 11:00 PM), https://www.forbes.com/sites/ajdellinger/2019/11/30/gifting-a-smart-speaker-this-holiday-only-one-passes-privacy-tests/#14cb47dd29d8 [https://perma.cc/2G9W-CSVZ] (estimating that there are over 120 million smarts speakers in American homes).

11. *See, e.g.*, Charlie Warzel & Stuart A. Thompson, Opinion, *Twelve Million Americans Were Tracked Through Their Phones*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/opinion/tracking-phone-data.html [https://perma.cc/Y4RR-SSHK]; Drew Harwell, *Colleges Are Turning Students' Phones into Surveillance Machines, Tracking the Locations of Hundreds of Thousands*, WASH. POST (Dec. 24, 2019, 5:00 AM), https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/ [https://perma.cc/F4J7-9N83] ("One company that uses school WiFi networks to monitor movements says it gathers 6,000 location data points per student every day."); Ian Barnett, John Torous, Patrick Staples, Luis Sandoval, Matcheri Keshavan & Jukka-Pekka Onnela, *Relapse Prediction in Schizophrenia Through Digital Phenotyping: A Pilot Study*, 43 NEUROPSYCHOPHARMACOLOGY 1660, 1664–65 (2018) (describing a study in which up to one million data points were collected from the phones of people with schizophrenia each day); *The Tech Giants, Monopoly Power, and Public Discourse*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (Nov. 14, 2019), https://knightcolumbia.org/content/the-tech-giants-monopoly-power-and-public-discourse-1 [https://perma.cc/LTY7-N93M] (describing how internet services are designed as consumer surveillance platforms); Eben Moglen, President, Software Freedom L. Ctr., Why Freedom of Thought Requires Attention (May 7, 2019), https://www.softwarefreedom.org/news/2019/jun/17/transcript-for-republica19/ [https://perma.cc/PF54-YHWX] (reporting that gram for gram, smartphones contain more sensors than spy satellites, and they are pointed directly at the users).

Recent advances in data storage, processing power, and AI make it possible to find hidden connections between variables stored in large databases. Specifically, data scientists use machine learning, a sophisticated form of AI that excels at pattern recognition, to analyze digital traces and reveal what they say about people.[12]

So far, the legal community has paid little attention to EMD mining. Most existing scholarship appears in the medical literature and emphasizes potential benefits. Surprisingly, little work has been done to characterize potential harms, and even less attention has been paid to potential regulation. For example, one 2019 article from the medical literature promotes analyzing social media with AI to predict who will abuse prescription medications.[13] However, the article contains no mention of potential risks or how to mitigate them. Numerous articles contain similar omissions.[14] This Article fills those gaps while emphasizing the impact of EMD mining on vulnerable populations, such as children, racial minorities, undocumented immigrants, people with disabilities, and members of the LGBTQ community. These groups may be disproportionately impacted by EMD mining and the interventions it triggers. Without adequate safeguards and oversight, EMD mining will continue to disrupt traditional flows of health information while circumventing privacy, data protection, human rights, and antidiscrimination laws.

This Article contains three parts. Part I explains how internet-enabled software and devices collect digital traces and feed them into machine learning algorithms that mine EMD. It analyzes current and potential applications for EMD, which include medical diagnosis, personalized medicine, public health surveillance, targeted advertising, and social credit scoring. Part I concludes by analyzing the risks of unregulated EMD mining and EMD-based profiling. It explains why these practices threaten human safety, autonomy, privacy, and equality.

Part II proposes six different ways of conceptualizing EMD mining, including framing it as a form of regulatory arbitrage that circumvents health privacy laws, as a breach of contextual integrity, as the unlicensed practice of medicine, as the marketing and operation of unregulated medical devices, as unregulated medical research, and as a breach of fiduciary duties.

Part III offers preliminary suggestions for regulating EMD mining. Possible approaches include banning or limiting the collection of digital traces, regulating the

---

12. Marks, *Hidden Health Data*, *supra* note 4.

13. Abeed Sarker, Annika DeRoos & Jeanmarie Perrone, *Mining Social Media for Prescription Medication Abuse Monitoring: A Review and Proposal for a Data-Centric Framework*, 27 J. AM. MED. INFORMATICS ASS'N 315 (2020).

14. *See, e.g.*, Barnett et al., *supra* note 11; John Torous, Patrick Staples, Ian Barnett, Luis R. Sandoval, Matcheri Keshavan & Jukka-Pekka Onnela, *Characterizing the Clinical Relevance of Digital Phenotyping Data Quality with Applications to a Cohort with Schizophrenia*, NPJ DIGIT. MED., Apr. 6, 2018, at 1 (describing a study in which researchers tracked the behavior of sixteen outpatients with schizophrenia using a smartphone app that does not mention privacy or potential risks to patients); Gang Liu, Philip Henson, Matcheri Keshavan, Jukka Pekka-Onnela & John Torous, *Assessing the Potential of Longitudinal Smartphone Based Cognitive Assessment in Schizophrenia: A Naturalistic Pilot Study*, 17 SCHIZOPHRENIA RSCH.: COGNITION, Sept. 2019, at 1.

algorithms that transform digital traces into EMD, and restricting the purposes for which EMD may be used once it is mined. Each of these options has benefits and drawbacks. For instance, a ban on the collection of digital traces might limit consumer exploitation. However, it would also limit the functionality of some websites and apps while foreclosing socially beneficial uses for EMD, such as public health surveillance. One alternative is restricting who can mine EMD and narrowly defining the range of acceptable applications.

## I. EMERGENT MEDICAL DATA

This Part further defines emergent medical data (EMD) and explains why it should be viewed as a new type of health information distinct from traditional health data. It explains how data scientists create EMD by using AI to analyze large sets of relatively mundane digital information, often without people's knowledge or consent.

### *A. Understanding the Concept of EMD*

EMD is health information inferred by AI from the digital traces produced through people's interactions with technology.[15] On the surface, EMD appears similar to other forms of health information such as the data in a patient's medical record, which can be thought of as traditional medical data (TMD). Other examples of TMD include prescription records generated by pharmacists, X-ray images captured by radiologists, and billing information submitted by hospitals to health insurance companies.

Both EMD and TMD convey details about people's health, such as the medical conditions they have, the illicit drugs and prescription medicines they consume, and the surgical procedures they have undergone.[16] Moreover, both types of health information can be used to guide medical, public health, and business decisions. However, EMD and TMD differ in important ways.

First, they differ in how they are collected.[17] TMD is usually acquired in clinical settings, such as hospitals, where patients voluntarily convey it to healthcare providers to receive accurate diagnoses and effective treatment. In the clinical setting, patients trust that providers have their best interests in mind. Informed consent and trust have long been hallmarks of the doctor-patient relationship.[18] Physicians are required by law to inform patients of the foreseeable risks associated

15. Marks, *Hidden Health Data*, *supra* note 4.

16. Daniela Hernandez, *Artificial Intelligence Is Now Telling Doctors How to Treat You*, WIRED (June 2, 2014, 6:30 AM), https://www.wired.com/2014/06/ai-healthcare/ [https://perma.cc/HSA8-VWUB].

17. *Id.*

18. *See* Swastika Chandra, Masoud Mohammadnezhad & Paul Ward, *Trust and Communication in a Doctor-Patient Relationship: A Literature Review*, 3 J. HEALTHCARE COMMC'NS, July 19, 2018, at 1, 2.

with medical care, including the risks of foregoing such care.[19] Patients trust their physicians to inform them of those risks. Part of that trust is earned; physicians undergo over a decade of higher education, rigorous professional examinations, and licensure by state and federal entities.[20] It is within the context of this trusted relationship that patients volunteer TMD.

EMD is different. Instead of being obtained directly and voluntarily from patients, it is synthesized from digital traces that people continuously shed through their daily interactions with technology.[21] They need not visit a hospital or doctor's office.[22] EMD is often produced from digital traces collected by software and devices developed by companies that operate outside the healthcare system.[23] If organizations have access to digital traces and the AI necessary to process them, they can mine EMD, and there are thriving markets for this new commodity.[24] Because it is often mined by entities outside the healthcare system, EMD is regulated differently than TMD.[25] For instance, in the United States, TMD is covered by health privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) whereas EMD often is not.[26]

EMD also differs from TMD in that it often contains systematic errors and bias produced through the mining process.[27] TMD is collected through direct observation and examination of patients' bodies using processes that are subject to scientific and regulatory scrutiny.[28] It is obtained through tests and questionnaires developed over the course of decades or centuries and validated for accuracy, safety, and efficacy.[29] Those tools are administered by physicians, nurses, and other

---

19. *See* Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 917–18 (1994).

20. *See* Andrew H. Beck, *The Flexner Report and the Standardization of American Medical Education*, 291 JAMA 2139 (2004).

21. Marks, *Project Nightingale*, *supra* note 4.

22. *Id.* (describing how Google's partnerships with hospitals and healthcare system give it access to electronic medical records from which it can collect digital traces and mine emergent medical data).

23. *Id.*

24. *See id.*; Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/F7XX-WM4X] (describing the activities of hundreds of data brokers, including Acxiom, which monitors up to 10,000 different attributes on 2.5 billion people; the information includes both health data and non-health related digital traces that could be converted into EMD).

25. *Health Information Privacy Law and Policy*, HEALTHIT.GOV, https://www.healthit.gov/topic/health-information-privacy-law-and-policy [https://perma.cc/W7AF-LZFD] (Sept. 19, 2018).

26. *Id.*; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

27. Sara Hajian, Francesco Bonchi & Carlos Castillo, *Algorithmic Bias: From Discrimination Discovery to Fairness-Aware Data Mining*, KDD '16: PROC. 22D ACM SIGKDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING, Aug. 2016, at 2125.

28. *Id.*

29. *See, e.g.*, Douglas J. Lanska & Christopher G. Goetz, *Romberg's Sign: Development, Adoption, and Adaptation in the 19th Century*, 55 HIST. NEUROLOGY 1201 (2000) (describing the nineteenth-century development, adaptation, and adoption of a neurological test that is routinely used by healthcare providers today).

healthcare providers with medical training, licenses issued by state medical boards, and certifications bestowed by professional organizations. Moreover, there is strict regulatory oversight of healthcare delivery at the local, state, and national levels to ensure compliance with professional standards.[30] In contrast, anyone can collect digital traces and mine EMD. There is no special training or certification required, there is no regulatory oversight, and there is little or no scientific validation of relevant machine learning algorithms.

The lack of regulatory oversight and testing for safety, fairness, and efficacy is problematic because EMD is currently used to drive decisions that profoundly impact people's lives.[31] For example, Facebook mines EMD from its users to predict which people are most likely to attempt suicide.[32] If the company perceives the risk to be high, it sends police to users' homes.[33] These decisions and their adverse effects are discussed further in Part II. In short, people's health may be endangered and their rights may be infringed due to opaque and untested EMD-based inferences.[34] People's homes can be searched without warrants, and they can be hospitalized and treated against their will.[35] If the EMD-based predictions made about them are shared with third parties, individuals may be denied access to resources such as housing and employment, and insurance companies may increase their premiums.[36]

Why call health inferences derived from analyzing digital traces emergent medical data? Emergent means "arising unexpectedly."[37] It is an appropriate descriptor for health inferences mined from seemingly trivial digital traces because the connections between those traces and people's health arise unexpectedly. A recent landmark study on Facebook data found that the use of religious language,

---

30. *See, e.g.*, Medical Practice Act, CAL. BUS. & PROF. CODE §§ 2000–2596 (West 2018); N.Y. COMP. CODES R. & REGS. tit. 10, § 405.1 (2013) (hospital regulations).

31. *See* Natasha Singer, *In Screening for Suicide Risk, Facebook Takes on Tricky Public Health Role*, N.Y. TIMES (Dec. 31, 2018), https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html [https://perma.cc/7U7S-C422].

32. Mason Marks, Opinion, *Facebook Is Predicting if You'll Kill Yourself. That's Wrong*, GUARDIAN (Jan. 30, 2019, 6:00 AM), https://www.theguardian.com/commentisfree/2019/jan/30/facebook-is-predicting-if-youll-kill-yourself-thats-wrong [https://perma.cc/K9CT-6UGN].

33. *Id.*

34. Mason Marks, *Suicide Prediction Technology Is Revolutionary. It Badly Needs Oversight*, WASH. POST (Dec. 20, 2018, 12:03 PM), https://www.washingtonpost.com/outlook/suicide-prediction-technology-is-revolutionary-it-badly-needs-oversight/2018/12/20/214d2532-fd6b-11e8-ad40-cdfd0e0dd65a_story.html [https://perma.cc/E4XP-T6QB].

35. *Id.*

36. *See* Mason Marks, *Algorithmic Disability Discrimination*, *in* DISABILITY, HEALTH, LAW, AND BIOETHICS 242 (I. Glenn Cohen, Carmel Shachar, Anita Silvers & Michael Ashley Stein eds., 2020); Whitney Kimball, *Airbnb's Software Patent Rates Your Psychopathy Based on Your Social Media Activity*, GIZMODO (Jan. 7, 2020, 2:10 PM), https://gizmodo.com/airbnbs-software-patent-rates-your-psychopathy-based-on-1840855354 [https://perma.cc/X4D7-E47N] (describing a patent owned by Airbnb that claims a software program that scans renters' social media profiles and analyzes them to identify "negative personality or behavior traits" such as narcissism and psychopathy).

37. *Emergent*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/emergent [https://perma.cc/P4EK-8UH7] (last visited Jan. 11, 2021).

such as the words *god*, *pray*, *Jesus*, and *lord*, in social media is associated with having diabetes.[38] Earlier studies claimed Facebook posts could reveal which people had substance use disorders, and the photo filters people choose on Instagram could reveal whether they are depressed.[39] These latent connections between medical conditions and the language or filters used on social media are surprising. They emerged only after AI analyzed large sets of Facebook and Instagram data.[40]

Emergent also means "calling for prompt action: urgent."[41] Because EMD mining disrupts the traditional flow of health information and circumvents privacy, human rights, and antidiscrimination laws, it is urgent that scholars and legislators act quickly to understand and mitigate the risks. Moreover, lawmakers should act promptly to close gaps in existing legislation that allow EMD to be produced and used without regulatory oversight.

Technology companies are working diligently to shift social norms by encouraging people to remain connected to internet-enabled devices and share as much information as possible through as many platforms as possible.[42] Collectively, technology companies are normalizing the notion that people are under constant surveillance and are powerless to do anything about it. According to a 2019 Pew Research Center study, "Americans are concerned about how much data is being collected about them."[43] However, "very few Americans believe they understand what is being done with the data collected about them."[44] Entities that mine EMD exploit this lack of understanding because few consumers recognize that EMD mining is possible, and thus they cannot fully grasp the implications of allowing companies to harvest their digital traces. If social norms shift too quickly, and laws are not updated to protect people from EMD mining, then it may be too late for meaningful reform.

Why do organizations mine EMD? Some applications are in the public interest. EMD can be used for epidemiological research and public health surveillance.[45] In 2008, Google attempted to infer whether people had the flu by

38. Merchant et al., *supra* note 3, at 7.

39. Andrew G. Reece & Christopher M. Danforth, *Instagram Photos Reveal Predictive Markers of Depression*, 6 EPJ DATA SCI., no. 15, 2017, at 1; Philipp Kutter, *Your Facebook Activity Reveals a Lot About Your Drug Use*, VICE: MOTHERBOARD (June 13, 2017, 2:26 PM), https://www.vice.com/en_us/article/ev454p/social-media-drug-use-research-study [https://perma.cc/7QGH-GPFD].

40. Reece & Danforth, *supra* note 39; Kutter, *supra* note 39.

41. *Emergent*, *supra* note 37.

42. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59 (2013) (describing how emerging technologies are often disorienting and can shift social norms without people realizing it).

43. Brooke Auxier & Lee Rainie, *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*, PEW RSCH. CTR.: FACT TANK (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ [https://perma.cc/3ZX4-G3VZ].

44. *Id.*

45. *See* Catherine Kreatsoulas & S.V. Subramanian, *Machine Learning in Social Epidemiology: Learning from Experience*, 4 SMM - POPULATION HEALTH 347 (2018); Stephen

analyzing their internet searches.[46] Though this early attempt to infer health conditions from consumer behavior failed, tech companies, including Google and its parent company Alphabet, have expressed renewed interest in using AI to make health inferences.[47] On March 13, 2020, Alphabet's life sciences division, Verily, announced it was developing a website to screen people for symptoms of COVID-19.[48] After accessing the system, which requires an active Google Account, each user is assigned a COVID-19 risk score.[49] If the system deems users eligible, it refers them to drive-through testing centers operated by Verily.[50]

Other organizations, including government agencies and healthcare systems, mine EMD to predict which people might harm themselves or attempt suicide.[51] When Facebook perceives the risk of suicide to be high, it contacts police and guides them to users' homes, which Facebook refers to as a "wellness check."[52] In 2019, President Trump vowed to use similar technology to detect mental illness and prevent mass shootings.[53] One company called Gaggle (not to be confused with Google) already mines EMD from the homework and communications of five

---

J. Mooney & Vikas Pejaver, *Big Data in Public Health: Terminology, Machine Learning, and Privacy*, 39 ANN. REV. PUB. HEALTH 95 (2018).

46. Ed Pilkington & Alok Jha, *Google Predicts Spread of Flu Using Huge Search Data*, GUARDIAN (Nov. 12, 2008, 7:01 PM), https://www.theguardian.com/technology/2008/nov/13/google-internet [https://perma.cc/K7SK-MF9T].

47. *See* Honor Hsin, Menachem Fromer, Bret Peterson, Collin Walter, Mathias Fleck, Andrew Campbell, Paul Varghese & Robert Califf, *Transforming Psychiatry into Data-Driven Medicine with Digital Measurement Tools*, NPJ DIGIT. MED., Aug. 22, 2018, at 1 (describing Verily's plan to mine EMD and usher in a new era of digital psychiatry); Sidney Fussell, *The Next Data Mine Is Your Bedroom*, ATLANTIC (Nov. 17, 2018), https://www.theatlantic.com/technology/archive/2018/11/google-patent-bedroom-privacy-smart-home/576022/ [https://perma.cc/73PU-MPMT] (describing Google's patent on a smart home that mines digital traces to detect when people are developing health condition such as substance use disorders and Alzheimer's disease).

48. Google Communications (@Google_Comms), TWITTER (Mar. 13, 2020, 2:16 PM), https://twitter.com/Google_Comms/status/1238574670686928906 [http://web.archive.org/web/20210324075211/https://twitter.com/Google_Comms/status/1238574670686928906].

49. Jennifer Elias, *Alphabet's Verily Launches a Limited Coronavirus Screening Website*, CNBC (Mar. 16, 2020, 12:45 AM), https://www.cnbc.com/2020/03/15/alphabets-verily-says-it-will-launch-a-limited-coronavirus-testing-website-monday.html [https://perma.cc/U8BQ-85BF].

50. *Delivering COVID-19 Screening and Testing Through Project Baseline and Community-Based Sites*, VERILY, https://verily.com/solutions/covid-19-testing/ [https://perma.cc/N5D2-4U9H] (last visited Nov. 25, 2020).

51. Marks, *supra* note 32; *see* Chris Poulin & Gregory Peterson, *Artificial Intelligence Technology Combats Suicide in Veterans*, ELSEVIER CONNECT (Nov. 11, 2015), https://www.elsevier.com/connect/artificial-intelligence-app-combats-suicide-in-veterans [https://perma.cc/HZT2-7LBQ]; Brett Ruskin, *Feds to Search Social Media Using AI to Find Patterns of Suicide-Related Behaviour*, CBC (Jan. 2, 2018, 7:00 AM), https://www.cbc.ca/news/canada/nova-scotia/feds-to-search-social-media-using-ai-to-find-patterns-of-suicide-related-behaviour-1.4467167 [https://perma.cc/2EEL-GDYX].

52. Marks, *supra* note 32.

53. Sigal Samuel, *Trump Wants to "Detect Mass Shooters Before They Strike." It Won't Work.*, VOX (Aug. 7, 2019, 12:40 PM), https://www.vox.com/future-perfect/2019/8/7/20756928/trump-el-paso-dayton-mass-shooting-ai-social-media [https://web.archive.org/web/20190807170638if_/https://www.vox.com/future-perfect/2019/8/7/20756928/trump-el-paso-dayton-mass-shooting-ai-social-media].

million students to infer their risk of suicide and gun violence.[54] Though these applications for EMD may seem socially desirable, they have significant limitations, and they put people at risk for discrimination and physical and emotional harm.

EMD can also be mined within the healthcare system from the digital traces stored in electronic health records, collected through surveillance of doctor-patient interactions, and harvested from patients' social media accounts, medical devices, wearables, and smartphone apps.[55] Some technology companies, including Google, are forming partnerships with hospitals and healthcare organizations to store patient records "in the cloud" where AI can analyze the digital traces contained therein and make inferences regarding patient health (and the health of the populations whose records are stored in the cloud).[56]

The remainder of this Section explains how EMD is mined by describing a landmark study conducted at the University of Pennsylvania (the "Penn Study").[57] In this study, the online behavior of a large population of Facebook users was analyzed, and researchers discovered surprising correlations between the use of certain words and phrases and various medical conditions.[58] For example, they learned that the use of religious language on Facebook is linked to having diabetes, and the use of words that convey hostility is linked to having substance use disorders.[59]

It is worth noting that EMD mining would be impossible without recent advances in artificial intelligence. The term "AI" describes a broad set of software tools such as machine learning, a type of software that can learn on its own and excel at pattern recognition. Machine learning is adept at identifying patterns in large

---

54. Caroline Haskins, *Gaggle Knows Everything About Teens and Kids in School*, BUZZFEED NEWS (Nov. 1, 2019, 3:48 PM), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education [https://perma.cc/HGR8-9F4N].

55. *See* Colin G. Walsh, Jessica D. Ribeiro & Joseph C. Franklin, *Predicting Risk of Suicide Attempts Over Time Through Machine Learning*, 5 CLINICAL PSYCH. SCI. 457, 459 (2017); Igor Bonifacic, *Amazon AI Generates Medical Records from Patient-Doctor Conversations*, ENGADGET (Dec. 2, 2019), https://www.engadget.com/2019/12/02/amazon-transcribe-medical-ai-aws/ [https://perma.cc/4S2F-VM4S] (describing Amazon's Transcribe Medical, a service that records doctor-patient conversations and transcribes them for addition to medical records, allowing EMD to be mined from those conversations, including portions that are not overtly medical); Press Release, Cedars-Sinai, Cedars-Sinai Taps Alexa for Smart Hospital Room Pilot (Feb. 25, 2019), https://www.cedars-sinai.org/newsroom/cedars-sinai-taps-alexa-for-smart-hospital-room-pilot/ [https://perma.cc/K7HH-MK4Z] (announcing a Cedars-Sinai Medical Center pilot program in which an Amazon Alexa-powered platform called Aviva was placed in more than 100 hospital rooms, allowing patients to use voice commands to contact medical staff and control elements of their rooms).

