Biomanipulation

LAURA K. DONOHUE*

TABLE OF CONTENTS

* J.D., Ph.D. Professor of Law, Georgetown Law. The McCourt School Tech & Public Policy program, directed by Michelle De Mooy, generously provided research funding. I am indebted to Elizabeth Brownstein and Yasmeen Rose for their help in compiling many of the patents cited in this Article. Ryan Calo, Julie Cohen, Chris Hoofnagle, David Luban, Michel Paradis, Jennifer Reich, and Mike Seidman provided excellent critiques, for which I am grateful. The Article further benefited from my colleagues' suggestions at the Georgetown Law Faculty Workshop.

INTRODUCTION

Scientific and technological advances in the latter part of the twentieth century transformed the field of biometrics. Carleton Simon, for instance, first postulated using retinal vasculature for biometric identification in 1935,[1] but it was not until forty years later that an Eyedentify patent brought the idea to fruition.[2] In 1937, John Henry Wigmore anticipated using oscilloscopes to identify individuals by speech patterns.[3] Decades later, digitization and speech processors made voiceprint identification possible.[4] In the 1970s, biological discoveries similarly led to the development of deoxyribonucleic acid (DNA) sequencing.[5] And while Alphonse Bertillon in the late nineteenth century postulated iris distinctions, it was only in 1991 that John Daugman patented a means of extracting and encoding their unique patterns.[6]

In this century, as algorithmic sciences, big data analytics, and artificial intelligence (AI) have gained ground, the biometric landscape again has radically

1. *See generally* Carleton Simon & Isadore Goldstein, *A New Scientific Method of Identification*, 35 N.Y. STATE J. MED. 901 (1935) (detailing new method of identification based on correlation of the optic nerve with patterns of blood vessels in the eye).

2. *See* Apparatus & Method for Identifying Individuals Through Their Retinal Vasculature Patterns, U.S. Patent No. 4,109,237 (filed Jan. 17, 1977) (issued Aug. 22, 1978).

3. JOHN HENRY WIGMORE, THE SCIENCE OF JUDICIAL PROOF AS GIVEN BY LOGIC, PSYCHOLOGY, AND GENERAL EXPERIENCE AND ILLUSTRATED IN JUDICIAL TRIALS 284–85 (3d ed. 1937) ("*Vocal Traits*. By means of a well-understood principle, having many applications, the vibrations of the spoken voice on a diaphragm may be accurately translated, through an electrical current, into oscillations of a needle, and . . . arranged to leave a continuous variable ink-tracing as a record. . . . [T]he spoken voice . . . can now . . . be made to leave a . . . record having minute differences of individuality," serving as a "mode of identification.").

4. *See, e.g.*, Voiceprint Identification Sys., U.S. Patent No. 6,356,868 (filed Oct. 25, 1999) (issued Mar. 12, 2002).

5. *See* INTECHOPEN, BIOMETRICS 139–52 (Jucheng Yang ed., 2011).

6. *See* ALPHONSE BERTILLON, IDENTIFICATION ANTHROPOMÉTRIQUE: INSTRUCTIONS SIGNALÉTIQUES 28, 67–79 (1893) (classifying the morphological qualities of each part of the ear); *id.* at 45 (noting upper and lower eyelid, pupil size, iris contours and color); *id.* at 63–65 (noting nose characteristics); *id.* at 82 (noting distance from the base of the nose to the lips, prominence of the lips, etc.); *id.* at 129–33 (noting front and side photographs of the head); Biometric Pers. Identification Sys. Based on Iris Analysis, U.S. Patent No. 5,291,560 (filed Jul. 15, 1991) (issued Mar. 1, 1994); John Daugman, *Iris Recognition: The Colored Part of the Eye Contains Delicate Patterns that Vary Randomly from Person to Person, Offering a Powerful Means of Identification*, 89 AM. SCIENTIST 326, 329 (2001); John Daugman & Cathryn Downing, *Epigenetic Randomness, Complexity and Singularity of Human Iris Patterns*, 268 PROC. ROYAL SOC'Y: BIOLOGICAL SCIS. 1737, 1737 (2001).