56. Bruce Japsen, *Mayo Clinic, Google Partner on Digital Health Analytics*, FORBES (Sept. 10, 2019, 10:13 AM), https://www.forbes.com/sites/brucejapsen/2019/09/10/mayo-clinic-google-partner-on-digital-health-analytics/#23e0e52036e7 [https://perma.cc/9A65-GDLD] (describing Google's ten-year deal with the Mayo Clinic through which Google will gain access to the patient records, and reporting that other tech companies, such as Microsoft and IBM, are forming similar partnerships).

57. Merchant et al., *supra* note 3.

58. *Id.* at 2.

59. *Id.* at 7.

data sets that are impossible for humans to see. It can be further subdivided into other types of AI, including deep learning, where artificial neural networks inspired by brain structures learn from massive data sets, and natural language processing, where machine learning algorithms interpret human language.[60] Other authors have defined these terms in detail, and they will not be discussed further here.[61] Suffice to say that machine learning is a sophisticated form of AI that can extend our ability to see connections between data points in large data sets. This characteristic is what makes EMD mining possible.

EMD is mined and applied through a multistage process consisting of the following steps:[62]

1. Collection Stage 1: Collection of digital traces and health information, or proxies for health information, from a population of individuals (the "training population").
2. Training Stage: Training of naïve EMD mining algorithms using data collected from the training population.
3. Collection Stage 2: Collection of digital traces from a second population of individuals from which EMD will be mined (the "deployment population").
4. Deployment Stage: Deployment of trained EMD mining algorithms to transform the deployment population's digital traces into EMD using connections identified during the training stage.
5. Application Stage: Use of the resulting EMD to draw conclusions about the deployment population (e.g., sorting its members into health-related categories, scoring and ranking them, etc.)

In the EMD mining process, digital traces are collected from two distinct populations. The first population serves as the training population, which is used to train naïve EMD mining algorithms. By providing those algorithms with the training population's digital traces and the health conditions of its members, researchers prepare the algorithms to discover hidden connections (statistical correlations) between specific digital traces obtained from the population, such as words and phrases used on Facebook and certain health conditions in that population.

Once the EMD mining algorithms have been trained, the digital traces of a second population (the "deployment population") can be collected. For the sake of

60. *See generally* Dina Moussa & Garrett Windle, Literature Review, *From Deep Blue to Deep Learning: A Quarter Century of Progress for Artificial Minds*, 1 GEO. L. TECH. REV. 72 (2016); Peng Lai "Perry" Li, Technology Explainers, *Natural Language Processing*, 1 GEO. L. TECH. REV. 98 (2016).

61. *E.g.*, David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 677 (2017).

62. These stages represent a simplified description of the EMD mining process that has been adopted for clarity. Other authors might define the stages differently or include additional stages.

simplicity, assume that this population is not used to train the algorithms.[63] Instead, the deployment population's digital traces are fed into the trained algorithms, and based on the connections identified by analyzing the training population, the algorithms make inferences and predictions about members of the deployment population.

In the final stage of EMD mining (the "application stage"), health inferences made about the deployment population may be used for a variety of purposes such as drawing conclusions about their health, designing personalized treatment programs for them, directing targeted advertisements to them based on their health conditions, or sorting them into categories for purposes of risk mitigation, for example, in the insurance industry.

The Penn Study illustrates how EMD is mined from digital traces and demonstrates how powerful it can be.[64] It linked the Facebook data (the digital traces) of 999 consenting individuals (the study's training population) to the data contained in their electronic health records.[65]

The study investigators wanted to answer two research questions: (1) "Can we predict individuals' medical diagnoses from language posted on social media?" and (2) "Can we identify specific markers of disease from social media posts?"[66] In other words, they wanted to know if it was possible to mine EMD from Facebook posts, and they wanted to identify words and phrases on Facebook that are correlated with health conditions. During the study, researchers collected "949,530 Facebook status updates containing 20,248,122 words" posted to Facebook by the 999 study participants.[67]

To infer people's medical diagnoses from social media posts, the researchers first built an AI model for inferring health conditions.[68] Model training is a preliminary step of EMD mining.[69] To build the model, the researchers first collected data. They obtained the social media activity and health record data of adults receiving medical care at an urban academic health system.[70] Of 1772 people who consented to share their data, the researchers chose 999 whose posts over the previous five years amounted to over 500 words each.[71] "For many projects, this

63. In reality, the digital traces collected from the deployment population may also serve to further train the algorithms, updating the correlations they are capable of recognizing.

64. *See* Merchant et al., *supra* note 3.

65. *Id.* at 1.

66. *Id.* at 2.

67. *Id.*

68. *See* Lehr & Ohm, *supra* note 61, at 672–73, 677 ("Machine-learning algorithms predict or estimate *something*, and the first step of any analysis is to define what that something should be and how it should be measured. . . . Once data scientists have conceptualized the goal of the machine-learning system and reduced that goal to a specified outcome variable, the data themselves have to be assembled — both for the outcome variable and the myriad input variables.").

69. *See id.* at 695.

70. Merchant et al., *supra* note 3, at 2.

71. *Id.*

[first collection stage] can be the most time-consuming stage, and it also holds enormous consequences; as commenters have noted previously, an algorithm is, at the end of the day, only as good as its data."[72]

After enrolling participants, the researchers had a large database containing both the medical information (in the form of 21 health conditions) and social media data (in the form of Facebook posts) of 999 people.[73] They had the raw materials necessary to train their predictive model. However, they lacked information regarding which pieces of social media data (i.e., which digital traces) were correlated with each of the 21 health conditions of interest. To find those connections and build a model for large-scale mining of EMD from Facebook data, the researchers turned to natural language processing, a type of machine learning that enables software to read and interpret human language.[74] Using natural language processing, "each participant's language was encoded as a 700 dimensional *patient language encoding*."[75] *In other words, machine learning algorithms read each study participant's Facebook posts and described them using 700 numbers.*[76] *This task's complexity illustrates why EMD mining exceeds human capabilities and some form of AI is necessary.*

The researchers built three different models for predicting health conditions from social media content. The first model looked solely at Facebook language in the form of unigrams (single words), bigrams (word pairs), and topics (clusters of words that share a common theme, such as religious language or language related to family).[77] The second model looked solely at demographic data, including age, sex, and race.[78] The third model used both language and demographic data.[79] After the three prediction models were built, they could be deployed to test their accuracy.[80]

"Prediction accuracy was evaluated using the area under the receiver operating characteristic curve (AUC), a measure of discrimination in which a value of 0.5 is expected due to chance, 0.6 is considered moderate, and above 0.7 is considered a strong prediction from a behavior."[81] Depending on the predictive model used, some conditions, such as genitourinary conditions, pregnancy, hypertension, and diabetes, had very high predictability (AUC above 0.7).[82] Other conditions, such as coagulopathy, substance use disorders, and psychosis, had relatively low predictability regardless of the model used; however, they still performed better than

72. Lehr & Ohm, *supra* note 61, at 677.
73. Merchant et al., *supra* note 3, at 2.
74. *See* Julia Hirschberg & Christopher D. Manning, *Advances in Natural Language Processing*, 349 SCI. 261, 261 (2015).
75. Merchant et al., *supra* note 3, at 2.
76. *Id.*
77. *Id.* at 3–4.
78. *Id.* at 5.
79. *Id.*
80. *Id.* at 5–6.
81. *Id.* at 6.
82. *Id.* at 5.

chance (AUC above 0.5).[83] Some conditions, such as sexually transmitted diseases, respiratory problems, obesity, and alcoholism, showed moderated predictability (AUC above 0.6).[84]

The power of these predictive models is impressive. The Penn Study shows that if researchers had access to people's social media timelines, researchers could deploy the models to mine EMD and infer which people have each medical condition (in many cases with relatively high accuracy).[85] Having access to medical records was essential to the study's success, and without medical records on which to train their algorithms (i.e., to build their models), the researchers could not have achieved such high accuracy.

It is instructive to compare the methods of the Penn Study to those of Facebook. The company currently uses AI to scan user-generated content on its site and predict which users are most likely to attempt suicide.[86] Like the researchers in the Penn Study, Facebook uses natural language processing to make its predictions.[87] However, unlike medical researchers, Facebook lacks access to health records.[88] As a result, it must cut corners during the training phase in which it builds its predictive models. Cutting corners is one of the sources of systematic inaccuracies that can plague EMD mining algorithms.

In 2018, Facebook was in talks to obtain patient records from university medical centers, including Stanford.[89] However, after the Cambridge Analytica scandal made international news, Facebook chose not to pursue the project.[90] Because Facebook lacks medical records, it cannot train its suicide prediction algorithms using actual medical data. Instead, it must use proxies for medical information as its training data during the model training stage, which inevitably affects the accuracy of its AI-based suicide predictions.[91] For example, instead of using suicide data derived from medical records, Facebook relies on reports from its community of users to train its algorithms.[92]

---

83. *Id.*

84. *Id.*

85. *Id.* at 7–9.

86. Marks, *supra* note 6, at 107–08.

87. *See, e.g.*, *Breaking Down Language Barriers*, FACEBOOK RSCH., https://research.fb.com/category/natural-language-processing-and-speech/ [https://perma.cc/8HJG-TA7D] (last visited Nov. 25, 2020).

88. *See* David Meyer, *Facebook Decides Now's Not a Great Time to Harvest Patients' Medical Data*, FORTUNE (Apr. 6, 2018, 12:30 AM), https://fortune.com/2018/04/06/facebook-medical-data-sharing-hospitals/ [https://perma.cc/HW5X-SDTR].

89. *Id.*

90. *Id.*

91. Marks, *supra* note 6, at 110.

92. *See id.* at 107–10; Vanessa Callison-Burch, Jennifer Guadagno & Antigone Davis, *Building a Safer Community with New Suicide Prevention Tools*, FACEBOOK (Mar. 1, 2017), https://about.fb.com/news/2017/03/building-a-safer-community-with-new-suicide-prevention-tools/ [https://perma.cc/A9KH-A7KV].

Facebook starts with user reports, submitted to its content moderation team, regarding posts that users perceived as concerning and likely to reflect a risk of self-harm.[93] For instance, a user might post a message saying, "I can't take this pain anymore, I'm done," and a friend or family member of the user might report the message to Facebook's team out of concern that the user might harm himself. Facebook will escalate the case to a human content moderator who determines whether an intervention is necessary, such as sending police to the user's home to perform a wellness check.[94] If such an intervention is made, Facebook uses that outcome as a proxy for a high risk of suicide, and it uses the original post, "I can't take this pain anymore, I'm done," as training data for its predictive model.[95] Once the model is deployed, it will scan the user-generated content of billions of users, searching for language similar to the post it used as proxy data during the training phrase.[96]

Using proxy data to train EMD mining algorithms introduces inaccuracies into Facebook's suicide predictions.[97] Model accuracy is highly dependent on the quality of input data, and low-quality input data produces low quality inferences and EMD. This relationship is often described as the garbage in, garbage out phenomenon.[98] A lack of accuracy in EMD mining algorithms can have dangerous effects, particularly when they are deployed at scale on Facebook's massive global platform with over 2.7 billion active users, and they trigger real world interventions such as home visits from police.[99] Several other internet platforms use proxies to train suicide prediction algorithms.[100] These platforms and the adverse effects of using proxy data to mine EMD will be discussed further in Part II.

Because Facebook lacks access to health records, its approach to EMD mining and suicide prediction differs from that of medical researchers who have that access. Dr. Colin Walsh and his colleagues at Vanderbilt University used 5,167 medical

---

93. Marks, *supra* note 6, at 107–10.

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.*

98. HILLARY SANDERS & JOSHUA SAXE, GARBAGE IN, GARBAGE OUT: HOW PURPORTEDLY GREAT ML MODELS CAN BE SCREWED UP BY BAD DATA 2 (2017), https://paper.seebug.org/papers/Security%20Conf/Blackhat/2017_us/us-17-Sanders-Garbage-In-Garbage-Out-How-Purportedly-Great-ML-Models-Can-Be-Screwed-Up-By-Bad-Data-wp.pdf [https://perma.cc/USM3-NKB8] ("If we're unable to accurately simulate the data we want our model to eventually perform on, we can't be sure of how it will do on deployment - which is essential.").

99. *See infra* notes 201–215 and accompanying text; Chris Mills Rodrigo, *Critics Fear Facebook Fact-Checkers Losing Misinformation Fight*, HILL (Jan. 20, 2020, 7:30 AM), https://thehill.com/policy/technology/478896-critics-fear-facebook-fact-checkers-losing-misinformation-fight [https://perma.cc/U3L7-ETTT] (reporting that Facebook has 2.4 billion active monthly users); Etan Vlessing, *Facebook Tops 2.7 Billion Monthly Active Users in Latest Quarter*, HOLLYWOOD REP. (July 30, 2020, 1:20 PM), https://www.hollywoodreporter.com/news/facebook-second-quarter-earnings-rise-continued-user-growth-1305161 [https://perma.cc/2GVG-AU64].

100. Marks, *supra* note 6, at 107.

records to predict suicide.[101] Instead of relying on proxy data intended to reflect suicidal thoughts, they used actual suicide data derived from patient records.[102] The researchers reported the accuracy of their predictive models in terms of accuracy under the curve (AUC).[103] Traditional methods of suicide prediction, such as pen and paper questionnaires administered by healthcare providers, may be little more accurate than a coin flip (a probability of about 50% or 0.50).[104] For patients attempting suicide for the first time, Walsh reported AUC values ranging from 0.82 "at 7 days prior to suicide attempts" to 0.75 "at 720 days prior to suicide attempts."[105] In other words, the predictions became more accurate when suicide attempts were imminent. As described by the Penn Study, an AUC value above 0.7 is considered a strong prediction.[106]

There are other important differences between the Penn and Vanderbilt studies and Facebook's suicide predictions. The research protocol for each academic study was approved by the relevant university's Institutional Review Board (IRB).[107] In contrast, Facebook's use of EMD mining algorithms apparently received no independent ethics review. Facebook does implement a review process; however, it bears little resemblance to those implemented in academic research settings.[108] Unlike academic IRBs, Facebook's ethics review committee is not independent, and consequently, it should not be viewed as an IRB.[109] It is composed entirely of Facebook employees, and its review of company research is optional; projects are submitted for review at the discretion of Facebook staff.[110]

Facebook is not the only tech company that lacks access to medical records and makes suicide predictions without independent ethics review, using AI trained on proxy data. Crisis Text Line is an international crisis response platform that analyzes text messages to predict suicide and other forms of self-harm.[111] Founded in 2013, the platform recently expanded operations to the United Kingdom, where it is called Shout.[112] The service received a flurry of press coverage when it was

101. Walsh et al., *supra* note 55, at 457.
102. *Id.* at 459.
103. *Id.*
104. *Id.* at 457.
105. *Id.* at 463.
106. Merchant et al., *supra* note 3, at 6.
107. *Id.* at 2; Walsh et al., *supra* note 55, at 460.
108. Marks, *supra* note 6, at 109.
109. *See id.*
110. Molly Jackman & Lauri Kanerva, *Evolving the IRB: Building Robust Review for Industry Research*, 72 WASH. & LEE L. REV. ONLINE 442, 452 (2016).
111. *See* Megan Rose Dickey, *Loris.ai, a Crisis Text Line Spin-out, Raises $2 Million to Help Companies Have Hard Conversations*, TECHCRUNCH (Feb. 6, 2018, 6:00 AM), https://techcrunch.com/2018/02/06/loris-ai-a-crisis-text-line-spin-out-raises-2-million-to-help-companies-have-hard-conversations/ [https://perma.cc/4G2H-N7V8].
112. Victoria Murphy, *Kate Middleton, Meghan Markle, Prince William, and Prince Harry Team Up to Launch Shout, a Crisis Text Line*, TOWN & COUNTRY (May 9, 2019), https://www.townandcountrymag.com/society/tradition/a27423462/kate-middleton-prince-william-meghan-markle-prince-harry-launch-shout/ [https://perma.cc/Z3MF-DWAY].

publicized by members of the British royal family.[113] Another platform that makes suicide predictions is Objective Zero, a smartphone app marketed to veterans.[114] It uses GPS location data to infer depression and suicidal thoughts.[115] Like Facebook, Crisis Text Line and Objective Zero engage in EMD mining to predict suicide without having access to health records and without subjecting their methods to independent ethics review.[116]

Compared to Facebook and other commercial platforms that mine EMD, Google has been more aggressive and successful in its attempts to obtain medical records. In 2017, "the University of Chicago Medical Center announced a partnership to share patient data with Google . . . . [T]he alliance was promoted as a way to unlock information trapped in electronic health records and improve predictive analysis in medicine."[117] Today, Google has at least twenty partnerships with prominent hospitals, including the Mayo Clinic and the Cleveland Clinic, that provide it with access to medical information, potentially serving as a source of digital traces to train its EMD mining algorithms.[118]

Google's sister company, Verily, recently partnered with Emory University, and Google's parent company, Alphabet, has data-sharing partnerships with six other University health systems through a program called Project Baseline.[119] These partnerships are notable because Alphabet owns Deep Mind, a U.K.-based AI company known for groundbreaking achievements that showcase the power of machine learning.[120] In other words, Alphabet and Google are positioning

---

113. *Id.*

114. Eillie Anzilotti, *This App Connects Veterans in Crisis with Other Veterans Who Are Willing to Talk*, FAST CO. (July 24, 2017), https://www.fastcompany.com/40439892/this-app-connects-veterans-in-crisis-with-other-veterans-who-are-willing-to-talk [https://perma.cc/VPG6-DNRR].

115. Jesse L, *Announcing the Winner of Our First 'Foursquare for Good' Program*, MEDIUM (Nov. 27, 2018) (quoting Kayla Bailey, CTO, Objective Zero), https://medium.com/foursquare-direct/announcing-the-winner-of-our-first-foursquare-for-good-program-c512f62e966e [https://perma.cc/U2EF-SB4V] ("Objective Zero has developed a platform and designed a machine learning algorithm to truly preempt and respond to suicidal ideation . . . [by] leverag[ing] geolocation technology to detect when veterans are most at risk and deliver location-based resources to them.").

116. Marks, *Hidden Health Data*, *supra* note 4.

117. Daisuke Wakabayashi, *Google and the University of Chicago Are Sued Over Data Sharing*, N.Y. TIMES (June 26, 2019), https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html [https://perma.cc/7QY9-7FL4].

118. *See* Marks, *Project Nightingale*, *supra* note 4.

119. Jackie Drees, *Alphabet's Verily Adds Mayo Clinic, Duke University Health to Consortium for Clinical Research*, BECKER'S HOSP. REV. (May 20, 2019), https://www.beckershospitalreview.com/healthcare-information-technology/alphabet-s-verily-adds-mayo-clinic-duke-university-health-to-consortium-for-clinical-research.html [https://perma.cc/W83M-3DW8] (reporting on Verily's data-sharing partnerships with the Mayo Clinic, Duke University Health System, Vanderbilt University Medical Center, the University of Mississippi Medical Center, Regional Health, and the University of Pittsburgh).

120. *See* Jason Daley, *A.I. Mastered Backgammon, Chess and Go. Now It Takes on StarCraft II*, SMITHSONIAN MAG. (Oct. 30, 2019), https://www.smithsonianmag.com/science-nature/deepmind-ai-mastered-backgammon-chess-game-go-now-takes-on-starcraft-ii-180973430/ [https://perma.cc/S2W6-7B9V]; Sissi Cao, *Google's DeepMind AI Beats Humans Again—This Time by Deciphering Ancient*

themselves to be the world's leaders in EMD mining and predictive analytics in healthcare generally. Google reportedly has access to the medical records of tens of millions of people in "at least three quarters of U.S. states."[121]

Alphabet and Google's intent to mine EMD is more than theoretical. Google has patented a smart home that can purportedly collect digital traces from occupants to infer their medical conditions and predict their future health.[122] In 2018, a team of scientists employed by Verily published an article (the "Verily article") on the future of psychiatry.[123] It articulates the potential advantages of AI-mediated health inferences over traditional methods of observing people with mental health conditions.[124]

The following Section describes a variety of applications for EMD in healthcare and business.

### *B. Medical, Public Health, and Commercial Applications of EMD*

EMD is potentially useful in a variety of settings, including medical research, personalized medicine, public health surveillance, and advertising. This Section describes current and potential uses for EMD in these contexts.

#### *1. Medical Research*

EMD mining augments traditional research methods by taking data that might previously have gone to waste and analyzing it for medical significance. Specifically, electronic surveillance paired with natural language processing allows researchers to utilize the entire medical record, including entries that previously would have been ignored or considered unimportant.

Instead of relying on manually inputted data, doctors can use smart speakers to capture entire conversations with patients, which are automatically transcribed into health records. Once there, the information can be analyzed by AI to squeeze out any potential medical significance that might otherwise have been overlooked. For example, if during a conversation a patient said, "I am so blessed to have my dog Sally; she is such a good girl," the physician might have excluded that information from the chart. If the physician did decide to include it, the entry likely

---

*Greek Text*, OBSERVER (Oct. 21, 2019, 12:59 PM), https://observer.com/2019/10/google-deepmind-ai-machine-learning-beat-human-ancient-greek-text-prediction/ [https://perma.cc/CKD2-VUVZ].

121. Rob Copeland, Dana Mattioli & Melanie Evans, *Paging Dr. Google: How the Tech Giant Is Laying Claim to Health Data*, WALL ST. J. (Jan. 11, 2019, 12:15 AM), https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700 [https://perma.cc/8M9Y-F88V] (reporting results of the Wall Street Journal's analysis of Google's contractual agreements with healthcare organizations including a deal with the Mayo Clinic that is estimated to provide access to 9.9 million records spread across four states, a partnership with Ascension involving 50 million records from twenty-five states, and a deal with the University of Chicago involving 2.3 million records from one state).

122. *See* Fussell, *supra* note 47.