altered.[7] The range of collectable Physiological Biometric Characteristics (PBCs), which measure innate human traits, has exploded.[8] The legal literature lags far behind, with almost every treatment of biometrics limited to a few PBCs, such as fingerprinting, facial recognition technology (FRT), or DNA.[9] Nor have scholars considered the rapid expansion in Behavioral Biometric Characteristics (BBCs)—biologically grounded habits and proclivities, such as voice prints, eye movement, or gait signatures. Instead, just a handful of pieces focus on one or two BBCs.[10] Yet thousands of scientific articles over the past fifteen years have focused on how to collect, analyze, and use PBCs and BBCs.[11] Hundreds of

7. *See, e.g.*, PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. STANDARDS & TECH., ONGOING FACE RECOGNITION VENDOR TEST (FRVT) PART 2: IDENTIFICATION 2 (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf [https://perma.cc/YQ86-TN8H].

8. I distinguish in this Article between unique markers associated with a particular body and attributes gleaned, such as age, gender, weight, hair or eye color, race, and ethnicity. Referred to in the literature, variously, as "soft" or "light" biometrics, they may aid in identification but lack distinctiveness and permanence. *See generally* Anil K. Jain et al., *Can Soft Biometric Traits Assist User Recognition?*, 5404 PROC. SPIE 561 (2004) (proposing integration of soft biometric features into outputs of primary biometric systems).

9. *See generally, e.g.*, Natalie Ram, *America's Hidden National DNA Database*, 100 TEX. L. REV. 1253 (2022) (emphasizing DNA); Elizabeth A. Rowe, *Regulating Facial Recognition Technology in the Private Sector*, 24 STAN. TECH. L. REV. 1 (2020) (focusing on FRT); Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 CATH. U. J.L. & TECH. 187 (2018) (isolating voice prints). Some articles focus on state biometric laws, which cover only a few biometrics. *See, e.g.*, Lisa P. Angeles, *Untag Me: Why Federal Judges Are Broadly Construing Illinois's Biometric Privacy Law*, 42 CARDOZO L. REV. 349, 353 (2020) (focusing on FRT aspects of Illinois's Biometric Information Privacy Act (BIPA)). Other works focus on specific use cases, such as collection of athletes' biometric data. *See, e.g.*, Nicholas Zych, *Collection and Ownership of Minor League Athlete Activity Biometric Data by Major League Baseball Franchises*, 14 DEPAUL J. SPORTS L. 129, 132 (2018) (summarizing potential use of Minor League Baseball players' Athlete Activity Biometric Data (AABD)); Skyler R. Berman, Note, *Bargaining over Biometrics: How Player Unions Should Protect Athletes in the Age of Wearable Technology*, 85 BROOK. L. REV. 543, 545 (2020) (advocating for a players' bill of rights to protect their biometric data). Articles looking at biometric privacy do not provide an in-depth examination of the field, instead tending to mention a few biometrics and then focusing on the absence of adequate provisions to address privacy interests. *See, e.g.*, Fiona Q. Nguyen, *The Standard for Biometric Data Protection*, 7 J.L. & CYBER WARFARE 61, 62 (2018); Andrew Serulneck, *The Importance of a Private Right of Action in Federal Biometric Privacy Legislation*, 73 RUTGERS U. L. REV. 1593, 1596–97 (2021); Hannah Zimmerman, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 638–39 (2018).

10. *See, e.g.*, Ian Taylor Logan, Comment, *For Sale: Window to the Soul, Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PA. ST. L. REV. 779, 782 (2019) (discussing eye tracking); Andrew McStay, *Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy*, BIG DATA & SOC'Y, Jan.–June 2020, at 1, 2 (discussing "using computer sensing to interact with emotional life"). While numerous scholars consider privacy in the context of the breadth of information that can be obtained about individuals, they fall short of handling the unique challenge posed by biometric data. *See generally, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) (discussing technology and the rising concern in scholarship over privacy).