123. Hsin et al., *supra* note 47.

124. *Id.*

would have excluded the patient's religious language and may have instead focused only on the fact that the patient has a dog and that it brings the patient joy. Even if the religious portion, "I am so blessed," was included in the record, medical researchers would likely ignore it if they included this patient in their research. However, if the sentence was captured by surveillance technologies, such as smart speakers, and analyzed by AI, then the religious language could be included in the analysis and might be identified as a predictor of diabetes as discovered by the Penn Study.[125]

Through EMD mining, health researchers can also study behaviors that occur outside the clinical setting which have traditionally been difficult to observe. Consider the many behaviors and activities that people engage in between doctor's visits. These behaviors make up a seemingly infinite number of variables that can now largely be captured by the internet-enabled devices that surround us and collect digital traces. Some researchers call the resulting cache of data the "human screenome" (a play on the term human genome), and they have proposed a Human Screenome Project (analogous to the Human Genome Project) to study it.[126] However, the scope of digital traces collected by surveillance technologies is much broader than people's interactions with the screens of computers, smartphones, and televisions. The variables that can be used to mine EMD include offline retail purchases, exercise habits, alcohol consumption, gambling, drug use, work habits, and social behavior. Information on these variables is collected by a variety of technologies, such as surveillance cameras, key cards, and biometric scanners, that do not involve screen usage.

One group uses the term "human digitome" to describe the digital traces collected by various technologies.[127] Another group refers to the entire collection of a person's digital traces as their "digital phenotype," and the process of collecting it as digital phenotyping, which they define as the "moment-by-moment quantification of the individual-level human phenotype *in situ* using data from personal digital devices."[128] *In situ* means "in position" or "on site," and digital phenotyping allows researchers and clinicians to study people in their natural environments: at home, at work, in school, and anywhere in between.[129] In biology,

125. Merchant et al., *supra* note 3.

126. Byron Reeves, Thomas Robinson & Nilam Ram, *Time for the Human Screenome Project*, NATURE (Jan. 15, 2019), https://www.nature.com/articles/d41586-020-00032-5 [https://perma.cc/URC3-XY77].

127. *Medable Joins the American Heart Association's Center for Health Technology & Innovation Innovators Network to Enhance Digital Real-World Evidence Patient Registries Powering a Human Heart Digitome*, BUS. WIRE (Aug. 12, 2019, 8:30 AM), https://www.businesswire.com/news/home/20190812005043/en/Medable-Joins-American-Heart-Association%E2%80%99s-Center-Health [https://perma.cc/FE74-AQZM].

128. Jukka-Pekka Onnela & Scott L. Rauch, *Harnessing Smartphone-Based Digital Phenotyping to Enhance Behavioral and Mental Health*, 41 NEUROPSYCHOPHARMACOLOGY 1691, 1691 (2016).

129. *In Situ*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/in%20situ [https://perma.cc/6GRD-2PQ9] (last visited Feb. 20, 2021) (defining "in situ" as "in the natural or original position or place").

a phenotype is "the observable characteristics or traits of an organism that are produced by the interaction of the genotype [the organism's genes] and the environment."[130] A digital phenotype consists of the observable properties of an organism produced by the combined influence of its genes, environmental factors, and its interactions with digital technologies. In other words, the digital phenotype is an electronic reflection of one's genotype and phenotype. Regardless of the label applied to the collection of health inferences derived from one's digital traces, EMD mining is the tool that allows those inferences to be made.

In the past, unless a research subject was continuously observed, for example, in an inpatient unit of a hospital, physicians and researchers had to rely on the subject's self-reports derived from memory and personal documentation. However, surveillance technologies that collect digital traces can automatically and continuously monitor research subjects and record their behaviors. The resulting rich data set, which was previously burdensome or impossible to obtain, can now be acquired and utilized to advance medical science.

Certain conditions and patient populations have historically been difficult to study, and advancements in their care have been slow and infrequent. For instance, people with schizophrenia are prone to episodes of psychosis, which makes obtaining accurate self-reports of their behavior challenging. Other individuals, such as people with Alzheimer's and other forms of dementia, may have difficulty remembering their behaviors and reporting them accurately to healthcare providers.[131]

EMD mining and digital phenotyping could make it easier for researchers to study these populations by identifying environmental triggers that exacerbate conditions, improving the odds of finding new treatments, and customizing existing treatments to patients. Instead of relying on the patient's self-reports, clinicians can employ surveillance technologies, consisting of personal sensors that observe them continuously, and the resulting data can be mined to identify which factors improve their condition and which do not. According to some researchers, "personal sensing . . . holds great promise as a method for conducting mental health research and as a clinical tool for monitoring at-risk populations."[132] One research group used a smartphone app to collect up to one million data points from individuals with schizophrenia each day.[133] Members of this group advocate for involving Facebook and other internet platforms in digital phenotyping.[134] They suggest that

---

130. *Phenotype*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/phenotype [https://perma.cc/JLX3-TKZK] (last visited Feb. 20, 2021).

131. Eric Dishman & Maria C. Carrillo, *Perspective on Everyday Technologies for Alzheimer's Care: Research Findings, Directions, and Challenges*, 3 ALZHEIMER'S & DEMENTIA 227 (2007).

132. David C. Mohr, Mi Zhang & Stephen M. Schueller, *Personal Sensing: Understanding Mental Health Using Ubiquitous Sensors and Machine Learning*, 13 ANN. REV. CLINICAL PSYCH. 23, 23 (2017).

133. John Torous, Matcheri Keshavan, Jukka-Pekka Onnela, Patrick Staples & Ian Barnett, *M48. Digital Phenotyping in Schizophrenia Using Smartphones*, 43 SCHIZOPHRENIA BULL. S228 (2017).

134. Ian Barnett & John Torous, *Ethics, Transparency, and Public Health at the Intersection of Innovation and Facebook's Suicide Prediction Efforts*, 170 ANNALS INTERNAL MED. 565 (2019).

platforms could follow individual users over time and make continuous observations and predictions regarding their mental health.[135]

The potential benefits of ubiquitous sensing and EMD-based medical research include identifying new markers of health and disease that can eventually be used for health screening, discovering new drug targets, and identifying areas to which research funding should be directed.[136] According to some psychiatrists, "digital measurement tools may similarly refine traditional boundaries of psychiatric diagnosis by potentially stratifying patient characteristics in a way that is clinically actionable."[137] In other words, digital phenotyping may help define new subtypes of human physiology and disease.

There are several potential downsides to using EMD for medical research. The ease with which data can be collected may promote exploitation of people for commercial gain. In the past, health research could only be conducted by trained specialists who must comply with ethical rules and professional standards. However, EMD mining is democratizing the research process, and healthcare professionals no longer have a monopoly. Tech companies with no previous involvement in health research can now mine EMD from consumers and conduct their own research studies. In doing so, they avoid the need to comply with health privacy laws, ethical standards, and potentially even international human rights treaties.

There is also a risk that tech companies will take what they learn mining EMD from electronic health records and use that knowledge to mine EMD from users of their commercial products such as Gmail, YouTube, Facebook, and Amazon Alexa.[138] This concern has been raised with respect to Google and Alphabet's many partnerships with hospitals and healthcare systems.[139]

### *2. Personalized Medicine*

There are clear benefits to using EMD to aid medical research. If data that might otherwise go to waste can be utilized, efficiency may be increased, and the quality of medical care could be improved. Furthermore, if EMD-based research results in the discovery of clinically significant disease subtypes, then EMD mining could be used clinically to identify people with those subtypes and prompt the appropriate treatment. Proponents of digital phenotyping argue that it could allow doctors to detect and diagnose disease early using commonly available tools such as cellphones, wearables, and smart homes.[140]

---

135. *Id.*

136. Hsin et al., *supra* note 47, at 1.

137. *Id.* at 2.

138. Marks, *Project Nightingale*, *supra* note 4 (describing how Google's medical record sharing deal with Ascension, the largest American non-profit healthcare organization, provides the tech company with a rich source of emergent medical data).

139. *Id.*

140. *Id.*

One risk is that healthcare providers will come to rely on EMD-based predictions instead of their own intuitions, training, and experience. Similar concerns have been raised regarding the use of AI-inferences within the criminal justice system.[141] Even if judges know that there is inherent inaccuracy in sentencing or parole algorithms, they might be nudged in one direction by AI-generated predictions and recommendations.[142] In healthcare contexts, it has been suggested that overreliance on AI might promote the de-skilling of physicians, where their ability to analyze problems independently degrades due to a dependence on software based decision-making aids.[143]

Reliance on EMD to guide clinical decision-making might also promote discrimination against people flagged by AI to be at risk for certain behaviors or conditions, such as depression or alcoholism.[144] Research suggests that healthcare providers can be biased against people with these so-called diseases of despair.[145] People with chronic pain might be predicted by an algorithm to abuse prescription medicines, and based on that prediction, doctors may deny them adequate pain control.[146] Pain management programs may require patients to sign up for digital surveillance and automated substance use disorder prediction as a prerequisite for treatment. Prescription drug monitoring databases administered by state public health departments already use AI to analyze prescribing information to predict who will abuse controlled substances.[147] They may soon incorporate other types of

---

141. *See* Karen Hao, *AI Is Sending People to Jail—and Getting It Wrong*, MIT TECH. REV. (Jan. 21, 2019), https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/ [https://perma.cc/Q9ZK-6UMT].

142. *See* Jason Tashea, Opinion, *Courts Are Using AI to Sentence Criminals. That Must Stop Now*, WIRED (Apr. 17, 2017, 7:00 AM), https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/ [https://perma.cc/EWR8-LR3K] (describing how the use of proprietary AI in courtrooms requires judges to relinquish some of their decision-making power to inscrutable automated systems). *Contra* Angela Chen, *How Artificial Intelligence Can Help Us Make Judges Less Biased*, VERGE (Jan. 17, 2019, 12:07 PM), https://www.theverge.com/2019/1/17/18186674/daniel-chen-machine-learning-rule-of-law-economics-psychology-judicial-system-policy [https://perma.cc/47KZ-R4QU].

143. A. Michael Froomkin, Ian Kerr & Joelle Pineau, *When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning*, 61 ARIZ. L. REV. 33, 70 (2019).

144. *See* Karla Lopez & Deborah Reid, *Discrimination Against Patients with Substance Use Disorders Remains Prevalent and Harmful: The Case for 42 CFR Part 2*, HEALTH AFFS.: HEALTH AFFS. BLOG (Apr. 13, 2017), https://www.healthaffairs.org/do/10.1377/hblog20170413.059618/full/ [https://perma.cc/3FQD-YAZ3].

145. *Id.*

146. *See* Ben Panko, *This Algorithm Can Tell How Much Pain You're In*, SMITHSONIAN MAG. (Sept. 7, 2017), https://www.smithsonianmag.com/smart-news/reading-pain-computer-180964795/ [https://perma.cc/M5JP-42LC].

147. *See* Bernie Monegain, *NIC Launches New Platform to Bring Machine Learning to Prescription Drug Monitoring Programs*, HEALTHCARE IT NEWS (Aug. 2, 2018, 2:01 PM), https://www.healthcareitnews.com/news/nic-launches-new-platform-bring-machine-learning-prescription-drug-monitoring-programs [https://perma.cc/698U-C7HP].

information, such as data from people's social media accounts, into their predictions.[148]

Like many fields of medicine, psychiatry has a dark history. For hundreds of years, psychiatric patients were isolated, abused, and used as guinea pigs in cruel experiments.[149] Lobotomies became a popular form of treatment, and the frontal lobes of thousands of patients were removed in vain attempts to treat their conditions.[150] Today, psychiatry is often criticized for becoming too impersonal.[151] Whereas prolonged talk therapy sessions were once the gold standard of psychiatry, clinicians now often spend fifteen minutes or less with patients to adjust their medications.[152]

The increasing popularity of digital psychiatry, which relies on smartphone apps, patient surveillance, and EMD mining to monitor and make predictions about psychiatric patients, could make the field more impersonal and increasingly reliant on products provided by for-profit companies. Psychiatrists may become detached data analysts instead of engaged humanists. Critics characterize the increasing reliance on AI-based inferences as a return to Skinnerian behaviorism.[153] In a time where diseases of despair claim the lives and happiness of millions of Americans, a holistic and humanistic approach to psychiatry is needed.[154] Overreliance on digital phenotyping and other unproven data analytics methods may be moving the field in the wrong direction.

There is also a risk that EMD mining will lead to increased stigmatization of certain patient populations. Even highly trained physicians can be biased against people with mental illnesses, substance use disorders, chronic pain conditions, and "idiopathic" diseases for which a cause has not yet been discovered. Using EMD to infer which patients have these conditions can stigmatize those individuals and reduce the quality of the care they receive. For example, imagine that a patient arrives at a doctor's office, and the medical record presents a red flag on the screen of the doctor's laptop warning that this patient is predicted to have a high suicide risk. Though based solely on statistical data, that warning will likely change the doctor's perception and treatment of the patient. If the patient undergoes surgery, the patient may receive a lower dose of pain medicine than patients who were not flagged as a suicide risk.

---

148. *See* Sarker et al., *supra* note 13.

149. *See* Jerome Groopman, *The Troubled History of Psychiatry*, NEW YORKER (May 20, 2019), https://www.newyorker.com/magazine/2019/05/27/the-troubled-history-of-psychiatry [https://perma.cc/AK23-UK2Z].

150. *Id.*

151. *See* NIALL MCLAREN, HUMANIZING PSYCHIATRISTS: TOWARD A HUMANE PSYCHIATRY 101–02 (2010).

152. *See id.* at 101.

153. *See* Yarden Katz, *Noam Chomsky on Where Artificial Intelligence Went Wrong*, ATLANTIC (Nov. 1, 2012), https://www.theatlantic.com/technology/archive/2012/11/noam-chomsky-on-where-artificial-intelligence-went-wrong/261637/ [https://perma.cc/2G7X-LTN7].

154. MCLAREN, *supra* note 151.

Increasing patient surveillance and reliance on EMD to guide treatment decisions may eliminate any remaining privacy between patients and doctors, which will erode patients' trust in doctors and the healthcare system. Some veterans who rely on the VA for healthcare already keep information from their doctors out of fear that it will be used against them.[155] Some patients may fear that doctors will learn information that they would prefer not to disclose because EMD allows doctors to see into their minds even if they say nothing. Trust is the cornerstone of effective doctor-patient relationships, and the presence of technological intermediaries threatens these relationships.[156]

Bias can also be built into EMD mining algorithms. It is well established that machine learning algorithms are often biased against racial minorities, sexual minorities, and other underrepresented groups.[157] In 2019, it was widely reported that AI-based healthcare decision-making software systematically discriminated against Black patients.[158]

Finally, the fact that EMD-based profiling and predictions are often inaccurate has not stopped them from being deployed. These systems will inevitably make mistakes that lead to unnecessary treatment of asymptomatic individuals and the withholding of necessary treatment from symptomatic individuals, both of which cause harm. These risks will be discussed further in Part II below.

Within the healthcare setting, EMD mining raises the following question: Should patients be permitted to keep any secrets from healthcare providers? Monitoring patients by video and recording their voices during clinical encounters is invasive. It collects information from patients that they may not have intended to disclose. Should sharing all information, including health inferences facilitated by EMD mining, be a requirement of seeking medical care? These and other questions must be addressed as surveillance technologies become commonplace in the healthcare sector. If they are not adequately addressed, widespread patient surveillance will become inevitable and may erode the trust that is essential to effective doctor-patient relationships and the delivery of high-quality care.

---

155. Ann M. Cheney, Christopher J. Koenig, Christopher J. Miller, Kara Zamora, Patricia Wright, Regina Stanley, John Fortney, James F. Burgess & Jeffrey M. Pyne, *Veteran-Centered Barriers to VA Mental Healthcare Services Use*, 18 BMC HEALTH SERVS. RSCH., no. 591, 2018, at 1, 10 (describing why veterans withhold information from VA physicians).

156. Carlos A. Pellegrini, *Trust: The Keystone of the Physician-Patient Relationship*, BULL. AM. COLL. SURGEONS, Jan. 2017, at 58.

157. *See* Andrew Thompson, *Google's Sentiment Analyzer Thinks Being Gay Is Bad*, VICE: MOTHERBOARD (Oct. 25, 2017, 10:00 AM), https://www.vice.com/en_us/article/j5jmj8/google-artificial-intelligence-bias [https://perma.cc/BN6F-C7NZ].

158. Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCI. 447 (2019) (reporting that black patients were far less healthy than white patients assigned the same overall health risk score).

*3. Monitoring and Promoting Public Health*

EMD mining can be used to monitor public health by continuously collecting digital traces from large segments of the population and using AI to draw conclusions about the population's welfare. Current uses include predicting when individuals may attempt suicide, experience drug overdoses, or conduct mass shootings or other violent acts. Other potential applications include monitoring the spread of infectious disease outbreaks and pandemics.[159] During the 2020 outbreak of coronavirus in Wuhan, China, journalists reported that an EMD mining algorithm called BlueDot was the first to warn of its spread.[160]

Two potential benefits of EMD over traditional health information are its potential to identify people who are sick or are about to become sick, perhaps even before they realize it themselves, and its ability to identify population-level health trends using data that was not generated for the purpose of studying public health.[161] If EMD is collected from consumers on a massive scale, for example from Facebook's 2.8 billion users, it can reveal population-level patterns that can be used to guide public health policies and decision-making. These patterns may be too subtle and complex to be identified without the aid of AI. Then EMD can trigger interventions that affect individuals and populations, such as quarantining those suspected of harboring a virus or directing resources to areas most affected by an outbreak.

In 2008, Google attempted to mine EMD by using people's internet searches to infer whether they had contracted influenza.[162] The program, called Google Flu Trends, generated excitement in the public health community.[163] "We really are excited about the future of using different technologies, including technology like this, in trying to figure out if there's better ways to do surveillance for outbreaks of influenza or any other diseases in the United States," said Joseph Bresee, currently Associate Director of Global Health Affairs for the Centers for Disease Control and Prevention (CDC) Influenza Division.[164]

---

159. *See* Eric Niiler, *An AI Epidemiologist Sent the First Warnings of the Wuhan Virus*, WIRED (Jan. 25, 2020, 7:00 AM), https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/ [https://perma.cc/XT2P-7F4J].

160. *Id.*

161. *See* Marcel Salathé, *Digital Epidemiology: What Is It, and Where Is It Going?*, 14 LIFE SCIS. SOC'Y & POL'Y, no. 1, 2018, at 1, 2 (defining digital epidemiology as epidemiology that uses data not generated for the purpose of practicing epidemiology").

162. David Lazer & Ryan Kennedy, Opinion, *What We Can Learn from the Epic Failure of Google Flu Trends*, WIRED (Oct. 1, 2015, 7:00 AM), https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/ [https://perma.cc/GBG7-JUA3].

163. Alexis C. Madrigal, *In Defense of Google Flu Trends*, ATLANTIC (Mar. 27, 2014), https://www.theatlantic.com/technology/archive/2014/03/in-defense-of-google-flu-trends/359688/ [https://perma.cc/G4B8-5H2X].

164. *Id.*

Influenza kills half a million people worldwide each year, and detecting it early can lead to better outcomes.[165] Google Flu Trends attempted to identify influenza patterns in numerous countries, but it was ultimately deemed ineffective and was shut down.[166] However, despite Google's early failure at mining EMD for public health monitoring, tech companies and government agencies have expressed renewed interest in mining EMD and framing it as a means of monitoring and promoting public health. [167]

Since the introduction of Google Flu Trends in 2008, there have been significant advances in AI, data storage, and cloud computing. Whereas Google analyzed only a single stream of digital traces—people's Google searches—today, companies have access to numerous data streams. For instance, Facebook accesses all the data that people post on its site, including status updates, private messages between users, photos, video, and likes.[168] It has data from other platforms under its umbrella, such as Instagram, WhatsApp, and Oculus.[169] Facebook also tracks users when they are not using the site; it has tracking pixels embedded in thousands of websites across the internet that record people's behavior online.[170] Facebook even tracks people who don't have Facebook accounts.[171] With access to all these sources of digital traces, Facebook and other platforms have a much richer and more varied source of data to transform into EMD than Google had in 2008.

The allure of EMD mining may be motivating Facebook and other platforms to acquire real medical data to boost the quality of their EMD-based predictions. In 2019, Facebook hired Dr. Roni Zeiger, the former head of Google Health who developed the ill-fated Google Flu Trends, to expand and oversee its health-related programs.[172] Shortly after hiring Zeiger, Facebook launched its Preventive Health

---

165. Jeremy Ginsberg, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski & Larry Brilliant, *Detecting Influenza Epidemics Using Search Engine Query Data*, 457 NATURE 1012, 1012 (2009).

166. *Id.*

167. *See* Mallory Locklear, *Canada Will Track Suicide Risk Through Social Media with AI*, ENGADGET (Jan. 2, 2018), https://www.engadget.com/2018/01/02/canada-track-suicide-risk-social-media-ai/ [https://perma.cc/Z5ZE-ZYSV]; Poulin & Peterson, *supra* note 51.

168. *Data Policy*, FACEBOOK, https://www.facebook.com/policy.php [https://perma.cc/W4TM-3X4X] (Jan. 11, 2021).

169. *Id.*

170. Allen St. John, *How Facebook Tracks You, Even When You're Not on Facebook*, CONSUMER REPS. (Apr. 11, 2018), https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/ [https://perma.cc/724S-P5HN].

171. Alex Hern, *Facebook Admits Tracking Users and Non-Users Off-Site*, GUARDIAN (Apr. 17, 2018, 6:26 AM), https://www.theguardian.com/technology/2018/apr/17/facebook-admits-tracking-users-and-non-users-off-site [https://perma.cc/VPD3-YHNQ].

172. Jonah Comstock, *Google Vet Roni Zeiger Leaves Smart Patients to Head Up Facebook's Growing Health Efforts*, MOBIHEALTH NEWS (May 28, 2019, 2:18 PM), https://www.mobihealthnews.com/content/north-america/google-vet-roni-zeiger-leaves-smart-patients-head-facebooks-growing-health [https://perma.cc/4ZAW-MF55].

tool ("Preventive Health"), which asks people to input their health information and reminds them when to seek medical screening and professional advice.[173]

According to Freddy Abnousi, Facebook's Head of Healthcare Research, Preventive Health gives Facebook users information about medical tests that are available and recommended for people with similar demographics.[174] Recommended tests may include colonoscopies, stool tests, and computerized tomography (CT) scans.[175] The Preventive Health interface prompts users to provide the date and time that each test is completed.[176] The service could potentially help some Facebook users remember to schedule routine health screenings.[177] However, Facebook's primary motivation is likely bringing additional users to its platform and retaining existing accounts.[178] Preventive Health may also be a means of coaxing users to reveal health information to the platform, which can then be used in lieu of medical records to train EMD mining algorithms.

Facebook claims it does not share information collected through Preventive Health "with third parties, such as health organizations or insurance companies, so it can't be used for purposes like insurance eligibility."[179] Further, Facebook says "we don't show ads based on the information you provide in Preventive Health."[180] However, on numerous occasions, Facebook has broken its promises to consumers.[181] Moreover, its promises not to use data acquired by Preventive Health for advertising and insurance purposes does not foreclose its use to train EMD mining algorithms.

Facebook has become infamous for this kind of verbal misdirection. In 2018, during his testimony before Congress, Mark Zuckerberg was asked whether Facebook sells user data.[182] Zuckerberg replied, "I can't be clearer on this topic: We

---

173. Mary Beth Griggs, *Facebook's New Preventive Health Tool Pushes People to Advocate for Their Health*, VERGE (Oct. 28, 2019, 4:03 PM), https://www.theverge.com/2019/10/28/20936541/facebook-preventative-health-cancer-heart-disease-flu-tool [https://web.archive.org/web/20200730100057/https://www.theverge.com/2019/10/28/20936541/facebook-preventative-health-cancer-heart-disease-flu-tool].

174. *Id.*

175. *Id.*

176. *Id.*

177. *See id.*; Fussell, *supra* note 47.

178. *See* Griggs, *supra* note 173.

179. *Id.*

180. *Id.*

181. *See* Len Sherman, *Zuckerberg's Broken Promises Show Facebook Is Not Your Friend*, FORBES (May 23, 2018, 12:22 PM), https://www.forbes.com/sites/lensherman/2018/05/23/zuckerbergs-broken-promises-show-facebook-is-not-your-friend/#4bb446be7b0a [https://perma.cc/V5SK-LMD6]; Ryan Nakashima, *Promises, Promises: Facebook's History with Privacy*, PHYS.ORG (Mar. 30, 2018), https://phys.org/news/2018-03-facebook-history-privacy.html [https://perma.cc/BEG2-7M4E].

182. *See Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Com.*, 115th Cong. (2018) (statement of Mark Zuckerberg, Cofounder/Chairman/CEO, Facebook).

don't sell data."[183] However, this response overlooks the fact that Facebook commercializes the intelligence it gains from user data.[184] Facebook may not literally sell the data it derives from user interactions with Preventive Health, but it could sell access to the knowledge it derives from that data to companies that wish to reach Facebook users with targeted ads, which may be no less harmful or invasive.[185] Statements like Zuckerberg's are misleading because they suggest that selling personal data is the only potential harm associated with widespread user surveillance. They ignore other potential harms, such as those associated with vulnerability-based marketing and consumer scoring, which are discussed in the following Section.

Surveillance of K–12 and university students to predict mental health and disciplinary issues is another public health application of EMD.[186] Companies in the United States and United Kingdom use machine learning to infer students' mental health status and predict their behavior in hopes of preventing bullying, violence, drug use, and school shootings.[187] Gaggle, a leading provider of school email and shared document monitoring, claims its technology continuously monitors 4.5 million students across 1,400 U.S. school districts.[188]

Gaggle tracks and analyzes everything from emails and instant messages to essays and homework assignments using a combination of AI and human content moderation.[189] It interfaces with popular software platforms, such as Google Workspace and Microsoft 365, and monitors all activity, including notifications received from major social networks.[190] Gaggle says that in the last academic year, its technology "helped districts save the lives of more than 700 students who were planning or actually attempting suicide."[191] One of Gaggle's competitors, named Bark, claims it has partnered with over a thousand U.S. school districts and claims

183. *Id.* at 18. *But see* Jon Porter, *Facebook Might Not Sell User Data, but Internal Documents Suggest It Was Certainly Considered*, VERGE (Nov. 29, 2018, 5:01 AM), https://www.theverge.com/2018/11/29/18117582/facebook-six4three-internal-documents-emails-selling-user-data [https://web.archive.org/web/20200730100057/https://www.theverge.com/2019/10/28/20936541/facebook-preventative-health-cancer-heart-disease-flu-tool].

184. *See* Kurt Wagner, *This Is How Facebook Uses Your Data for Ad Targeting*, VOX (Apr. 11, 2018, 6:00 AM), https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg [https://perma.cc/3J4L-78XR].

185. *Id.*

186. *See* Todd Feathers, *Schools Spy on Kids to Prevent Shootings, but There's No Evidence It Works*, VICE: MOTHERBOARD (Dec. 4, 2019, 6:00 AM), https://www.vice.com/en_us/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works [https://perma.cc/95KX-EQN6].

187. *Id.*

188. Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, GUARDIAN (Oct. 22, 2019, 1:00 AM), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle [https://perma.cc/QE2C-5F2G].

189. Haskins, *supra* note 54.

190. *Id.*

191. Beckett, *supra* note 188.

its technology has helped prevent "16 credible school shootings" and detected "twenty thousand severe self-harm situations."[192]

In one reported incident in Florence, South Carolina, school officials were alerted when a student allegedly "started writing about suicide while working on an in-class English assignment."[193] During the exercise, Gaggle detected and analyzed the words she typed into a Google search query.[194] According to school officials, the student was removed from class within minutes for a conversation with administrators.[195] In a separate event in Cincinnati, Ohio, school administrators called the police on a student whom Gaggle reportedly flagged for writing about self-harm while using a word processing application.[196] The student was hospitalized and received treatment.[197]

As suicide rates rise in teens and young adults, the opioid crisis claims more lives, and school shootings are an ever-present concern, school officials feel immense pressure to do something to keep students safe.[198] Some schools have faced lawsuits for failing to protect students who were bullied or died by suicide.[199] However, many students and parents are unaware of the scale and invasiveness of student surveillance and that health information is being inferred from non-health-related behavior.[200]

Clearly, it is socially desirable to reduce suicide rates, prevent drug overdoses, and stop school shootings. But is it desirable to do so at all costs? Is it even possible to reduce these threats to public health by continuously monitoring students and mining their EMD? Could EMD mining potentially backfire and contribute to suicide and other public health problems? The answers to these questions are unknown. However, the lack of answers has not stopped numerous public and private entities from implementing EMD-based mental health predictions on a national and global scale.

Facebook, Crisis Text Line, Gaggle, Bark, and many other platforms use EMD-based predictions that potentially trigger home visits from police and other first responders. However, profiling people for suicidal intent and sending police to their homes could paradoxically increase the risk of violence and suicide.[201] There are numerous examples of police "wellness checks" resulting in incarceration or

192. *Id.*
193. *Id.*
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *See id.*
201. Marks, *supra* note 34.

fatal confrontations with police, and the victims are often members of vulnerable minority groups.[202]

According to Crisis Text Line, five percent of its users identify as Native American or Native Alaskan, which is over three times their representation in the U.S. population.[203] Hispanics, members of the LGBTQ community, and people who identify as homeless or undocumented immigrants are also overrepresented.[204] It is unknown how being labeled violent or suicidal by algorithms may affect their health, safety, identity, and autonomy.

Police are often ill equipped to handle mental health issues such as suicide attempts and drug overdoses. It is not entirely their fault; police officers receive far more training on how to discharge their firearms than they do learning methods to de-escalate emotionally charged situations.[205] Yet the lack of training can have tragic consequences.

In one highly publicized incident, a mother called the police for help with her thirty-eight-year-old son, Jason Harrison, who had been diagnosed with bipolar disorder and schizophrenia.[206] When officers arrived on the scene, Harrison came to the door holding a small screwdriver.[207] As he approached the officers, they quickly drew their firearms and fatally shot him.[208] There are many other examples. In 2014, eighteen-year-old Keith Vidal was shot and killed by police when his mother asked 911 dispatchers for help transporting him to a hospital for mental health treatment.[209] In 2016, another schizophrenic, thirty-one-year-old Terrence Coleman, was shot and killed by Boston police after his mother called them.[210] In

202. Doug Criss & Leah Asmelash, *When a Police Wellness Check Becomes a Death Sentence*, CNN (Oct. 19, 2019, 7:33 AM), https://www.cnn.com/2019/10/19/us/wellness-check-police-shootings-trnd/index.html [https://perma.cc/YD2K-VTQB].

203. Wharton School, *Social Impact Perspective: Bob Filbin | 2018 Wharton People Analytics Conference*, YOUTUBE (May 9, 2018), https://www.youtube.com/watch?v=e3WWCDFQqmA [https://perma.cc/YUE2-79QJ].

204. *Id.*

205. Curtis Gilbert, *Not Trained to Not Kill*, APM REPS. (May 5, 2017), https://www.apmreports.org/story/2017/05/05/police-de-escalation-training [https://perma.cc/UCZ7-QJ7X].

206. Tom Dart, *Video Released of Dallas Police Shooting Mentally Ill Black Man Dead at Home*, GUARDIAN (Mar. 18, 2015, 4:22 PM), https://www.theguardian.com/us-news/2015/mar/18/video-dallas-police-shooting-mentally-ill-black-man [https://perma.cc/EC7L-LARQ].

207. *Id.*

208. *Id.*

209. Alisa Roth, *A Worried Mom Wanted the Police to Take Her Mentally Ill Son to the Hospital. They Shot Him.*, VOX (May 30, 2018, 9:40 AM), https://www.vox.com/the-big-idea/2018/5/30/17406900/police-shootings-mental-illness-book-vidal-vassey-mental-health [https://perma.cc/MD7V-X3Q5].

210. Benjamin Swasey & Simón Rios, *Mother Whose Son Was Fatally Shot by Boston Cop Files a Civil Rights Lawsuit*, WBUR (Apr. 4, 2018), https://www.wbur.org/news/2018/04/04/coleman-shooting-lawsuit [https://perma.cc/TPR5-5YDY].

2019, twenty-nine-year-old Osaze Osagie was shot by police when his father called them to perform a wellness check on his son.[211]

Harrison, Coleman, and Osagie were Black. There is evidence suggesting that racial minorities are more often shot by police responding to mental health calls.[212] People with disabilities and members of the LGBTQ community may also be at risk. In 2012, a blind man was shot with a Taser by police who mistook his white stick for a samurai sword.[213] In 2017, a deaf man was shot and killed by police despite neighbors' warnings that he could not hear their commands.[214] In 2018, police responded to the home of Chelsea Manning with guns drawn after she posted a concerning tweet that led fans to believe she might attempt suicide.[215]

In 2021, it is increasingly entities other than parents, friends, and physicians who call on police to perform wellness checks. It is often technology companies, including Facebook, Gaggle, and Bark, who contact law enforcement due to proprietary EMD-based predictions. These platforms contact law enforcement because their algorithms detect a high risk of violence or self-harm. However, their algorithms are not tested for safety or accuracy, they are trained using poor-quality proxy data, and their design and function are obscured from public view.[216] Yet tech companies send armed, inadequately trained police to people's homes in response to their algorithmic predictions. Under such conditions, racial minorities, sexual minorities, and people with disabilities may be singled out by biased algorithms with harmful and fatal consequences.

Predicting bullying, self-harm, suicide, and violence in school-age children in educational settings comes with similar risks. Flagging students and treating them differently based on EMD-derived predictions may harm those individuals. Inaccurate predictions could have unexpected and enduring downstream effects on students' lives. Based on those predictions, individuals may be removed from the general student population, hospitalized against their will, and stigmatized by school

---

211. Gary Sinderson, *State College Police to Receive Outside Report Following 2019 Use of Deadly Force*, WJAC (Aug. 10, 2020), https://wjactv.com/news/local/state-college-police-to-receive-outside-report-following-2019-use-of-deadly-force [https://perma.cc/5HBD-Y6V9].

212. Shaun King, *If You Are Black and in a Mental Health Crisis, 911 Can Be a Death Sentence*, INTERCEPT (Sept. 29, 2019, 5:00 AM), https://theintercept.com/2019/09/29/police-shootings-mental-health/ [https://perma.cc/9QRH-ZMB7].

213. Helen Carter, *Police Taser Blind Man Mistaking His White Stick for a Samurai Sword*, GUARDIAN (Oct. 17, 2012, 8:21 PM), https://www.theguardian.com/uk/2012/oct/17/police-taser-blind-man-stick [https://perma.cc/Y4NE-XMWQ].

214. Matthew Haag, *Deaf Man Is Fatally Shot by Oklahoma City Police, Despite Pleas*, N.Y. TIMES (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/us/oklahoma-city-police-shooting-deaf.html [https://perma.cc/RP4P-8LHG].

215. Micah Lee & Alice Speri, *Police Broke into Chelsea Manning's Home with Guns Drawn—in a "Wellness Check,"* INTERCEPT (June 5, 2018, 7:13 AM), https://theintercept.com/2018/06/05/chelsea-manning-video-twitter-police-mental-health/ [https://perma.cc/4K4C-RL8A].

216. *See* Sara Gorman & Jack M. Gorman, *Are Facebook's Suicide Prevention Tactics Misguided?*, PSYCH. TODAY (Apr. 7, 2019), https://www.psychologytoday.com/us/blog/denying-the-grave/201904/are-facebook-s-suicide-prevention-tactics-misguided [https://perma.cc/S78Z-7J6N]; Singer, *supra* note 31.

officials and their peers. Once labeled and treated differently by algorithms, children may start behaving differently and be treated differently by their peers in a sort of self-fulfilling prophecy.[217]

Continuous twenty-four-hour student surveillance can be viewed as a form of social control that encourages students to conform to codes of appropriate behavior.[218] Such control may stifle creativity and inhibit personal expression. If students learn that the words and phrases they type will be mined for EMD and result in scrutiny from school officials, home visits from police, and forced hospitalizations, then they may not explore certain topics in their assignments or electronic communications with peers and teachers. Instead of speaking honestly about their feelings, they may conceal them. Such censorship could paradoxically increase the feelings of isolation associated with depression, problematic substance use, suicidal thoughts, and violent behavior.[219]

Using EMD to predict and prevent suicide, drug use, and gun violence aims to achieve socially desirable ends: the protection of vulnerable individuals and society. However, companies may claim to be using EMD for those purposes while surreptitiously using it for other purposes that exploit the full value of EMD. Because companies derive economic value from health inferences, they are incentivized to use them to exploit consumers in addition to protecting them. The following Section describes the use of EMD for advertising and vulnerability-based marketing.

#### *4. Targeted Advertising and Vulnerability-Based Marketing*

Most online shoppers have had the uncanny experience of purchasing items and subsequently seeing ads for those items follow them around the internet.[220] If people buy a sleeping bag online, they may be categorized as outdoor enthusiasts, and ads for camping gear may appear in their Facebook and Twitter feeds. This type

---

217. *See* Monica J. Harris, Richard Milich, Elizabeth M. Corbitt, Daniel W. Hoover & Marianne Brady, *Self-Fulfilling Effects of Stigmatizing Information on Children's Social Interactions*, 63 J. PERSONALITY & SOC. PSYCH. 41 (1992); Lee Jussim, Jacquelynne Eccles & Stephanie Madon, *Social Perception, Social Stereotypes, and Teacher Expectations: Accuracy and the Quest for the Powerful Self-Fulfilling Prophecy*, 28 ADVANCES EXPERIMENTAL SOC. PSYCH. 281 (1996).

218. Andrew Hope, *Seductions of Risk, Social Control, and Resistance to School Surveillance*, *in* SCHOOLS UNDER SURVEILLANCE: CULTURES OF CONTROL IN PUBLIC EDUCATION 230, 230–42 (Torin Monahan & Rodolfo D. Torres eds., 2010).

219. *See* Timothy Matthews, Andrea Danese, Jasmin Wertz, Candice L. Odgers, Antony Ambler, Terrie E. Moffitt & Louise Arseneault, *Social Isolation, Loneliness and Depression in Young Adulthood: A Behavioural Genetic Analysis*, 51 SOC. PSYCHIATRY & PSYCHIATRIC EPIDEMIOLOGY 339 (2016); Kee-Lee Chou, Kun Liang & Jitender Sareen, *The Association Between Social Isolation and DSM-IV Mood, Anxiety, and Substance Use Disorders: Wave 2 of the National Epidemiologic Survey on Alcohol and Related Conditions*, 72 J. CLINICAL PSYCHIATRY 1468 (2011); Dinur Blum & Christian Gonzalez Jaworski, *From Suicide and Strain to Mass Murder*, 53 SOC'Y 408 (2016).

220. *See* Christopher Elliott, *Why Does That Online Ad Keep Following Me?*, USA TODAY (Nov. 6, 2016, 6:01 PM), https://www.usatoday.com/story/travel/advice/2016/11/06/retargeting-online-ads/93282408/ [https://perma.cc/N8AS-JY9C].

of behavioral profiling is only the tip of the iceberg, and market segments are not limited to people's hobbies or shopping habits.

Companies analyze digital traces collected from retail purchases, activity on social media, and other consumer behavior to sort people into categories or "market segments," which are used for targeted advertising.[221] Oftentimes, the inferences they draw about consumers are health related. When Target analyzed its customers' purchases to infer which ones were pregnant, its goal was to send them pregnancy- and newborn-related promotions.[222] The company was mining medical information from consumers not because it cared about their health, but because it wanted to sell products.

Some companies take consumer surveillance and profiling a step further. EMD can be used to tailor ads for people based on their health conditions, even if they never disclosed their health status to platforms or advertisers. People with diabetes can be targeted with ads for medical devices and other products that may be useful to them. People with substance use disorders could be made aware of treatment programs and products that might help them reduce or eliminate dependence on a drug. These applications for targeted advertising may appear useful to consumers. Facebook would say they allow companies to show users more relevant ads.[223] However, there is a darker, more manipulative side to microtargeted ads.

Diseases of despair, such as depression, substance use disorders, and suicide, are rising in the United States and contributing to decreased life expectancy.[224] Facebook has previously capitalized on this trend. According to a leaked report, Facebook once told advertisers it had the ability to identify teens who feel

---

221. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 25, 47 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/2Z5B-74PM] (describing verified market segments including "expectant parent," "diabetes interest," "cholesterol focus," "AIDS," "HIV"); *see also What Information Do Data Brokers Have on Consumers, and How Do They Use It?*: *Hearing Before the S. Comm. on Com., Sci., & Transp.*, 113th Cong. (2013) (statement of Pam Dixon, Executive Director, World Privacy Forum), www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf [https://perma.cc/754A-AW5R] (testifying that data brokers sort consumers into categories including "rape sufferers," "HIV/AIDS," and "cancer").

222. *See* Duhigg, *supra* note 1.

223. Louise Matsakis, *Facebook's Targeted Ads Are More Complex than It Lets On*, WIRED (Apr. 25, 2018, 4:04 PM), https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/ [https://perma.cc/5Q4J-67KP].

224. *See* Joshua Cohen, *'Diseases of Despair' Contribute to Declining U.S. Life Expectancy*, FORBES (July 19, 2018, 1:12 PM), https://www.forbes.com/sites/joshuacohen/2018/07/19/diseases-of-despair-contribute-to-declining-u-s-life-expectancy/#4d1aacbe656b [https://perma.cc/SX2F-33MQ]; A.H. Weinberger, M. Gbedemah, A.M. Martinez, D. Nash, S. Galea & R.D. Goodwin, *Trends in Depression Prevalence in the USA from 2005 to 2015: Widening Disparities in Vulnerable Groups*, 48 PSYCH. MED. 1308 (2017).

"anxious," "useless," "hopeless," and like a "failure."[225] Facebook claimed it could track teens' emotions throughout the week and anticipate when they are most in need of a confidence boost.[226]

Platforms that surveil users and mine EMD are not limited to monitoring people's emotions—they can also influence them. In 2012, Facebook intentionally manipulated the emotions of nearly 700,000 users during its famed "emotional contagion study."[227] The ability to manipulate people's emotions was long the dream of advertisers, and platforms that mine EMD can provide that capability to them.[228] The danger is that tech companies and advertisers can create strong emotions in people, and then leverage those emotions to induce people to behave in ways that benefit advertisers while harming the manipulated individuals and society. People with certain health conditions may be particularly susceptible to such manipulation, and EMD mining can allow advertisers to exploit their health-related vulnerabilities.

People with gambling disorders can be targeted with ads for gambling websites and casino vacations. Children inferred to have attention deficit disorder or gaming addiction can be targeted with ads for "loot boxes," a type of gambling designed for children who play video games.[229] Similarly, people with eating disorders can be targeted with ads for stimulants, laxatives, and illicit weight loss products, and people with cancer or chronic pain can be targeted with ads for unproven or illicit pain medications. This type of "vulnerability-based marketing" exploits people's health-related susceptibilities, traps them in unhealthy patterns of behavior, and can exacerbate their health conditions.

According to one report about onlineadvertising:

> affiliates once had to guess what kind of person might fall for their unsophisticated cons, targeting ads by age, geography, or interests. Now Facebook does that work for them. The social network tracks who clicks on the ad and who buys the pills and then starts targeting others whom its algorithm thinks are likely to buy. Affiliates describe watching their ad

225. Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling 'Insecure' and 'Worthless*,' GUARDIAN (May 1, 2017, 3:01 PM), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens [https://perma.cc/Y6WF-D7RZ].

226. *Id.*

227. Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (Sept. 8, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ [https://perma.cc/53RU-CS6E].

228. *See* Rae Ann Fera, *The Rise of Sadvertising Why Brands Are Determined to Make You Cry*, FAST CO. (May 4, 2014), https://www.fastcompany.com/3029767/the-rise-of-sadvertising-why-brands-are-determined-to-make-you-cry [https://perma.cc/9KRM-FK29].

229. Aaron Drummond & James D. Sauer, *Video Game Loot Boxes Are Psychologically Akin to Gambling*, 2 NATURE HUM. BEHAV. 530 (2018).

> campaigns lose money for a few days as Facebook gathers data through trial and error, then seeing the sales take off exponentially.[230]

One advertiser said of Facebook's marketing algorithms: "They go out and find the morons for me."[231]

Facebook claims the predictions made by its suicide screening software are not used for advertising purposes.[232] However, it is conceivable that a platform could mine EMD to predict suicide while simultaneously using it to categorize consumers for marketing and social credit scoring. The information could also be used to deny rights to targeted individuals. For instance, in 2018, the Department of Housing and Urban Development (HUD) filed a complaint against Facebook for discriminating against users based on race, religious affiliation, and disability.[233] According to HUD, individuals in certain categories were prevented by Facebook's algorithms from receiving housing-related ads.[234] This type of vulnerability-based advertising excludes people from accessing employment, housing, and other resources, and EMD mining can serve as the means of sorting them into categories for the purposes of exclusion.[235]

Just as disabled Facebook users were denied access to housing ads, individuals whom AI predicts to be potentially violent or suicidal could lose rights and privileges such as the ability to drive a car, rent an apartment, or purchase a firearm. To this day, many states ask individuals who are applying for licenses to practice law or medicine whether they have substance use or mental health issues. If government agencies are permitted to mine EMD to monitor public health, should the information be used for other purposes such as determining who is fit to practice law or medicine in the state?