11. *See, e.g.*, Amjad Hassan Khan M.K. & P.S. Aithal, *Voice Biometric Systems for User Identification and Authentication – A Literature Review*, 6 INT'L J. APPLIED ENG'G & MGMT. LETTERS 198, 199 (2022); Yimin Yin et al., *Deep Learning for Iris Recognition: A Review*, ARXIV, Mar. 2023, at 1, 3–4; Shuaijie Shan et al., *Prospect of Voiceprint Recognition Based on Deep Learning*, J. PHYSICS: CONF. SERIES, 2021, at 1; Punam Kamari & Seeja K.R., *Periocular Biometrics: A Survey*, 32 J. KING SAUD U. – COMPUT. & INFO. SCIS. 1086, 1087 (2022); Jarina B. Mazumdar & S.R. Nirmala, *Retina*

thousands of patent applications have kept pace.[12] Looking at just six of the most prominent companies, the numbers are staggering: between 2012 and 2022, they collectively applied for or obtained 12,000 to 19,000 biometric-related patents per year.[13]

Legal scholarship has not only missed the depth and breadth of information that can be collected, analyzed, and deployed, but it also has largely overlooked a concerning new practice: biomanipulation, which I define as the use of biometric data to identify, analyze, predict, and manipulate a person's beliefs, desires, emotions, cognitive processes, and/or behavior.[14] Books and articles on consumer and market manipulation, of course, have been around for decades; but the role of biometric data in presenting an immediate, more personalized, and more concerning form of insight and potential control has gone largely unnoticed.[15]

Based Biometric Authentication System: A Review, 9 INT'L J. ADVANCED RSCH. COMPUT. SCI. 711, 712 (2018).

12. *See* Patent Database of Applications Filed 1991–2023 (maintained by author).

13. Amazon: 20,318 patent applications 2000–2023; Apple: 51,045 patent applications 2000–2023; Samsung: 113,207 patent applications 2000–2023; NEC: 19,502 patent applications 2000–2023; Meta/Facebook: 11,982 patent applications 2000–2023. *Id.* (last searched Feb. 2024). Some, like NEC, specifically market their biometric technologies. *See Biometric Authentication*, NEC, https://www.nec.com/en/global/solutions/biometrics/index.html [https://perma.cc/F9E4-F4VN] (last visited Dec. 31, 2024) (listing as the company's "six original biometric authentication technologies": face recognition, iris recognition, fingerprint and palmprint recognition, finger vein recognition, voice recognition, and ear acoustic authentication). Others use it as part of their other products or services. The global biometric technology market, estimated to be worth $34.27 billion in 2022, is expected to expand at a compound annual growth rate of 20.4% until 2030. GRAND VIEW RSCH., BIOMETRIC TECHNOLOGY MARKET SIZE, SHARE & TRENDS ANALYSIS REPORT BY COMPONENT, BY OFFERING, BY AUTHENTICATION TYPE, BY APPLICATION, BY END-USE, BY REGION, AND SEGMENT FORECASTS, 2023 - 2030, https://www.grandviewresearch.com/industry-analysis/biometrics-industry [https://perma.cc/MQH2-YWFQ].

14. During a multi-year social media project that I directed at Georgetown Law, Jennifer Reich, the project coordinator, and I first coined the term to describe the future collection and use of biometric data in virtual reality. This Article builds on that work, further defining the term and offering a broader theoretical grounding. The word also exists in the environmental science literature, but it carries a very different meaning. *See, e.g.*, Joseph Shapiro et al., *Biomanipulation: An Ecosystem Approach to Lake Restoration*, *in* THE PROCEEDINGS OF A SYMPOSIUM ON WATER QUALITY MANAGEMENT THROUGH BIOLOGICAL CONTROL 85, 85 (Patrick L. Brezonik & Jackson L. Fox eds., 1975) (using biomanipulation to describe the use of biological and nutrient solutions to shape water quality and combat eutrophication); Rinaldo Antonio Ribeiro Filho et al., *Eutrophication Indexes Used as Fish Production Parameters in the Itaipu Reservoir (Brazil)*, 4 J. ENV'T. PROT. 151, 152 (2013) (using biomanipulation to describe control of phytoplankton by means of trophic cascade management).

15. *See generally, e.g.*, Kirsten Martin, *Manipulation, Privacy, and Choice*, 23 N.C. J.L. & TECH. 452 (2022) (arguing for the regulation of companies able to manipulate individuals but not discussing biometrics); Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959 (2020) (discussing online tracking without mentioning biometrics); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157 (2019) (weighing the usefulness of legal intervention against manipulative technology but not discussing biometrics); Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1 (2019) (discussing online manipulation without addressing biometrics); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (omitting biometrics); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (noting the use of behavioral data to target consumers/redirection without calling out biometrics); CASS R. SUNSTEIN, THE ETHICS OF INFLUENCE: GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE (2016) (drawing a distinction between coercion and influence without focusing on biometrics).