## II. CONCEPTUALIZING EMD MINING

This Part explains how EMD mining can be framed in six different ways and examines the social risks of using EMD to profile people. Examining EMD mining

---

230. Zeke Faux, *How Facebook Helps Shady Advertisers Pollute the Internet*, BLOOMBERG BUSINESSWEEK (Mar. 28, 2018, 9:15 AM), https://www.bloomberg.com/news/features/2018-03-27/ad-scammers-need-suckers-and-facebook-helps-find-them [https://perma.cc/AN69-STDF].

231. *Id.*

232. Norberto Nuno Gomes de Andrade, Dave Pawson, Dan Muriello, Lizzy Donahue & Jennifer Guadagno, *Ethics and Artificial Intelligence: Suicide Prevention on Facebook*, 31 PHIL. & TECH. 669, 680 (2018).

233. Tracy Jan & Elizabeth Dwoskin, *HUD Is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe*, WASH. POST (Mar. 28, 2019, 3:59 PM), https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/ [https://perma.cc/B24L-ZBMW].

234. *Id.*

235. *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Ryan Calo, *OfficeMax Letter to 'Daughter Killed in Car Crash' Could Be Privacy's Whale Song*, FORBES (Jan. 19, 2014, 4:09 PM), https://www.forbes.com/sites/ryancalo/2014/01/19/officemax-letter-to-daughter-in-car-crash-could-be-privacys-whale-song/?sh=11d93a1b3fb8 [https://perma.cc/JLD5-LHVG].

through different lenses highlights those risks and aids efforts to guide effective regulation, which is the subject of Part III. EMD mining can be framed in the following six ways: as a form of regulatory arbitrage that circumvents privacy and human rights laws, as a breach of contextual integrity, as the corporate or unlicensed practice of medicine, as the marketing and operation of unregulated medical devices, as unregulated health research, and as a breach of fiduciary duties.

### *A. As Regulatory Arbitrage that Circumvents Privacy Laws*

Traditional medical data is obtained by healthcare providers, insurance companies, and their business associates through direct interaction with patients during clinical care or while seeking reimbursement for medical services.[236] This flow of information, from patient to provider, is the traditional flow of health data, which has existed nearly unchanged for millennia.[237]

Throughout recorded history, social norms and laws have evolved to protect the privacy of TMD. When healthcare providers collect TMD from patients, they are bound by various laws and traditions to maintain its confidentiality.[238] These laws and traditions have ancient roots.[239] One line from the Hippocratic Oath suggests that physicians in Ancient Greece acknowledged the implicit value of health data: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."[240] To uphold this Oath, ancient physicians maintained the confidentiality of TMD and vowed not to share it with others outside the bounds of the treatment relationship.

During their medical training, modern-day physicians take an updated version of the Hippocratic Oath, which contains a promise to protect the confidentiality of patient information: "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[241] The Declaration of Geneva, a modern successor to the ancient Hippocratic Oath adopted by the World Medical

---

236. Mason Marks, *How Companies Use AI to Infer Sensitive Health Data from Consumer Behavior – Harvard Law School*, YOUTUBE (July 11, 2018), https://www.youtube.com/watch?v=1zlTmvNaHbM [https://perma.cc/73U8-HQHH].

237. *Id.*

238. *See Physician Oaths*, AAPS, https://www.aapsonline.org/ethics/oaths.htm [https://perma.cc/BPH9-CHWX] (last visited Nov. 28, 2020); AM. MED. ASS'N, AMA CODE OF MEDICAL ETHICS: PRINCIPLES OF MEDICAL ETHICS (2001), https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/principles-of-medical-ethics.pdf [https://perma.cc/FS9K-RHMD]; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); CAL. CIV. CODE § 56.10 (West 2017); MD. CODE ANN., HEALTH–GEN. § 4-301 (West 2017).

239. *See* Howard Markel, *"I Swear by Apollo"—On Taking the Hippocratic Oath*, 350 NEW ENG. J. MED. 2026, 2026 (2004).

240. *Id.* at 2028.

241. Don Colburn, *Under Oath*, WASH. POST (Oct. 22, 1991), https://www.washingtonpost.com/archive/lifestyle/wellness/1991/10/22/under-oath/53407b39-4a27-4bca-91fe-44602fc05bbf/ [https://perma.cc/U7DY-FQMV].

Association, contains a similar promise: "I will respect the secrets which are confided in me, even after the patient has died."[242]

In addition to the oaths sworn by modern physicians, society imposes fiduciary duties on healthcare providers. These strict obligations include a duty to maintain the confidentiality of medical information and to be loyal to patients, which forbids the physician from using patients' information to manipulate or exploit them.[243] Similarly, in the United States, the HIPAA Privacy Rule requires entities in the healthcare system to protect patient data as it flows from patients to providers and from those providers to other covered entities such as hospitals and health insurance companies (and their business associates).[244]

Prior to the advent of EMD mining, entities outside the healthcare system could not access consumer health information unless consumers voluntarily provided it or the entities obtained it from healthcare providers in compliance with HIPAA. Patients trusted that their health information would not be shared with third parties unless sharing it was directly related to their medical care. However, EMD mining enables entities outside of healthcare, such as corporations and government agencies, to infer health data from nonmedical information, providing them access to data that previously would have been difficult or impossible to obtain. Moreover, they can access health data without having to comply with HIPAA and other regulations of the U.S. healthcare system. Accordingly, EMD mining can be viewed as a form of healthcare regulatory arbitrage. Due to a lack of effective regulation, any entity that collects, aggregates, and analyzes data can acquire sensitive health information and use it for nearly any purpose.

The preamble to the regulation implementing HIPAA's privacy requirements suggests that one of HIPAA's primary purposes is to protect the rights of consumers by controlling the inappropriate flow and use of patients' health information.[245] It includes quotes by jurists, writers, and philosophers on the importance of maintaining privacy.[246] In 1890, Louis D. Brandeis and Samuel D. Warren famously defined the right to privacy as "the right to be let alone."[247] According to Janna Malamud Smith, "[i]f we continually, gratuitously, reveal other people's privacies, we harm them and ourselves, we undermine the richness of the

242. Ramin Walter Parsa-Parsi, *The Revised Declaration of Geneva: A Modern-Day Physician's Pledge*, 318 JAMA 1971 (2017).

243. Dayna Bowen Matthew, *Implementing American Health Care Reform: The Fiduciary Imperative*, 59 BUFF. L. REV. 715, 726–29 (2011).

244. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160.103 (2014); *see also* U.S. DEP'T HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 3 (2013), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/J4AR-99SM] ("The Privacy Rule protects all '*individually identifiable health information*' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.").

245. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

246. *Id.*

247. *Id.*

personal life, and we fuel a social atmosphere of mutual exploitation."[248] The concerns expressed in these quotes motivated the implementation of HIPAA in the 1990s, and they are no less compelling today. They illustrate that HIPAA's roots can be traced to the ancient Hippocratic Oath, and like the Oath, HIPAA was drafted before EMD mining would have been conceivable.

When HIPAA was drafted, the only foreseeable ways for someone to obtain and exploit people's health information were to steal medical records or acquire them through legal means and use them inappropriately. As a result, HIPAA focuses on security to prevent unauthorized actors from gaining access and on privacy to ensure that actors who should have access maintain the confidentiality of patient data.[249] However, HIPAA's drafters could not have foreseen the advent of EMD mining.

The ability to conjure health data from digital traces undermines the assumptions underlying HIPAA's adoption by expanding the means through which health data can be obtained and exploited. Now, any entity that collects large volumes of data can potentially obtain health data, and it need not steal data in the traditional sense or violate existing health laws to obtain it. Instead, EMD miners can manufacture health data from the digital traces that are plentiful in the Digital Age. Lawmakers must now decide whether to throw out thousands of years of health privacy norms due to the arrival of EMD mining or to implement new regulations to control aberrant streams of health data flow.

In the United States, in addition to circumventing HIPAA, EMD mining can help police sidestep fundamental rights such as the warrant requirement of the Fourth Amendment.[250] If police rely on AI-based suicide predictions to enter people's homes and institutionalize them, they may deprive people of liberty without due process.[251] The Fourth Amendment protects people and their homes from warrantless searches.[252] However, according to exigent circumstances doctrine, police may enter homes without warrants if they reasonably believe entry is necessary to prevent physical harm.[253] Preventing violence and suicide clearly falls within this exception.[254] Nevertheless, it may be unethical to rely on EMD and EMD-based profiling to circumvent Fourth Amendment protections when little information regarding their accuracy and safety is publicly available.[255] Using opaque algorithms to circumvent fundamental rights is becoming more common due to emerging public-private surveillance networks such as Facebook's suicide

248. *Id.*

249. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

250. Marks, *supra* note 6, at 120.

251. *Id.*

252. *Id.*

253. *Id.*

254. *Id.*

255. *Id.*

prediction program and Amazon's ongoing collaboration with police forces through its Ring doorbell platform.[256]

Unlike U.S. health privacy law, which takes a sectoral approach to data privacy and is exemplified by HIPAA, the European Union (EU) treats all health data the same regardless of its origin. In 2016, it adopted the General Data Protection Regulation (GDPR) to replace the 1995 Data Protection Directive (the Directive), which was adopted when the internet was in its infancy.[257] The Directive contained "principles of fair information processing" that can be traced to the 1981 Treaty of Strasbourg.[258] The drafters of the GDPR borrowed heavily from the Directive.

Having been adopted in 2016 and implemented in 2018, the GDPR is relatively new.[259] Though inferences are not specifically referenced in its text, some sections are relevant to EMD mining. Nevertheless, a significant amount of statutory interpretation is necessary to understand whether various forms of EMD mining are lawful under the GDPR. Presumably, due to uncertainty surrounding how the GDPR applies to health inferences, some companies have opted not to implement certain forms of EMD mining in the European Union. For instance, in 2018, Facebook announced it would expand its AI-based suicide prediction program internationally except in the EU, presumably due in part to the GDPR.[260] Nevertheless, Facebook's suicide predictions could potentially be lawful under the GDPR, and they serve as a useful case to analyze how the law applies to EMD mining.

For data processing to be lawful under the GDPR, it must meet at least one of the conditions set forth in article 6. Section 6(1)(a) requires that data subjects consent to the processing of personal data for one or more specific uses.[261] Therefore, if a data subject provides consent for EMD to be mined for a specific purpose, then data processors could lawfully mine EMD for the specified purpose only. However, the requirement for consent can be waived if one of several other conditions of article 6 is met, which raises the possibility that EMD could be mined lawfully without a data subject's consent.

---

256. Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 3:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/F8HX-WAW2].

257. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) (repealing and replacing "Directive 95/46/EC," the official name of the Data Protection Directive).

258. *See* BART HERMAN MARIA CUSTERS, THE POWER OF KNOWLEDGE: ETHICAL, LEGAL AND TECHNOLOGICAL ASPECTS OF DATA MINING AND GROUP PROFILING IN EPIDEMIOLOGY 28 (2004).

259. *The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/US5E-5LFJ] (last visited Nov. 29, 2020).

260. *See* Guy Rosen, *Getting Our Community Help in Real Time*, FACEBOOK (Nov. 27, 2017), https://about.fb.com/news/2017/11/getting-our-community-help-in-real-time/ [https://perma.cc/6DZQ-KFJV].

261. Council Regulation 2016/679, *supra* note 257, art. 6.

Section 6(1)(d) allows processing of personal data if it is "necessary in order to protect the vital interests of the data subject or of another natural person."[262] Section 6(1)(e) allows for the processing of personal data if "processing is necessary for the performance of a task carried out in the public interest."[263] Because suicide prediction can potentially protect the vital interests of people and serve the public interest, it is one example of data processing that could potentially satisfy either section 6(1)(d) or section 6(1)(e) and be performed without the consent of data subjects.

With respect to section 6(1)(d), mining EMD for use in suicide prediction could be deemed necessary to protect the vital interests of a data subject. In the United States, and in other regions outside the EU where Facebook makes suicide predictions, EMD-based suicide prediction often results in police-mediated wellness checks that could protect the lives of data subjects if their suicide attempts are prevented or interrupted.[264] However, as described above, sending police to Facebook users' homes deprives people of autonomy and exposes them to potentially violent confrontations with police.[265] Moreover, their risk of suicide may paradoxically increase if they are institutionalized against their will and released from institutions without proper support. In other words, wellness checks triggered by EMD-based suicide predictions can potentially endanger Facebook users and threaten their vital interests. Viewed in this light, EMD mining for suicide prediction without user consent might not meet the requirements of section 6(1)(d).

Facebook would have to provide empirical evidence demonstrating that its suicide predictions and subsequent interventions protect people's vital interests. However, the company currently maintains the details of its predictions as trade secrets, which should cast doubt on claims that its predictions protect one's vital interests.[266]

With respect to section 6(1)(e), which allows data processing without consent, if it is necessary for the performance of a task carried out in the public interest, EMD-based suicide prediction could be viewed as necessary for suicide prevention, which is clearly of benefit to the public if carried out safely and effectively. Every year, suicide attempts take immense social and economic tolls on society. They can devastate families and communities while raising healthcare costs. However, there

---

262. *Id.*

263. *Id.*

264. Catherine Card, *How Facebook AI Helps Suicide Prevention*, FACEBOOK (Sept. 10, 2018), https://about.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/ [https://perma.cc/YJS8-KQUY]; David Sentendrey, *Police Rescue Man Threatening Suicide on Facebook Live*, FOX 46 CHARLOTTE (June 5, 2018, 2:46 AM), https://www.fox46.com/news/police-rescue-man-threatening-suicide-on-facebook-live/ [https://perma.cc/73HQ-C923]; *Assam Police Saved a Girl After Facebook Alerted It About Her Suicidal Post*, NEWS 18 INDIA (July 26, 2018, 1:44 PM), https://www.news18.com/news/india/facebook-saves-a-life-after-detecting-suicidal-post-of-a-minor-girl-and-alerting-assam-police-1824419.html [https://perma.cc/DG6C-GVNG].

265. *See supra* notes 201–215 and accompanying text.

266. *See* Singer, *supra* note 31; Marks, *supra* note 6, at 98.

is insufficient evidence to establish that AI and EMD can effectively protect people from self-harm. If vulnerable populations, such as racial minorities, members of the LGBT community, and people with mental illnesses and other disabilities, are disproportionately targeted and negatively impacted by suicide prediction algorithms and the real-world interventions they trigger, such as wellness checks, then EMD-based suicide prediction may not serve the public interest. Such interventions may do more harm than good, creating negative externalities that further marginalize vulnerable populations and contribute to healthcare costs.

Such interventions may lead to social isolation that prevents people from openly discussing issues such as depression and suicide on social media. Specifically, if people know that they may receive a visit from police and be hospitalized against their will, they may be less likely to speak freely about important issues such as depression, drug use, and suicide. The withdrawal of populations vulnerable to suicide from the public sphere is detrimental to society and does not serve the public interest as required by section 6(1)(e).

These examples illustrate the importance of taking a holistic approach to interpreting article 6 of the GDPR. If one takes a narrow view of EMD-based suicide prediction, one might conclude that it easily satisfies the requirements of sections 6(1)(d) and 6(1)(e). However, a closer look reveals that the situation is more complex. AI-based suicide prediction is not as straightforward and effective as social media platforms might have us believe.[267] Their view of these tools is a sanitized version that is presented as much for public relations purposes as public health promotion. This example underscores the importance of employing experts from a variety of fields to interpret privacy legislation such as the GDPR. Individuals who are not experienced in identifying the risks of algorithmic systems may gloss over the potential harms.

Article 9 of the GDPR prohibits the processing of special categories of personal data, including health information, unless at least one of ten exceptions is met.[268] Therefore, even if a data processing use, such as EMD mining for suicide prediction, meets the requirements of sections 6(1)(d) or 6(1)(e), it will still be prohibited if it involves health information unless it meets one of these exceptions.

Continuing with the suicide prediction example, because data on suicide risk is related to health, the processing of personal information for suicide prediction must satisfy at least one of article 9's ten exceptions. Two exceptions are relevant to suicide prediction: section 9(2)(g) allows processing if it is "necessary for reasons of substantial public interest";[269] and section 9(2)(i) allows processing that is "necessary for reasons of public interest in the area of public health."[270] The requirements of these exceptions parallel those of sections 6(1)(d) and 6(1)(e), and

267. *See* Gomes de Andrade et al., *supra* note 232, at 679–80.
268. Council Regulation 2016/679, *supra* note 257, art. 9.
269. *Id.*
270. *Id.*

similar concerns apply. Clearly, implementing effective suicide prevention is useful for reasons of substantial public interest and in the area of public health. What is less clear is whether mining EMD is necessary for those purposes. If the methods used are opaque, inaccurate, and potentially harmful, then they are not necessary, and they frustrate the purpose of section 9(2)(i).

Article 22 of the GDPR allows EU citizens to opt out of fully automated processing that has a legal effect on that citizen.[271] A Facebook-initiated wellness check by first responders can affect the legal status of the data subject by forcing them to be hospitalized and treated. Therefore, if Facebook implemented its suicide prediction algorithms in the EU, then EU citizens could ostensibly be entitled to opt out of suicide prediction by invoking their rights under article 22. However, in its current incarnation, Facebook's suicide prevention platform still involves human judgment at certain stages.[272] The algorithmic system assigns a suicide risk score to each piece of content, and the content with the highest scores is forwarded to a team of human content moderators who decide whether to initiate a wellness check.[273] The presence of human decision-makers may put Facebook's system outside the scope of article 22.

Unlike HIPAA, the GDPR protects health data regardless of its source.[274] However, loopholes in the law represented by article 22 and the exceptions to articles 6 and 9 make it possible for EMD miners to collect health data without people's consent and to use it in ways that affect their rights.

In the United States, entities that mine EMD may circumvent anti-discrimination laws such as the Americans with Disabilities Act (ADA). [275] In the EU, such entities may circumvent child protection laws such as the United Nations Convention on the Rights of the Child (CRC) and fundamental human rights laws such as the EU Charter of Fundamental Human Rights, which includes rights to privacy, protection of personal data, equality, and antidiscrimination.[276] This Article focuses primarily on privacy and data protection laws. However, the circumvention of human rights, child protection, and antidiscrimination laws may be discussed in future articles.

### *B. As a Breach of Contextual Integrity*

EMD mining can be framed as a breach of social norms regarding information flow. Under Helen Nissenbaum's theory of contextual integrity, all spheres of

---

271. *Id.* art. 22.

272. Card, *supra* note 264.

273. *Id.*

274. *See* Council Regulation 2016/679, *supra* note 257, art. 4 (defining "data concerning health" as all "personal data related to the physical or mental health of a natural person . . . which reveal information about his or her health status").

275. *See* Marks, *supra* note 34.

276. *See* Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3; Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

human activity are governed by information flow norms.[277] In other words, nearly all our actions occur within social contexts that are influenced by factors such as location, politics, history, and custom.[278] Throughout the day, as we move from one location to the next, we pass through different environments that have unique social contexts such as classrooms, doctors' offices, retail stores, courthouses, and restaurants.[279]

Each environment has unique rules for how information should ideally flow. For example, a busy comedy club has different information flow norms than a public library or a courtroom. In a comedy club, it is acceptable to convey happiness by laughing, clapping, or even whistling. However, heckling a comedian by yelling out verbal expressions of praise or condemnation is generally discouraged. By comparison, in a library, all forms of audible information flow are discouraged, and in a courtroom, people are expected to speak only when spoken to by a judge or clerk of the court. When people violate the information flow norms of these environments, they may be reprimanded (by comedians, librarians, and judges respectively).

Nissenbaum describes two types of information norms: those that determine appropriateness and those that govern the flow of information.[280] If either type of norm is violated, then contextual integrity is breached, and one's privacy may be violated.[281] In the comedy club, it is socially acceptable to express emotion verbally or non-verbally (an information flow norm). However, it is inappropriate to express negative emotion, which is characteristic of heckling (an appropriateness norm). If an audience member violates either of these norms, then he has breached contextual integrity.

When companies mine EMD from consumer behavior, they violate contextual norms for the flow of health data. However, because they do it surreptitiously, usually without consumers' knowledge or consent (and often without the knowledge of regulators and legislators), there is nobody to reprimand them.

Most people do not expect corporations to use AI to analyze their digital traces and infer their risk of suicide, substance use disorders, and other health conditions. When those inferences are made, consumers are not sitting in doctors' offices where it is customary for health information to be collected. Instead, they are behaving in non-medical contexts such as posting on Facebook, shopping at Walmart, or sending messages through WhatsApp or Gmail. Each of these activities has its own well-established social context, such as drafting personal correspondence or shopping online or in retail stores. In most circumstances, medical information has nothing to do with those contexts. However, mining for health inferences allows

277. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 137 (2004).
278. *Id.*
279. *See id.*
280. *Id.* at 138.
281. *Id.*

companies to surreptitiously breach consumer expectations regarding where their data flows by transforming mundane behavioral data observed in non-medical contexts into sensitive health data.

Consider the Uber example. Imagine that you are hailing an Uber driver to take you to an upcoming doctor's appointment. Uber drivers may have a reputation for violating some appropriateness norms.[282] However, their behavior typically falls short of collecting sensitive medical information. If you selected a hospital or medical clinic as your destination, and the Uber driver asked about your health, then an appropriateness norm would be violated, contextual integrity would be breached, and your privacy would also be invaded. This type of question is not generally accepted in the context of transportation. Similarly, if the Uber app records that you were dropped off outside a medical clinic, and it cross references your location with the doctor's offices in the clinic, and your recent credit card purchases, to mine EMD and infer your medical condition, that process would violate an information flow norm. Consequently, contextual integrity would be breached, and so would your privacy.

Unless one is traveling by ambulance, one's medical data has nothing to do with the social context of transportation. According to Nissenbaum, "[w]e should not expect social norms, including informational norms, simply to melt away with the change of medium to digital electronic any more than from sound waves to light particles."[283] In the context of this example, changing the means through which you hire a driver, from waiving or whistling to hail a cab on the streets of New York to pressing a button on the Uber app, should not permit a disruption in established norms of information flow. However, this is the kind of disruption that EMD allows.

In the past, people communicated primarily by sending letters or making phone calls. However, it would be a breach of social norms if phone carriers listened in on personal calls or the Postal Service opened every piece of mail. However, in the Digital Age, e-mail providers, social media platforms, and smartphone app developers routinely use AI to "read" the contents of private messages sent between users.

In a 2018 interview, Facebook CEO Mark Zuckerberg commented on shifting social norms regarding privacy. He said, "[t]he world is changing quickly" and

---

282. *See* Christina Cauterucci, *Uber Now Bans Flirting in Its Vehicles. Will That Stop Creepy Drivers?*, SLATE (Dec. 9, 2016, 4:19 PM), https://slate.com/human-interest/2016/12/uber-now-bans-flirting-in-its-vehicles-will-that-stop-creepy-drivers.html [https://perma.cc/J3KL-X3CB]; Nojan Hicks, *Uber, Lyft Driver Suspended After Secretly Livestreaming Hundreds of Passengers*, N.Y. POST ( July 22, 2018, 2:32 PM), https://nypost.com/2018/07/22/uber-lyft-driver-suspended-after-secretly-livestreaming-hundreds-of-passengers/ [https://perma.cc/F5ST-GDKX].

283. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DÆDALUS, Fall 2011, at 32, 43.

"social norms are changing quickly."[284] Eight years earlier, in 2010, Zuckerberg said, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. . . . That social norm is just something that has evolved over time."[285] In many ways, Zuckerberg is correct. With the arrival of social media, people likely share more information than they used to. However, lawmakers and regulators must not confuse technological change and the resulting shifts in information flow for shifts in social norms. Though people may share more information with internet platforms than ever before, EMD-mining forces consumers to share more information with corporations than they know. Most people are unaware that EMD can be extracted from non-medical data, and the fact that EMD can be mined should not be taken as evidence that it should be mined, that society has accepted this practice, or that consumers have consented to it.

Nissenbaum argues that to protect people's privacy online, one must identify contexts, explain the meaning of well-established information norms, identify disruptive information flows, and evaluate them against the backdrop of existing norms "based on general ethical and political principles as well as context specific purposes and values."[286]

Social norms governing the flow of medical information are very old and well-established. As described in Part I, the importance of safeguarding medical privacy has been recognized for millennia. It was articulated over 2,000 years ago in the Hippocratic Oath, which established a duty of physicians to maintain patient privacy.[287] One can imagine that even in ancient Greece, there were individuals who hoped to profit from knowing details about a patient's physical or mental states.[288]

Some data scientists argue that their profession should adopt its own version of the Hippocratic Oath.[289] Microsoft floated the idea in a 2018 book on AI and its role in society.[290] However, such an Oath is an example of self-regulation that is merely aspirational and has no legal effect.

Doctors take the Hippocratic Oath during their training and aspire to meet its standards for the duration of their careers. Though it is not legally binding, if they

---

284. Nicholas Thompson, *Mark Zuckerberg Talks to Wired About Facebook's Privacy Problem*, WIRED (Mar. 21, 2018, 9:00 PM), https://www.wired.com/story/mark-zuckerberg-talks-to-wired-about-facebooks-privacy-problem/ [https://perma.cc/8KC2-NW6X].

285. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/269M-67EH].

286. Nissenbaum, *supra* note 283, at 38.

287. PAUL CARRICK, *The Hippocratic Oath*, *in* MEDICAL ETHICS IN ANTIQUITY 69 (1995).

288. *Id.*

289. Tom Simonite, *Should Data Scientists Adhere to a Hippocratic Oath?*, WIRED (Feb. 8, 2018, 7:00 AM), https://www.wired.com/story/should-data-scientists-adhere-to-a-hippocratic-oath/ [https://perma.cc/KLM3-DJBN].

290. MICROSOFT, THE FUTURE COMPUTED: ARTIFICIAL INTELLIGENCE AND ITS ROLE IN SOCIETY (2018), https://news.microsoft.com/uploads/2018/01/The-Future-Computed.pdf [https://perma.cc/MR64-P2UT].

breach elements of the Oath, they may face sanctions from state medical licensing boards.[291] Failure to maintain the confidentiality of patient information would also violate HIPAA and the fiduciary duties imposed on them by common law.[292] In other words, physicians are incentivized to comply with the Hippocratic Oath under penalty from state law and professional organizations. No comparable safeguards currently exist in the technology sector. Nevertheless, if such an oath was adopted by the tech industry, it could reinforce privacy norms that are under assault by rapid technological advancement and the normalization of data mining and health inferences.

However, despite casual promises by tech CEOs to respect and protect consumer privacy, the trend appears to be moving in the direction of fewer privacy safeguards and greater exploitation of consumer data. It is becoming normal for people to expect to have their privacy violated and their personal information taken by tech companies without their permission.

### *C. As the Unlicensed Practice of Medicine*

Companies that mine EMD claim they are not acting as healthcare providers when they make health inferences. For instance, Facebook frames its suicide prediction algorithms as a public safety tool instead of a health screening platform, and Crisis Text Line says it is a data analytics company, not a mental health organization.[293] Similarly, developers of smartphone apps for managing anxiety and insomnia define their products as "wellness apps" instead of health apps.[294] However, the operation of these platforms can meet the definition of the unlicensed or corporate practice of medicine, which typically includes the diagnosis, prevention, or treatment of disease by individuals or corporations that lack state medical licenses.[295]

---

291. *See* FED'N OF STATE MED. BDS., GUIDELINES FOR THE STRUCTURE AND FUNCTION OF A STATE MEDICAL AND OSTEOPATHIC BOARD (2018), https://www.fsmb.org/siteassets/advocacy/policies/guidelines-for-the-structure-and-function-of-a-state-medical-and-osteopathic-board.pdf [https://perma.cc/ATJ9-VYSF].

292. Steve Adler, *What Is Considered Protected Health Information Under HIPAA?*, HIPAA J. (Apr. 2, 2018), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ [https://perma.cc/BQ6R-97R4]; MacDonald v. Clinger, 446 N.Y.S.2d 801, 805 (App. Div. 1982) (explaining that doctors have a fiduciary responsibility to patients that are implicit and essential to the doctor-patient relationship); Martin v. Baehler, Civ. A. No. 91C-11-008, 1993 WL 258843, at *3 (Del. Super. Ct. May 20, 1993) ("[T]his Court joins the majority and holds that an actionable wrong lies for a physician's breach of his or her duty to maintain confidences.").

293. *See* Alice Gregory, *R U There?*, NEW YORKER (Feb. 2, 2015), https://www.newyorker.com/magazine/2015/02/09/r-u [https://perma.cc/7Q3Q-S85W] (reporting that the CEO of Crisis Text Line built the company "more along the lines of a tech company than a nonprofit" and thinks of it as "a lot more like Airbnb or Uber or Lyft").

294. *See* Megan Thielking, *How Do You Make a Mental Health App People Actually Want to Use? Take a Page from Podcasts and Pixar*, STAT (July 15, 2019), https://www.statnews.com/2019/07/15/mental-health-app-podcast-pixar/ [https://perma.cc/WV3H-CS49].

When doctors diagnose patients, they gather information about lifestyle, family, symptoms, and medications. They combine this information with test results and feed it into decision-making algorithms they learned during their training. In medical school and residency, doctors memorize hundreds of diagnostic algorithms. For instance, an algorithm for diagnosing pneumonia might include the following questions: "Does the patient have a cough? If yes, branch right in the decision tree. If not, branch left." Medical diagnosis essentially boils down to navigating a large set of branching decision trees. When companies mine EMD and use it to draw health-related conclusions, the process is comparable to medical diagnosis. Companies collect data from consumers and feed it into machine learning algorithms that have been trained to identify medical conditions. The result is a health-related categorization, or more accurately, a diagnosis. A diagnosis is really nothing more than an estimation of a person's health based on probabilities.

Virtually all U.S. states have laws that prohibit corporations and unlicensed individuals from practicing medicine. In California, the unlicensed practice of medicine consists of unlicensed diagnosis or treatment, and violations are punishable by fines of up to $10,000 and imprisonment for up to one year.[296] The state Business and Professions Code defines "diagnosis" as "any undertaking by any method, device, or procedure whatsoever, and whether gratuitous or not, to ascertain or establish whether a person is suffering from any physical or mental disorder."[297] This description sounds a lot like the act of collecting digital traces, mining EMD, and sorting consumers into health-related categories.

When companies sort people into health-related categories, they are acting like medical diagnosticians. Framing EMD-based profiling as the practice of medicine is controversial. One objection is that EMD-based profiling is based on probabilities, whereas medical diagnosis does not appear to be.[298] However, the premise of this objection is incorrect. Even medical diagnoses are based on probabilities, and oftentimes physicians create a list of diagnoses and rank them in order of descending likelihood.[299] Seasoned doctors recognize that "diagnosis and prognosis always have varying degrees of uncertainty and at best can be stated as *probable* in a particular case."[300] Both EMD-based profiling and medical diagnosis use data derived from population-level research to make predictions about an individual's health. Therefore, the fact that EMD-based profiling is based on

295. *See* CAL. BUS. & PROF. CODE § 2052 (West 2011); MO. ANN. STAT. § 332.010 (West 2017).

296. BUS. & PROF. § 2052.

297. *Id.* § 2038.

298. Marks, *Emergent Medical Data*, *supra* note 4 (defining emergent medical data).

299. *See* HUW LLEWELYN, HOCK AUN ANG, KEIR LEWIS & ANEES AL-ABDULLAH, OXFORD HANDBOOK OF CLINICAL DIAGNOSIS 44, 65 (3d ed. 2014); *see also* A. Cahan, D. Gilon, O. Manor & O. Paltiel , *Probabilistic Reasoning and Clinical Decision-Making: Do Doctors Overestimate Diagnostic Probabilities?*, 96 Q.J. MED. 763 (2003).

300. A. Banerjee, S.L. Jadhav & J.S. Bhawalkar, *Probability, Clinical Decision Making and Hypothesis Testing*, 18 INDUS. PSYCHIATRY J. 64 (2009).

probabilities is not adequate grounds for dismissing the comparison to medical diagnosis.

A second objection rests on the fact that patients visit doctors to receive diagnoses, whereas consumers usually do not browse the Internet, utilize social media, or use ride-sharing apps to receive diagnoses. According to this objection, because consumers do not ask to be placed in health-related categories by data controllers, and because the controller does not return a diagnosis to the consumer, EMD-based profiling should not be viewed as a form of medical diagnosis. However, a patient's intent does not determine whether a doctor's opinion is regarded as diagnostic of the patient's condition, and the same should be true for EMD-based profiling and predictions. If an unconscious driver is rushed to the emergency room following a car crash, nobody would claim that a doctor's attempt to determine the nature and extent of the driver's injuries does not constitute medical diagnosis because the patient did not request medical treatment. If the driver then dies in the emergency room, the doctor's appraisal of his injuries would remain a diagnosis regardless of whether the doctor communicated this information to the patient. Similarly, whether a data controller returns its EMD-based predictions to consumers should not determine whether EMD-based profiling constitutes medical diagnosis.

This objection seems more like an argument for respecting contextual integrity than an objection to framing EMD-based profiling as medical diagnosis. It demonstrates how deeply ingrained social norms are into our thinking about medicine, and it reflects the belief that only doctors can make diagnoses and they must be made in medical settings. The objection boils down to the following argument: EMD-based profiling cannot constitute medical diagnosis because it does not fit within our traditional understanding of who can practice medicine and where medicine is practiced. However, in the Digital Age, where traditional data flows have been disrupted and machines are taking on the roles of human decision-makers, technology is challenging our long-held beliefs about what constitutes health information. However, just as medical data remains medical information whether it is obtained in a doctor's office or through EMD-mining, medical diagnosis is medical diagnosis whether it is performed by a licensed physician, a corporation, or a machine learning algorithm.

Most states have laws that prohibit corporations from practicing medicine, which are grounded in the policy that only licensed physicians should make decisions that impact patients' health.[301] Though EMD-based profiling may not be perfectly equivalent to medical diagnosis, EMD-based profiling violates established norms regarding who should be making medical diagnoses, handling sensitive health

301. AM. MED. ASS'N, ISSUE BRIEF: CORPORATE PRACTICE OF MEDICINE (2015), https://www.ama-assn.org/sites/default/files/media-browser/premium/arc/corporate-practice-of-medicine-issue-brief_1.pdf [https://web.archive.org/web/20170629015707/https://www.ama-assn.org/sites/default/files/media-browser/premium/arc/corporate-practice-of-medicine-issue-brief_1.pdf].

information, and practicing medicine. Moreover, EMD mining produces the same type of harms that state unlicensed practice of medicine laws are intended to prevent. Those laws arose in response to harms posed by unqualified individuals posing as healthcare providers who preyed on vulnerable members of the public.[302]

A third objection to framing EMD mining as medical diagnosis is essentially a slippery slope argument. It goes as follows: "If we call Facebook's suicide predictions medical diagnosis, then we will have to call any casual, off-the-cuff diagnosis made by a person's friends and family medical diagnosis." In other words, "If we are going to expand the definition of medical practice to include algorithmic health screening tools, then isn't every opinion offered by a layperson the diagnosis of disease?" No, because unlike a friend or family members' casual appraisal of one's health condition, which is an isolated event, Facebook and other platforms' health screening occurs in a more systematic manner and on a massive scale. Consider the following example. If a door-to-door salesman standing on your front porch offers his opinion that you look ill and offers you a sip of his homemade herbal remedy, most people would not consider him to be practicing medicine. He is merely a concerned citizen making a considerate offer. However, if he goes door-to-door and systematically appraises the health of thousands of people and offers them different remedies depending on his appraisal, then his behavior starts to look more like the practice of medicine. There is something about the systematic nature of his investigations of people's health and the scale on which he makes them. Facebook's suicide predictions are made systematically and on a massive scale; the platform makes suicide predictions about billions of its users located in nearly every country in which it operates.

### *D. As the Operation of Unregulated Medical Devices*

"Many smartphone-based health and wellness apps are designed as modern-day Trojan horses. Developers market them to consumers as solutions to common health problems, such as insomnia and anxiety.[303] However, under the hood, the apps use AI to mine EMD without consumers' knowledge or consent. The FDA acknowledges that these apps can meet the Food Drug and Cosmetic Act's definition for medical devices, which includes software "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."[304] However, the FDA elects not to regulate them because it relies on an outdated risk assessment framework to decide where to focus its

---

302. MARK A. HALL, DAVID ORENTLICHER, MARY ANNE BOBINSKI, NICHOLAS BAGLEY & I. GLENN COHEN, HEALTH CARE LAW AND ETHICS 1260 (9th ed. 2018).

303. *See* Thielking, *supra* note 294.

304. The FDA acknowledges that wellness apps can be medical devices. In general, it refers to "software as a medical device" as SaMD. *See Digital Health Software Precertification (Pre-Cert) Program*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-program [https://perma.cc/5P5G-854J] (Sept. 14, 2020).

regulatory attention. This framework was designed to assess physical injuries caused by traditional medical devices (such as mechanical ventilators and MRI machines).[305] It fails to account for the more nuanced harms associated with EMD mining and EMD-based profiling, such as systematic bias resulting in discrimination, physical and emotional injury resulting from police wellness checks, and the damaging behavioral patterns and public health impact of vulnerability-based marketing. As a result, even though smartphone apps infer sensitive health information and often trigger real-world interventions, the FDA does not regulate them.

To make matters worse, the FDA appears to be moving in the direction of even less regulatory oversight for some software-based medical devices. Through its Digital Health Software Precertification (Pre-Cert) Program, the agency is creating a regulatory pathway akin to the Transportation Security Administration's PreCheck Program.[306] Through the FDA's Pre-Cert Program, if companies demonstrate to the FDA that they are trustworthy, they are permitted to fast-track digital health products into the marketplace with limited oversight, almost as if they were travelers breezing through airport security without having to remove their shoes.[307]

In 2019, three U.S. lawmakers expressed concern that the Pre-Cert program will not ensure public safety.[308] In a letter to the FDA's Acting Commissioner Norman Sharpless, Senators Elizabeth Warren, Patty Murray, and Tina Smith criticized the FDA's reliance on poorly defined "excellence appraisals" to determine whether medical device manufacturers are trustworthy and questioned the agency's choice to withhold the results of such appraisals.[309]

Instead of moving in the direction of less oversight for AI-based medical devices, including wellness apps, the FDA should increase its regulatory scrutiny of such devices and modernize its methods of assessing risk to account for privacy harms and other downstream effects of EMD-based predictions that threaten people's safety and autonomy.

---

305. *See* U.S. FOOD & DRUG ADMIN., SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION (2017), https://www.fda.gov/media/100714/download [https://perma.cc/8R84-BAXG].

306. *Digital Health Software Precertification (Pre-Cert) Program*, *supra* note 304.

307. *Id.*

308. Greg Slabodkin, *Senators Voice Concerns with FDA Software Precertification Program*, HEALTH DATA MGMT. (Oct. 31, 2019, 11:31 PM), https://www.healthdatamanagement.com/news/senators-voice-concerns-with-fda-software-precertification-program [https://perma.cc/H2AH-7MEN].

309. Letter from Elizabeth Warren, Patty Murray, and Tina Smith, U.S. Sens., to Norman E. Sharpless, Acting Comm'r, U.S. Food & Drug Admin., and Jeffrey Shuren, Dir., Ctr. for Devices & Radiological Health, U.S. Food & Drug Admin. (Oct. 30, 2019), https://www.warren.senate.gov/imo/media/doc/2019.10.30%20Letter%20with%20Senators%20Murray%20and%20Smith%20to%20FDA%20requesting%20additional%20information%20on%20the%20agency's%20software%20pre-certification%20pilot%20program..pdf [https://perma.cc/433F-9FMN].

### *E. As Unregulated Health Research*

Internet platforms often experiment on their users to improve their products and services. The term "A/B testing" describes the process of exposing one group of users to one set of circumstances and a different group of similar users to a second set of circumstances and observing the differences in their responses. Facebook conducted this type of testing during its infamous "emotional contagion" experiment.[310] In 2014, Facebook published the results of this research in which it manipulated the news feeds of 689,003 users and measured "the effects on their emotions."[311]

Targeted advertising can be viewed as a form of A/B testing. After sorting consumers into health-related market segments, advertising algorithms can experiment on members of each group by showing them different ads and measuring their responses to determine which ads elicit the desired response (such as click-throughs or purchases). This practice is a form of experimentation on human subjects.

Wearable manufacturers, including Apple, are now leveraging smartphones and wearables to conduct research on consumers. If owners of the Apple watch choose to opt in to the company's health research, then biometric information and activity data from their devices will be uploaded to Apple's servers and used for research.[312]

James Grimmelmann points out that when tech companies such as Facebook and Apple conduct empirical research on users and publish the results, "they're acting like academics."[313] However, tech companies and academic researchers have different values and procedures.[314] It is a common refrain that Silicon Valley startups aspire to "move fast and break things."[315] In contrast, academia takes a more measured approach, particularly with respect to research on human subjects.

---

310. Gregory S. McNeal, Opinion, *Facebook Manipulated User News Feeds to Create Emotional Responses*, FORBES (June 28, 2014, 1:10 PM), https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/#221bac6439dc [https://perma.cc/HD45-U9X3].

311. *Id.*

312. *Apple Research App: The Future of Health Research Is You*, APPLE, https://www.apple.com/ios/research-app/ [https://perma.cc/AYK4-DPC6] (last visited Nov. 29, 2020); *We're Committed to Protecting Your Data*, APPLE, https://www.apple.com/privacy/features/ [https://perma.cc/L9JA-2NQL] (last visited Nov. 29, 2020).

313. James Grimmelmann, *Do You Consent? If Tech Companies Are Going to Experiment on Us, They Need Better Ethical Oversight.*, SLATE (May 27, 2015, 8:14 AM), www.slate.com/articles/technology/future_tense/2015/05/facebook_emotion_contagion_study_tech_companies_need_irb_review.html [https://perma.cc/CAT9-RUPH].

314. *Id.*

315. Erin Griffith, *Everyone Hates Silicon Valley, Except Its Imitators*, WIRED (Feb. 13, 2018, 7:00 AM), https://www.wired.com/story/everyone-hates-silicon-valley-except-its-imitators/ [https://perma.cc/2RMK-C2ZN].

Major universities and academic medical centers have IRBs that review and monitor research to ensure that the rights and welfare of human subjects are protected.[316]

History is full of examples in which powerful organizations experimented on vulnerable groups without their consent.[317] During World War II, the Nazi's committed countless atrocities by experimenting on prisoners, including disabled people and members of the LGBT community, in German concentration camps.[318] During the Tuskegee syphilis incident, 399 African American men were denied treatment for syphilis so that scientists could observe their symptoms as they developed.[319] In the Willowbrook Experiments, children with cognitive impairments were intentionally injected with various strains of the hepatitis virus so that scientists could follow the course of the resulting illness.[320] These and similar human rights abuses inspired the formation of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in 1974.[321] The Commission published its Belmont Report in 1979, which emphasizes the central importance of informed consent to research involving human subjects. The Report heavily influenced the U.S. Federal Policy for the Protection of Human Subjects, which is also known as the "Common Rule."[322] This policy has been codified by fifteen federal agencies and departments.[323]

Under its version of the Common Rule, 45 C.F.R. § 46, the Department of Health and Human Services (HHS) requires all federally funded research to be reviewed by an IRB.[324] HHS requires IRBs to consist of "at least five members, with varying backgrounds . . . including consideration of race, gender, and cultural backgrounds and sensitivity to such issues as community attitudes."[325] When research involves vulnerable human subjects such as children or people with

316. *Institutional Review Boards Frequently Asked Questions*, U.S. FOOD & DRUG ADMIN. (Jan. 1998), https://www.fda.gov/RegulatoryInformation/Guidances/ucm126420.htm [https://perma.cc/62YM-CSP2]; *see also* Richard S. Saver, *Medical Research Oversight from the Corporate Governance Perspective: Comparing Institutional Review Boards and Corporate Boards*, 46 WM. & MARY L. REV. 619, 623 (2004).

317. Robert L. Berger, *Nazi Science—The Dachau Hypothermia Experiments*, 322 NEW ENG. J. MED. 1435 (1990); Vanessa Northington Gamble, *Under the Shadow of Tuskegee: African Americans and Health Care*, 87 AM. J. PUB. HEALTH 1773 (1997).

318. Berger, *supra* note 317.

319. Gamble, *supra* note 317.

320. Walter M. Robinson & Brandon T. Unruh, *The Hepatitus Experiments at Willowbrook State School*, *in* THE OXFORD TEXTBOOK OF CLINICAL RESEARCH ETHICS, 80, 80–81 (Ezekiel J. Emanuel, Christine C. Grady, Robert A. Crouch, Reidar K. Lie, Franklin G. Miller, David D. Wendler eds., 2011).