For the past fifteen years, companies have delved headlong into this realm, pushing the boundaries and looking for ways to capitalize on biometrically enabled inventions. Paralleled by scientific and technological advances, a fundamentally different world has emerged. Early on, emphasis was placed on consumer behavior. Meta, for example, has patented a system to extract linguistic data (words, word stems, and communication patterns) and facial markers, and pair them with demographic and social network information.[16] It considers the level of influence wielded by a node in a network, the number of connections, and engagement patterns, as well as biographic data (e.g., affinities, work experience, education, hobbies, location, and preferences), for news feeds, ranking, advertising, and other activities.[17]

What is at stake, though, is more than just purchasing patterns. Biometric data can be used to generate insight into an individual's beliefs, desires, emotions, and fears—and then to alter them.[18] In 2022, for instance, Amazon secured a patent to analyze an individual's emotional state, set a new target state, deliver content to get the individual to hit that goal, evaluate the impact of stimuli delivered, and continue to shape the individual's emotions until the desired emotional state has been reached.[19] The company explained,

> [I]f a content provider intends to scare a user playing a game, the system may select content known to be scary, such as monsters or zombies, or may present video or audio (e.g., dark colors, scary sounds, or the like) to present in the game to the user. . . . The system may modify content based on a target or desired emotion to cause. For example, additional zombies may be added to an existing scene, or the tone or pitch of audio may be adjusted without causing an interruption to the presentation of the content.[20]

Prior systems fell short; they failed to "account for a user's current emotional state and how significant the transition from the user's current emotional state to

16. Determining User Personality Characteristics from Soc. Networking Sys. Commc'ns & Characteristics, U.S. Patent No. 9,740,752 B2 col. 1 ll. 56–61, col. 4 ll. 3–12 (filed June 3, 2016) (issued Aug. 22, 2017).

17. *Id.* col. 1 ll. 31–33, col. 2 ll. 36–39.

18. *See infra* Sections II.A and II.B. Some propose relatively innocuous, or even welcome, shifts. One baby monitor design, for instance, anticipates the collection of auditory, cardiovascular, respiratory, and other sensory information. *See* Remote Biometric Monitoring Sys., U.S. Patent No. 10,643,081 B2 (filed Oct. 24, 2018) (issued May 5, 2020). The aim is to shape the target's behavior by altering the environment around them. By combining actigraphy data (which measures motor activity) and respiration rates with the target's typical sleep patterns, the system can ascertain whether or not the subject is in light sleep, rapid eye movement, or deep sleep and initiate changes in the temperature or humidity of the room to alter the sleeping state. *Id.* col. 4 ll. 9–10, col. 12 ll. 31–37. It may play music, change the lighting, project images, or release a scent into the air, based on the target's profile. *Id.* col. 4 ll. 23–29, col. 8 ll. 3–9. However welcome such inventions might be, the fact that they are able to use biometric data to alter the subject's mental and physical state represents something different in kind than what has hitherto existed.

19. Interactive Media Facial Emotion-Based Content Selection Sys., U.S. Patent No. 11,373,446 B1 (filed Apr. 26, 2019) (issued June 28, 2022). *See* Figure 1, below.