321. U.S. DEPT. OF HEALTH, EDUC. & WELFARE, THE BELMONT REPORT (1979), https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf [https://perma.cc/W4GC-S6U9].

322. *Federal Policy for the Protection of Human Subjects ('Common Rule')*, HHS.GOV, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html [https://perma.cc/5MHT-P9L6] (Mar. 18, 2016).

323. *Id.*

324. 45 C.F.R. §§ 46.101–.505 (2021).

325. *Id.* § 46.107.

disabilities, "consideration shall be given to the inclusion of one or more individuals who are knowledgeable about and experienced in working with these subjects."[326]

Companies engaged in EMD-based profiling are essentially conducting research involving human subjects. However, they are not required to obtain IRB approval for EMD-based profiling because they do not receive federal funding. However, some scholars argue that the relationship between biomedical scientists and research subjects should be considered a fiduciary relationship.[327] If so, researchers have duties of care, confidentiality, and loyalty toward research subjects. These duties would obligate researchers to obtain informed consent and have their protocols reviewed by an independent IRB regardless of whether their research is federally funded. Similarly, if companies conducting EMD-based profiling are framed as information fiduciaries conducting research on human subjects, then they may be obligated by their duties toward human research subjects to consult an IRB before commencing research on humans.

In 2016 two Facebook employees published a law review article describing the company's internal research review process.[328] Some commentators have criticized the article and the review process it describes.[329] According to one critic, Facebook's description of its review process is vague and raises more ethical questions than it answers.[330] A second commentator argues that members of the research review group cannot make impartial decisions because they are Facebook employees.[331] She claims that the members of true IRBs are insulated from corporate influence.[332] Furthermore, because Facebook managers retain discretion over whether to escalate a proposal to the research review group, the review process may be entirely optional unlike traditional IRB approval, which is mandatory for federally funded research.[333]

The 2016 article by Facebook employees cites Nissenbaum's work on contextual integrity. According to the authors, in keeping with Nissenbaum's perspective on information flow, "we [Facebook employees] try to make sure that our methodology is consistent with people's expectations of how their information is collected and stored."[334] However, the Cambridge Analytica scandal, and

---

326. *Id.*

327. Paul B. Miller & Charles Weijer, *Fiduciary Obligation in Clinical Research*, 34 J.L. MED. & ETHICS 424 (2006). *Contra* E. Haavi Morreim, *The Clinical Investigator as Fiduciary: Discarding a Misguided Idea*, 33 J.L. MED. & ETHICS 586 (2005).

328. Jackman & Kanerva, *supra* note 110, at 442.

329. Anna Lauren Hoffman, *Facebook Has a New Process for Discussing Ethics. But Is It Ethical?*, GUARDIAN (June 17, 2016, 7:00 AM), https://www.theguardian.com/technology/2016/jun/17/facebook-ethics-but-is-it-ethical [https://perma.cc/EX8J-77VC]; *see also* Zoltan Boka, Opinion, *Facebook's Research Ethics Board Needs to Stay Far Away from Facebook*, WIRED (June 23, 2016, 4:49 PM), https://www.wired.com/2016/06/facebooks-research-ethics-board-needs-stay-far-away-facebook/ [https://perma.cc/3KK3-S3HV].

330. Hoffman, *supra* note 329.

331. Boka, *supra* note 329.

332. *Id.*

333. *Id.*

334. Jackman & Kanerva, *supra* note 110, at 455.

subsequent debacles, such as the Department of Housing and Urban Development's 2018 complaint against Facebook for discriminatory advertising, have eroded public trust in the company and cast doubt on the assertion that Facebook respects user expectations.[335] Eroding trust in Facebook, and growing skepticism towards Big Tech generally, underscore the importance of implementing independent IRBs to approve research protocols and creating mechanisms to oversee ongoing research after it is initiated.[336] Though the authors of the article are correct that private companies are not obliged to comply with the Common Rule and seek IRB approval, private companies may have moral and legal obligations to obtain informed consent from research subjects.

In *Abdullahi v. Pfizer*, a 2009 case before the U.S. Court of Appeals for the Second Circuit, the appellants alleged that in 1996, U.S. drug company Pfizer conducted a test of its antibiotic, Trovan, in Northern Nigeria during an epidemic of bacterial meningitis.[337] According to the appellants, Pfizer administered Trovan to Nigerian children without obtaining consent from them or their guardians, and the tests caused the deaths of eleven children.[338] The Court held that non-consensual medical experimentation by private actors is actionable under international law in part because the "prohibition on nonconsensual medical experimentation on human beings" is a norm of customary international law "accepted by nations around the world without significant exception."[339] The opinion cited Nazi war crimes, the Nuremberg trials, the World Medical Associations Declaration of Helsinki, and the 1955 International Covenants of Human Rights.[340] The latter states that "no one shall be subjected without his free consent to medical or scientific experimentation involving risk, where such is not required by his state of physical or mental health."[341]

To establish trust with consumers and ensure compliance with ethical norms and the norms of international law, companies that collect and process EMD could submit their research protocols for review by independent IRBs. Facebook recently created an external board to review its content moderation decisions. Originally dubbed "Facebook's Supreme Court," the body, now called Facebook's Oversight Board, will initially be funded for six years by a $130 million trust established by the

335. Stephanie Ebbs, *HUD Files Formal Complaint Against Facebook for Housing Discrimination*, ABC NEWS (Aug. 17, 2018, 4:07 PM), https://abcnews.go.com/Politics/hud-files-formal-complaint-facebook-housing-discrimination/story?id=57248710 [https://perma.cc/UZ69-W8UF].

336. Jacob Metcalf & Casey Fiesler, *One Way Facebook Can Stop the Next Cambridge Analytica*, SLATE (Mar. 18, 2018, 3:30 PM), https://slate.com/technology/2018/03/cambridge-analytica-demonstrates-that-facebook-needs-to-give-researchers-more-access.html [https://perma.cc/YJ9A-DLE6]; *see also* Editorial, *Cambridge Analytica Controversy Must Spur Researchers to Update Data Ethics*, 555 NATURE 559 (2018).

337. Abdullahi v. Pfizer, Inc., 562 F.3d 163, 168 (2d Cir. 2009).

338. *Id.* at 169.

339. *Id.* at 177.

340. *Id.* at 177, 180–81.

341. *Id.* at 180.

company.[342] Facebook says the forty-person board will function independently.[343] However, the company funds the board and appointed its initial members, and ethical concerns remain regarding its independence.[344] Nevertheless, a similar external body could potentially oversee Facebook's health and research projects.

### *F. As a Breach of Trust and Fiduciary Duties*

Some legal scholars argue that society should impose fiduciary duties on companies that collect large volumes of data from consumers.[345] Fiduciary duties reduce exploitation in relationships characterized by trust and asymmetries of knowledge and power.[346] Classic fiduciaries include doctors, lawyers, and certain financial advisors. The asymmetries of knowledge and power between these professionals and their clients create opportunities for exploitation. To minimize the risk of harm, society imposes duties of care, loyalty, and confidentiality on the professionals.

Like doctors and lawyers, companies that process digital traces have specialized knowledge, and they encourage consumers to trust them and to disclose as much information as possible. Moreover, corporations have more market and political power than the average consumer. Due to these asymmetries, Jack Balkin calls them "digital information fiduciaries."[347]

One way to ensure that corporations use EMD fairly is to impose fiduciary duties on them.[348] Companies like Facebook, Google, and Instagram hold themselves out as companies that consumers can trust.[349] In many cases, they rely on consumer-generated content to make a profit. As a result, they encourage consumers to reveal as much information as possible. Yet consumers know very little about these companies or how they operate. Furthermore, unlike individual consumers, these companies wield tremendous market and political power.[350]

---

342. *See* Mark Latonero, *Can Facebook's Oversight Board Win People's Trust?*, HARV. BUS. REV. (Jan. 29, 2020), https://hbr.org/2020/01/can-facebooks-oversight-board-win-peoples-trust?ab=hero-main-text [https://perma.cc/HKL3-A82Z].

343. Casey Newton, *Facebook Is Putting Surprising Restrictions on Its Independent Oversight Board*, VERGE (Jan. 30, 2020, 6:00 AM), https://www.theverge.com/interface/2020/1/30/21113273/facebook-oversight-board-jurisdiction-bylaws-restrictions [https://perma.cc/9MEC-ZGFJ].

344. *See* Steven Overly & Alexandra S. Levine, *Facebook Announces First 20 Picks for Global Oversight Board*, POLITICO (May 6, 2020, 3:37 PM), https://www.politico.com/news/2020/05/06/facebook-global-oversight-board-picks-240150 [https://perma.cc/3H9W-2GWY].

345. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1225 (2016).

346. *See* Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 168.

347. Balkin, *supra* note 345, at 1225.

348. Strandburg, *supra* note 346, at 168.

349. Michael Kan, *Zuckerberg: I Don't Care if You Like Me, I Just Want to Be Understood*, PCMAG (Jan. 30, 2020), https://www.pcmag.com/news/zuckerberg-i-dont-care-if-you-like-me-i-just-want-to-be-understood [https://perma.cc/F7NK-GEEA].

350. Balkin, *supra* note 345, at 1232.

Balkin points out that the law should treat information fiduciaries differently depending on "the nature of their business and the reasonable expectations of the public."[351] Thus, one can imagine a spectrum of information fiduciaries with varying obligations toward consumers depending on how the companies use data and set consumers' expectations. Because medical data is particularly sensitive, entities that mine EMD might be considered a special class of information fiduciaries with heightened duties toward their customers. Entities that collect EMD are in the business of buying and selling medical information, the privacy of which is important to consumers.[352] Furthermore, when people are ill or disabled, the asymmetries of knowledge and power that define their relationships with information fiduciaries may be increased. As a result, the duties owed by information fiduciaries to those populations may be magnified compared to those owed to people who are not members of these groups.

## III. REGULATING EMERGENT MEDICAL DATA

This Part presents preliminary thoughts on regulating EMD mining. Potential approaches include adapting existing laws to the purpose of regulating EMD mining; amending and implementing proposed health privacy laws such as the Protecting Personal Health Data Act and the Smartwatch Data Act, which currently do not go far enough to mitigate the risks of EMD mining; and designing a new generation of health data privacy laws that acknowledge the benefits and risks of EMD mining and contain effective measures to protect people from harm.

New forms of regulation could govern several different steps in the EMD mining process. For instance, regulation could regulate or ban the collection of digital traces; restrict which entities can produce, possess, or operate EMD mining algorithms; limit the situations in which EMD mining algorithms can be deployed; constrain the uses for EMD after it is harvested; and require transparency and safety testing for EMD mining algorithms.

### *A. Adapting Existing Laws to Regulate EMD*

One approach to regulating EMD is to adapt existing laws for that purpose. For instance, some scholars suggest expanding the scope of HIPAA to include companies outside the traditional healthcare system, such as app developers and wearable manufacturers.[353] It may also be possible to employ existing frameworks of notice and consent to enable people to opt in to services that mine EMD the way that Apple asks users of its smart watch to opt in to medical research. However,

351. *Id.* at 1186.

352. *E.g.*, David J. Kaufman, Juli Murphy-Bollinger, Joan Scott & Kathy L. Hudson, *Public Opinion About the Importance of Privacy in Biobank Research*, 85 AM. J. HUM. GENETICS 643 (2009).

353. Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 46–47 (2016).

there are limits to how far existing legal mechanisms can be stretched to meet the needs of EMD regulation.

### *1. Expanding the Scope of HIPAA*

One approach to regulating EMD involves expanding HIPAA's definition of covered entities to include entities outside the healthcare sector.[354] The goal is to regulate health data collected outside of clinical contexts.[355] To that end, Elizabeth Brown recommends bringing employers, app developers, and wearable manufacturers within HIPAA's definition of covered entities.[356]

Brown also suggests amending HIPAA to include a private right of action, enabling consumers to sue employers, app developers, and wearable manufacturers for health data breaches.[357] However, expanding HIPAA's scope is inadequate to address the risks posed by EMD mining. Though fines imposed on companies for HIPAA violations are sometimes substantial, ranging from thousands to millions of dollars, they are often insignificant compared to the profits of major hospitals and health systems responsible for the violations, and thus their effectiveness as a deterrent for data breaches is dubious.

In 2019, HHS, which enforces HIPAA violations, increased the maximum penalties to account for inflation.[358] The largest available penalty became $1,711,533.[359] Fines of this magnitude are small compared to the profits of leading healthcare organizations, and they are even smaller compared to the profits of tech platforms that mine EMD. For instance, Alphabet's net profit was $34.34 billion in 2019.[360] Facebook's was $18.48 billion.[361] The maximum penalty under HIPAA is less than a hundredth of one percent of each company's annual net profits.[362] If HIPAA's definition of covered entities was expanded to include them, its maximum fines would be ineffective deterrents.

---

354. *Id.*

355. *Id.*

356. *Id.*

357. *Id.*

358. Steve Alder, *HHS Increases Civil Monetary Penalties for HIPAA Violations in Line with Inflation*, HIPAA J. (Nov. 11, 2019), https://www.hipaajournal.com/hhs-increases-civil-monetary-penalties-for-hipaa-violations-2019-inflation/ [https://perma.cc/4BQQ-636Z].

359. *Id.*

360. Press Release, Alphabet, Alphabet Announces Fourth Quarter and Fiscal Year 2019 Results (Feb. 3, 2019), http://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf [https://perma.cc/6YKT-G46M].

361. Press Release, Facebook, Facebook Reports Fourth Quarter and Full Year 2019 Results, (Jan 29, 2020), https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx [https://perma.cc/5HUJ-RYDZ].

362. Joseph Johnson, *Revenue of Google from 1st Quarter 2008 to 4th Quarter 2020*, STATISTA (Feb. 8, 2021), https://www.statista.com/statistics/267606/quarterly-revenue-of-google/#:~:text=In%202019%2C%20Google%20accounted%20for,Search%2C%20Google%20Maps%20and%20more [https://perma.cc/36G4-4M6S]; Press Release, Microsoft, Microsoft Cloud Strength Drives Third Quarter Results (Apr. 24, 2019), https://www.microsoft.com/en-us/Investor/earnings/FY-2019-Q3/press-release-webcast [https://perma.cc/3WD3-CJGK].

One recent study suggests that HIPAA may have done little to deter data breaches during the past decade.[363] According to the authors, the health data of approximately 169 million Americans was exposed through 1,461 data breaches involving 1,388 entities between 2009 and 2019.[364] Adding a private right of action to HIPAA, including the option to file class action suits, could be beneficial. If done in conjunction with an expansion of HIPAA's scope, it might serve as a deterrent. However, another serious drawback of adapting HIPAA to regulate EMD is that it contains loopholes that allow entities to profit from patient data if the data is first de-identified. In other words, if certain identifying information is removed from the data, then it is no longer considered personal health data (PHI) under HIPAA, and it can be bought and sold for nearly any purpose. This feature of HIPAA is another example of how the law is somewhat antiquated. Numerous studies demonstrate that de-identified health information can often be re-identified.[365] When HIPAA was drafted, medical records were stored in paper charts, and re-identification would have been extremely difficult, if not impossible. However, today re-identification is aided by the same advances in AI and big data that make mining for EMD possible.

Nicolas Terry and Lindsay Wiley have critiqued HIPAA's lack of a private right of action and explored other means of holding wearable manufacturers liable for breaches of consumer health data such as the common law privacy torts.[366] Claims of intrusion upon seclusion or public disclosure of private facts could help consumers combat the collection and use of their EMD. However, such claims require a showing of specific intent, which can be difficult to prove.[367] Attributing specific intent to app developers and wearable makers may be particularly challenging in cases where EMD mining software functions autonomously and draws conclusions that developers might not have foreseen.

### *2. Relying on Notice and Consent*

One way to regulating EMD is to improve upon existing approaches to protecting privacy through notice and consent. This approach could require entities that mine EMD to provide people with meaningful notice of their actual data mining practices, and if consumers consent, then any amount of EMD mining would be permissible. However, if they do not consent, then no EMD mining would be permitted. To be effective, this approach requires a pure opt-in model and

363. John (Xuefeng) Jiang, *Types of Information Comprised in Breaches of Protected Health Information*, 172 ANNALS INTERNAL MED. 159, 159 (2020).

364. *Id.*

365. *See, e.g.*, Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019, 3:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ [https://perma.cc/L268-QVBF].

366. Nicolas P. Terry & Lindsay F. Wiley, *Liability for Mobile Health and Wearable Technologies*, 25 ANNALS HEALTH L. 62, 93 (2016).

367. *Id.*

complete transparency on behalf of platforms, which is very different from their prevailing practices. Many platforms mine EMD surreptitiously and by default, without providing options for users to opt out. For instance, Facebook mines EMD from people by default and prevents them from opting out. It even collects data from people who do not have Facebook accounts.[368] Moreover, its data policy does not disclose to users that their digital traces will be collected, analyzed, and used to calculate a suicide score that could influence whether police are sent to their homes.[369] In fact, its policies contain no mention of suicide.[370] Similarly, individuals in crisis who may benefit from speaking to counselors at Crisis Text Line have no way to opt out of having their texting data mined for EMD. If they do not want to have their digital traces collected and analyzed, then their only option is to avoid using the platform. Offering no means for people to opt out of invasive data collection and EMD mining incentivizes them to avoid seeking help.

A robust notice and consent model would require Facebook to provide meaningful notice to its users that suicide screening is performed and describe the associated risks (to date, Facebook has acknowledged no risks associated with its suicide prediction system and emphasizes only its potential benefits). However, it is challenging to force platforms to ensure that users are fully informed. They tend to bury information in privacy policies that are too long and cumbersome to read, or they compel users to agree to their terms by deploying dark patterns that nudge users to reveal more data than they would prefer to provide.[371] Furthermore, even if people are given adequate notice and opportunities to opt out of EMD collection, there are many problems with the opt-out approach. For instance, companies often deploy dark patterns, user interface designs that exploit people's cognitive biases and coerce them to do things they would rather not do, to prevent people from finding opt-out options or nudge them to keep data collection enabled.[372]

A better approach entails requiring people to opt in to EMD mining while placing limits on the types of EMD that may be collected and how it may be used. For example, the users of social media platforms could be presented with a menu of options that include predictions about self-harm, substance use, mental health conditions, and physical health conditions. They could be prompted to choose which types of EMD-based health surveillance programs they would like to opt in

368. *See* Russel Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense*, VERGE (Apr. 11, 2018, 3:53 PM), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy [https://perma.cc/259Q-CEY8].

369. *Data Policy*, *supra* note 168.

370. *Id.*

371. *See, e.g.*, Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the 'Privacy Paradox*,*'* 31 CURRENT OP. PSYCH. 105, 107 (2020) (describing dark patterns, features of user interfaces designed to exploit cognitive biases and nudge people to do things they would not otherwise do).

372. *See, e.g.*, Hana Habib & Lorrie Cranor, *It's Shockingly Difficult to Escape the Web's Most Pervasive Dark Patterns*, FAST CO. (Nov. 4, 2019), https://www.fastcompany.com/90425350/its-shockingly-difficult-to-escape-the-webs-most-pervasive-dark-patterns [https://perma.cc/N38Q-VXBZ]; *see also, e.g.*, Waldman, *supra* note 371.

to and whether they would like the information to be used for other purposes such as targeted advertising. Specifically, Facebook users could be prompted to opt in to suicide screening. Additional options could be provided, such as which interventions should be initiated if Facebook's systems calculate a high risk of suicide or substance use for the user. Available options might include notifying friends or family, contacting healthcare professionals, providing the user with suicide prevention resources, and sending first responders to the person's home. If users were adequately informed, and they affirmatively opted in to such a system, then under this regulatory approach, it would be permissible for Facebook to mine EMD for suicide prediction and prevention purposes. Implementing a way for users to choose from a menu of options is within the technical capabilities of internet platforms, and their decision to exclude this feature is overly paternalistic, demonstrating a lack of respect for user privacy, safety, and autonomy.

An opt-in approach to EMD mining would better inform consumers about how their digital traces are collected and used. Moreover, it would address concerns associated with breaching contextual integrity. If people are fully informed about how their data is utilized, then the bounds of contextual integrity remain intact even when EMD is mined. However, even opt-in approaches have shortcomings. For instance, companies might continue to implement misleading policies and manipulative dark patterns to coerce people to opt in to EMD mining.[373] Alternatively, they may penalize or deny access to people to who choose not to opt in. For this reason, it is important to include non-discrimination provisions in privacy legislation to prevent companies from penalizing people for exercising their privacy rights.[374]

One reason to prohibit EMD mining by default is that digital traces are often collected from the environment without people's knowledge. For example, ambient intelligence technologies in public spaces can mine EMD regardless of whether data subjects have relationships with the companies collecting their digital traces. Moreover, companies including Facebook collect data on people who never signed up for their services.[375] It is unclear how one could provide adequate notice to people that their digital traces will be collected every time they visit a website, walk down a street, or enter a store. Even if it was possible to provide adequate notice, it is unclear how they could opt out. Their only effective option would be to stop using the site, walk down a different street, or visit a different store, which is clearly

373. *See* Waldman, *supra* note 371, at 109.

374. *See* Jerel Pacis Agatep, *Prop 24 (California Privacy Rights Act) Extends CCPA's Antidiscrimination/Retaliation Provision to Employees, Applicants, and Independent Contractors.*, NAT'L L. REV. (Nov. 13, 2020), https://www.natlawreview.com/article/prop-24-california-privacy-rights-act-extends-ccpa-s-anti-discriminationretaliation [https://perma.cc/NY23-PJG2] (describing anti-discrimination and retaliation provision of the California Privacy Rights Act).

375. *See* Kurt Wagner, *This Is How Facebook Collects Data on You Even if You Don't Have an Account*, VOX (Apr. 20, 2018, 1:02 PM), https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg [https://perma.cc/6UXB-FAN2] (describing Facebook's creation of "shadow profiles" on people who do not use Facebook).

undesirable from a public policy perspective because it would inhibit people from engaging in commerce and social interaction.

The EU's GDPR relies on notice and consent without requiring it by default.[376] As described above, article 6(1)(a) of the GDPR requires that data subjects consent to the processing of personal data for one or more specific uses. However, articles 6 and 9 contain exceptions to the consent requirement that may allow EMD to be mined even if data subjects are not informed of the risks, or they know of the risks and do not consent. Organizations that mine EMD can potentially rely on the exceptions to mine EMD without people's knowledge. This example illustrates the importance of instituting safeguards that go beyond notice and consent.

Consent has proven to be too slippery a concept to provide much real protection from EMD mining, and effective implementation is challenging if not impossible. Facebook's insistence that users have consented to being analyzed and scored for suicide risk illustrates that views differ on what constitutes adequate notice and consent, and platforms can influence and distort those views. Moreover, members of some populations, such as school-age children and people with cognitive impairments, may have difficulty evaluating the risks of EMD mining and be unable to consent. There must be mechanisms to protect those individuals that go beyond notice and consent.

### *B. Proposed Privacy and Data Protection Laws Do Not Go Far Enough*

There have been several recent proposals to fill the gaps left by HIPAA and regulate health data collected by wearable makers, app developers, and manufacturers of other internet-enabled devices. However, they either specifically exclude EMD from their scope or acknowledge the potential for health inferences to be made yet contain loopholes that allow entities to mine EMD for a wide variety of purposes. Though Congress is unlikely to enact these proposals, their strengths and shortcomings are useful for developing more effective health privacy laws.

#### *1. Protecting Personal Health Data Act*

In 2019, U.S. Senators Amy Klobuchar and Lisa Murkowski introduced the Protecting Personal Health Data Act.[377] The bill aims to protect health information collected by fitness trackers, wellness apps, social media sites, and direct-to-consumer DNA testing companies.[378]

---

376. Elettra Bietti, *The Discourse of Control and Consent over Data in EU Data Protection Law and Beyond*, LAWFARE (Jan. 10, 2020, 8:00 AM), https://www.lawfareblog.com/discourse-control-and-consent-over-data-eu-data-protection-law-and-beyond [https://perma.cc/D5UB-Q57E].

377. Protecting Personal Health Data Act, S. 1842, 116th Cong. (2019).

378. *See id.*

Though the Protecting Personal Health Data Act is innovative, it would put consumers at risk because it contains an express exception for EMD.[379] One section of the bill excludes from its scope "products on which personal health data is derived solely from other information that is not personal health data, such as Global Positioning System [GPS] data."[380] In other words, the bill would only regulate TMD and create a safe harbor for health data inferred from digital traces, which is essentially the definition of EMD.[381] If passed, the bill would allow entities to continue mining EMD to surveil people's health with impunity.[382] However, most public discussion of the bill has overlooked this detail.[383]

### *2. Smartwatch Data Act*

Other efforts to regulate data collected by wearables and apps include a bill proposed by Senators Bill Cassidy and Jacky Rosen called the "Stop Marketing And Revealing The Wearables and Trackers Consumer Health" (SMARTWATCH) Data Act (or simply the "Smartwatch Data Act").[384] The bill would bring the regulation of health data collected by apps and wearables under the purview of the Department of Health and Human Services, which is currently responsible for enforcing HIPAA violations.[385] According to Senator Cassidy, "The Smartwatch Act prevents big tech data harvesters from collecting intimate private data without patients' consent. Americans should always know their health information is secure."[386]

The Smartwatch Data Act is notable because it includes within its definition of consumer health information "any information about . . . health status . . . that is created or collected by a personal consumer device, whether detected from sensors or input[ted] manually."[387] This definition should encompass EMD because it is created by consumer devices that collect digital traces through sensors and manual input. Moreover, the Act includes software within its definition of consumer device, which suggests that social media platforms and smartphone apps fall within its

379. *See* Marks, *Emergent Medical Data*, *supra* note 4 (defining emergent medical data).

380. S. 1842 § 3(C)(i).

381. *See* Marks, *Emergent Medical Data*, *supra* note 4.

382. *See id.*

383. *See* Donna Rosato, *What Your Period Tracker App Knows About You*, CONSUMER REPS. (Jan. 22, 2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you/ [https://perma.cc/BU6X-UHTU]; Tyrone Richardson, *Senate Privacy Bill Would Expand HIPAA, Restrict Health Apps*, BLOOMBERG L. (June 14, 2019, 2:41 PM), https://news.bloomberglaw.com/privacy-and-data-security/lawmakers-float-federal-wearable-devices-privacy-legislation [https://perma.cc/WPS7-G9GG].

384. Stop Marketing and Revealing the Wearables and Trackers Consumer Health Data Act, S. 2885, 116th Cong. (2019).

385. Andrea Park, *Senators Propose Legislation to Regulate Harvesting, Sharing Smartwatch Data*, BECKER'S HOSP. REV. (Nov. 20, 2019), https://www.beckershospitalreview.com/healthcare-information-technology/senators-propose-legislation-to-regulate-harvesting-sharing-smartwatch-data.html [https://perma.cc/6FCG-AK8H].

386. *Id.*

387. S. 2885 § 2(6).

scope. Nevertheless, the Smartwatch Data Act provides less protection than is desirable to shield people from the potential harms of EMD mining.

Like HIPAA, the Smartwatch Data Act includes exceptions for data that is "aggregated" or deidentified.[388] Furthermore, like the GDPR, the Act contains exceptions for data that is used "in the public interest."[389] Specifically, it allows even non-anonymized data to be "provided to academic, medical, research institutions, or other nonprofit organizations acting in the public interest for the purpose of detecting or responding to security incidents; preventing fraud; conducting scientific, historical, or statistical research, or preserving the security and safety of people or property."[390] This broad exception would allow personally identifiable data, including EMD, to be transferred for the listed purposes. As a result, companies such as Facebook, Google, and Crisis Text Line could mine EMD from users and transfer it to other entities for a variety of purposes. Stronger regulation is required to protect consumers from the risks of EMD mining.

### *3. Consumer Online Privacy Rights Act*

On November 26, 2019, U.S. Senators Maria Cantwell, Amy Klobuchar, Ed Markey, and Brian Schatz proposed the Consumer Online Privacy Rights Act (COPRA).[391] The Act defines covered data as "information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data."[392] It further defines derived data as "data that is created by the derivation of information, data, assumptions, or conclusions from facts, evidence or another source of information or data about an individual."[393] This definition suggests that EMD, which is derived from digital traces, should be captured by the term derived data, and because derived data is included in the Act's definition of covered data, EMD is covered by the Act.

Section 101 creates a duty of loyalty that prohibits covered entities from engaging in deceptive or harmful data practices.[394] Thus, the Act imposes one of the classic fiduciary duties upon covered entities.[395] Section 101 defines a deceptive data practice as "an act or practice involving the processing or transfer of covered data in a manner that constitutes a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act."[396] When framed as a breach of

388. *Id.* § 3(a)(1).
389. *Id.* § 3(b)(1)(F).
390. *Id.*
391. Tony Romm, *Top Senate Democrats Unveil New Online Privacy Bill, Promising Tough Penalties for Data Abuse*, WASH. POST (Nov. 26, 2019, 4:45 AM), https://www.washingtonpost.com/technology/2019/11/26/top-senate-democrats-unveil-new-online-privacy-bill-promising-tough-penalties-data-abuse/ [https://perma.cc/3TF8-BMYU].
392. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. § 2(8)(A) (2019).
393. *Id.* § 2(11).
394. *Id.* § 101(a).
395. *See id.*
396. *Id.* § 101(b)(1).

contextual integrity, EMD mining should meet the Act's definition for deceptive data practices because it violates people's expectations regarding the collection of data in one context and its processing and use in another.

Section 101 also prohibits harmful data practices, which it defines as "the processing or transfer of covered data in a manner that causes or is likely to cause any of the following: [f]inancial, physical, or reputational injury to the individual" or "[p]hysical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person."[397] This provision is notable because it offers a way to leverage the common law tort of intrusion upon seclusion without having to prove the specific intent of a covered entity. If the intrusion would be offensive to a reasonable person, then section 101's requirements to establish harm have been met. Because most people remain unaware that EMD mining occurs, and due to the sensitive nature of the information inferred from digital traces, EMD mining would likely be offensive to a reasonable person.

Section 102(a) creates a right of access requiring covered entities, upon receipt of a verified request, to "provide the individual, in a human-readable format that a reasonable individual can understand," with copies or accurate representations of the covered information the entities possess about the individual.[398] Covered entities must also disclose the names of third parties to which they have transferred the individual's data and the purpose for the transfer.[399] This section seemingly creates a powerful individual right to request that platforms reveal the third parties with whom their EMD has been shared. However, without an effective means of enforcing it, the right may be ignored by large tech companies. Early reports suggest that Facebook failed to comply adequately with requests made under the right of access created by the California Consumer Privacy Act.[400]

Section 103(1) creates a right for individuals to request that entities delete covered data about the individual that the entity possesses.[401] Notably, because EMD falls within the Act's definition of covered data, this section creates a right to delete EMD that covered entities have mined.[402] However, section 103(2) requires covered entities only to inform third parties to which they have transferred an individual's covered data of the individual's deletion request.[403] There is no

397. *Id.* § 101(b)(2).

398. *Id.* § 102(a).

399. *Id.*

400. Kari Paul, *Was Anyone Ever So Young? What 10 Years of My Instagram Data Revealed*, GUARDIAN (Jan. 17, 2020, 1:00 AM), https://www.theguardian.com/technology/2020/jan/16/instagram-my-data-california-privacy-law-request [https://perma.cc/3BRW-Z6RT] (reporting that Facebook failed to provide all the information it acquires on users through its Instagram platform in response to a request made under the California Consumer Privacy Act).

401. S. 2968 § 103(1).

402. *See id.*

403. *Id.* § 103(2).

requirement that the entity to which covered data was transferred delete the data.[404] The Act's failure to require third parties to delete people's data in response to a request exercised under section 103 is one of its shortcomings.

Section 104 creates a right to correct inaccuracies in covered data collected by covered entities.[405] However, like section 103(2), it only requires covered entities to inform third parties to which an individual's data has been transferred of a request to correct inaccuracies.[406] It does not require third parties to correct those inaccuracies.

Section 105(a) creates a right to data portability that requires covered entities, upon receipt of a valid request, to export the individuals covered data.[407] However, the section creates an exclusion for derived data, and therefore, covered entities would not be required to export EMD in response to a request from individuals.[408] This exception is problematic because it treats derived data (and EMD) as the property of the collecting entity instead of the individual from whom the data is derived. Viewed in this light, suicide predictions derived by Facebook and other platforms would not need to be exported to the individuals about whom the predictions were made.

Section 108 creates civil rights protections.[409] Specifically, it prohibits covered entities from processing or transferring covered data "on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion . . . or disability" for a variety of purposes, which include advertising, leasing, housing, employment, and educational opportunity "in a manner that unlawfully discriminates against or otherwise makes the opportunity unavailable to the individual or class of individuals."[410] This section aims to address the type of discrimination described by HUD's 2018 complaint against Facebook.[411]

Section 110(d) includes exceptions to the express consent requirement.[412] In other words, it creates loopholes through which EMD can be mined without people's knowledge or consent. It states, "A covered entity may process or transfer covered data without the individual's affirmative express consent for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose."[413] However, the listed purposes are overly broad. For instance, section 110(d)(1)(F) creates an exception if the covered entity is processing a person's data "to prevent an individual from suffering harm where the covered entity believes in good faith that the individual is in danger of

404. *See id.*
405. *Id.* § 104.
406. *Id.* § 104(2).
407. *Id.* § 105(a).
408. *See id.*
409. *Id.* § 108(a).
410. *Id.*
411. *See* Jan & Dwoskin, *supra* note 233.
412. *See* S. 2968 § 110(d).
413. *Id.* § 110(d)(1).

suffering death or serious physical injury."[414] This section is likely applicable to suicide, substance use, and violence detection algorithms, and the requirement that covered entities must have only a good faith belief that the individual is in danger is overly permissive. When Facebook and other platforms send police to people's homes, they may have a good faith belief that the individuals are in danger.[415] However, a higher standard should be implemented requiring at least a reasonable belief, thereby demanding a higher degree of certainty on the part of covered entities before this exception applies.

Section 110(d)(1)(H) creates an exception to the consent requirement if a covered entity is processing data "to conduct scientific, historical, or statistical research in the public interest."[416] To the drafters' credit, this section requires that such research be "governed by an institutional review board or a similar oversight entity."[417] However, the phrase "or similar oversight entity"[418] creates too much wiggle room for EMD-mining entities to create sham oversight boards that are not independent or whose review is optional or at the discretion of corporate employees.

### *C. Next Generation Data Protection for Minimizing EMD-Related Risks*

The following Section offers preliminary recommendations for what should be included in the next generation of privacy and data protection laws to mitigate the risks of EMD mining. Potential regulatory options are outlined in broad strokes, and more specific recommendations may be discussed in future articles. The strengths and weaknesses of current and proposed privacy and data protection laws should inform the drafting of the next generation of laws.

Regulation could potentially govern several different steps in the EMD mining process. For instance, it could require entities to obtain explicit informed consent from people before digital traces are collected. However, as discussed above, there are limits to how effective a notice and consent regime can be. Accordingly, any new privacy or data protection laws should regulate the collection of digital traces regardless of whether consent is obtained. Potential options include limiting which entities can collect digital traces or restricting the uses for which they may collect them; controlling which entities can develop, possess, or deploy EMD mining algorithms; limiting the situations in which EMD mining algorithms can be deployed; constraining the use of EMD after it is mined; and regulating the testing, safety, and transparency of EMD mining algorithms.

---

414. *Id.* § 110(d)(1)(F).

415. It is difficult to know for sure because Facebook keeps the information on which it bases its beliefs a secret. *See* Singer, *supra* note 31.

416. S. 2968 § 110(d)(1)(H).

417. *Id.*

418. *Id.*

*1. Ban or Regulate the Collection of Digital Traces*

One approach is to regulate EMD mining at the collection stage, the points at which digital traces are produced, regardless of whether people provide consent. This type of regulation might prohibit all entities from collecting digital traces, prevent only certain types of entities from doing so, or limit collection to certain types of digital traces or specific contexts.

Technically, it would be possible for companies such as Facebook and Google to offer their services to users without collecting digital traces. Facebook could allow people to post text, video, and images without collecting any data about the user-generated content. However, such an austere solution would be extremely unpopular with tech companies because they derive a substantial portion of their profits from user surveillance. They would have almost no ability to offer targeted advertisements or tailor their interfaces based on users' perceived preferences. Banning the collection of digital traces might also be undesirable from a public policy perspective because it would undermine platforms' ability to moderate content. For instance, Facebook uses AI to scan uploaded images for evidence of weapons, child pornography, and other objectionable content.[419] Banning the collection of digital traces would prevent it from using this technology.

A complete ban would also prevent public health applications for EMD mining. Without collecting digital traces, it would be impractical to use social media to monitor the spread of infectious diseases and other public health concerns such as suicide and substance use disorders. However, as described above, even these potentially beneficial uses have risks, and it may be desirable to ban or restrict their use.

Nevertheless, because there are at least some socially desirable reasons to collect digital traces, a more sensible approach would be to limit the contexts in which digital traces may be collected and the ways in which they can be used. For instance, it may be reasonable to restrict the collection of digital traces in contexts where sensitive information changes hands, such as in doctor's offices and on crisis help lines.

Banning the collection of digital traces in these contexts will maintain the trust essential to forming effective relationships. Moreover, it may be desirable to prohibit the collection of digital traces from information that users believe is private. For instance, Facebook might be permitted to collect digital traces from information posted on publicly accessible parts of its website, but not from private messages exchanged between users. For the purposes of suicide prediction, the site

419. *See* Catherine Shu, *Facebook Says It Removed 8.7M Child Exploitation Posts with New Machine Learning Tech*, TECHCRUNCH (Oct. 24, 2018, 7:48 PM), https://techcrunch.com/2018/10/24/facebook-says-it-removed-8-7m-child-exploitation-posts-with-new-machine-learning-tech/ [https://perma.cc/M5LM-2ZJJ]; *Facebook's AI Wipes Terrorism-Related Posts*, BBC NEWS (Nov. 29, 2017), https://www.bbc.com/news/technology-42158045 [https://perma.cc/DAZ6-BEKG].

currently treats all data the same regardless of the user's perceptions regarding whether it is public or private.

### *2. Regulate EMD Mining Algorithms*

A second approach is to regulate the possession and use of EMD mining algorithms. Certain entities would be prevented from training EMD mining algorithms (regulating the training stage) or from deploying them to produce EMD (regulating the deployment stage). One way to regulate which entities can possess and use the algorithms is to implement a licensing system. Entities seeking a license could be required to state the purpose of their proposed EMD mining models, define the societal risks and benefits of deploying them, and subject the models to standardized safety testing and privacy evaluation. Under this regulatory model, if an entity is not among the groups that are licensed to use EMD mining algorithms, then it cannot mine EMD regardless of whether users provide consent.

Unlike current and proposed data protection laws, which start from a presumption that any organization can possess and use EMD mining algorithms, a licensing system would start with the presumption that entities cannot possess and use such algorithms unless they successfully meet certain requirements. Licenses might be made available only to certain types of entities such as public health agencies and hospitals, and internet platforms such as Facebook and Google might be prohibited from receiving them. Alternatively, a licensing system could allow any organization to train and use EMD mining algorithms if it meets certain requirements regarding testing, transparency, and safety.

Treating EMD mining algorithms as medical devices would essentially be a form of licensing. Under this approach, anyone could use the algorithms if they meet the safety, accuracy, and transparency requirements of the FDA. However, there are many details that must be worked out. For instance, how can the safety, accuracy, and transparency of EMD mining algorithms best be evaluated? For algorithms that predict suicide, substance use disorders, and violence, what level of accuracy should be considered safe and effective? These and many other questions remain unanswered. However, given the FDA's current inclination, it is unlikely to contemplate the nuanced harms of EMD-based algorithms because its outdated risk assessment framework was designed to address the more immediately recognizable harms of traditional medical devices. Moreover, in the name of promoting innovation, the FDA appears to be moving in the direction of less oversight for AI-based medical devices than is required of traditional devices. This approach will allow devices that mine EMD to slip through the cracks without adequate testing for safety and effectiveness.

Regulators must modernize their risk assessment frameworks to include the harms of EMD-associated stigmatization, discrimination, and manipulation in addition to more cognizable harms such as physical injury and death. They should acknowledge that harms may occur several steps downstream of the devices' use. For instance, when Facebook calculates a suicide risk score for users, it is not

necessarily the score itself that causes harm. Rather, it is Facebook's collaboration with law enforcement, which lacks adequate training for safely responding to mental health emergencies, that causes the physical harm. Thus, regulators must look beyond the traditional dyad, consisting of the medical device manufacturer and the user, to entities with which the manufacturer shares data, such as law enforcement and advertisers, to comprehend the full scope and scale of potential harms. Regulators should think in terms of systems of which device manufacturers and users are two elements. They must also decrease their reliance on the manufacturer's stated purpose for a device when evaluating its risk because the stated purpose of a wellness app, such as relaxation or weight loss, might obscure its deeper purpose as a data mining (and EMD-generating) tool.

### *3. Regulate How EMD Can Be Used*

A third option is to regulate how EMD can be used. This type of regulation would not affect the collection of digital traces or their transformation into EMD. Rather, it would regulate the applications for EMD after it is produced. For example, organizations might be permitted to use EMD to monitor public health but prohibited from intervening. Or they could be allowed to intervene in some ways and not others. Platforms could be permitted to deploy algorithms that screen content for violence, terrorism, and child exploitation while being prohibited from using them for other purposes. Uses for EMD that serve no public health purpose, such as targeted advertising and social credit scoring, could be banned.

Imposing fiduciary duties on EMD miners falls within this category of regulatory solutions. For instance, if entities owed individuals from whom they mine EMD a duty of loyalty, then they would be prohibited from using EMD in ways that harm or do not promote the interests of those individuals. One shortcoming of this approach is the possibility that advertisers will argue that providing people with targeted ads based on their inferred health information promotes their welfare because it makes advertisements more relevant to their needs and interests. The duty of loyalty created by COPRA's section 101 partially addresses this possibility through its intrusion upon seclusion provision. If using EMD to drive targeted ads was found to be offensive under a reasonable person standard, then it would violate the covered entity's duty of loyalty. For example, if a reasonable person would find it offensive that algorithms mine private messages for digital traces to infer one's health status and customize ads based on that inference, then the practice could constitute an intrusion upon seclusion.

### *4. Require IRB Approval for EMD Mining Research*

Because companies engaged in EMD-based profiling are essentially conducting research involving human subjects, they could be required to obtain IRB approval before commencing their research. As discussed above, section 110(d)(1)(H) of COPRA requires such oversight while leaving too much room for

covered entities to design their own in-house versions of IRBs that lack independence.

The next generation of data protection laws must go further. There must be mechanisms to ensure the independence of private ethics boards, and their membership should be diverse. When AI-based research could impact vulnerable populations, such as people with disabilities, the IRB should include people who are members of those populations or who have special experience with the unique risks of doing research involving those groups. Otherwise, the needs of these populations and the risks to their safety and autonomy may be overlooked.

## CONCLUSION

Emergent medical data is a new type of health information made possible by AI paired with internet-enabled devices that allow continuous surveillance of people in all spheres of human activity. Though EMD may have socially beneficial uses, the risk for exploitation is high, and privacy laws designed before the Digital Age provide inadequate protection. Even recently proposed data protection laws, intended to protect health data collected by wearables and smartphone apps, contain gaps that allow EMD mining to proceed unregulated.

Legislators must acknowledge that EMD mining is a pernicious, disruptive practice that violates social norms, defies people's expectations, circumvents existing laws, breaches ethical standards, and can cause serious harm. Moreover, EMD's adoption by the healthcare system represents the interposition of for-profit companies within the doctor-patient relationship. This relationship, defined by compassion and trust, was once considered sacrosanct. In fields such as psychiatry, where the treatment relationship has become increasingly impersonal, the surreptitious use of EMD mining for digital psychiatry and digital phenotyping threatens to erode what trust remains between doctors and patients.

In advertising, EMD allows companies to infer people's thoughts and secrets without their knowledge or consent. Once mined, the information can be used as leverage to manipulate people for the benefit of wealthy corporations while damaging the health of vulnerable individuals and groups. In medical research, EMD mining may advance our understanding of human physiology in states of wellness and disease. However, companies should not be permitted to use it while circumventing ethical standards that evolved to minimize human suffering and exploitation. Doing so would represent a failure to learn from appalling human rights abuses of the past century.

Advancing the socially beneficial uses for EMD while protecting the public from exploitation requires laws that put health inferences front and center instead of treating them as an afterthought. However, current proposals either fail to address health inferences or mention them only tangentially. They rely too heavily on notice and consent, which companies frequently circumvent by implementing dark patterns and other coercive design practices.

When companies outside the healthcare system choose to act like medical researchers or clinicians, they should be subject to legal requirements on par with those imposed on medical professionals.