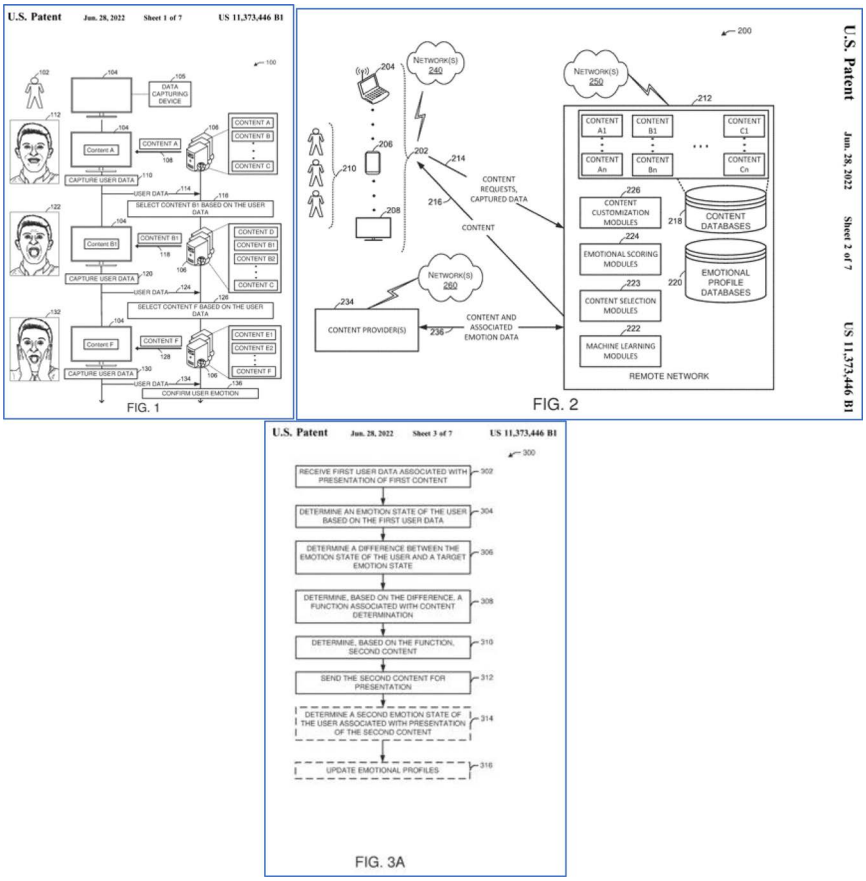
20. *Id.* col. 2 ll. 9–13, 18–22.

a target emotional state at a given time may be."[21] The proposed system selected and customized content to elicit the most direct emotional impact *for each user*, allowing it to obtain the "desired change to the user's emotional state" within time limits.[22] It employed "cameras, microphones, heartrate monitors, biometric sensors, [and] other . . . devices . . . to analyze and identify a user's emotional state at a given time."[23] It could take into account body, arm, and hand position, heartrate, and other indicators, such as "fingerprints, face recognition, blood flow, retinal data, voice data, scents, and other data" to determine the user's precise emotional state.[24] The information could yield insight into "which content is associated with causing certain emotions, how often, how long it takes a user to transition from one emotion to another emotion, and other data."[25] The aim was to develop a system that could manipulate a target's *future* emotions.[26]

Applied in the context of gaming or movies, such technological advances might appear relatively benign. People like to be entertained. But the fact that such information can be harvested and employed to any number of ends without restriction or oversight raises concern, as does the fact that such markers tend to be immutable: it can be very difficult, if not impossible, for targets to change their biometric markers, leaving the target vulnerable to manipulation for the rest of their lives from any actor with access to the data who may be driven by any number of purposes.

21. *Id.* col. 2 ll. 25–28.
22. *Id.* col. 2 ll. 30–33.
23. *Id.* col. 2 ll. 38–41.
24. *Id.* col. 2 ll. 41–60.
25. *Id.* col. 2 ll. 62–65.
26. *See infra* fig. 1.

Figure 1. Interactive Media Facial Emotion-Based Content Selection System, U.S. Patent No. 11,373,446 B1[27]



The above example is just one potential avenue in a sea of new ways to access and use biometric data. Others propose employing it to engage targets on social or political matters, to get them to interact with certain people and ideas, or to alter a target's mood.[28] Levels of attentiveness and propensities revealed by biometric collection can have myriad real-world implications, from determining which university courses a student should take (or avoid taking), to ascertaining

27. '446 Patent, *supra* note 19, figs. 1, 2, 3A.

28. *See, e.g.*, Apparatus for Generating Persuasive Rhetoric, U.S. Patent Application No. 16/109,647 (filed Aug. 22, 2018) (employing biometrics for verification and persuading targets to vote); Device & Method for Inferring Depressive State & Program for Same, U.S. Patent Application No. 17/413,476 (filed Dec. 13, 2019) (employing biological data to predict depressive state of depression or manic-depression); Mach. Learning for Olfactory Mood Alteration, U.S. Patent Application No. 15/427,596 (filed Feb. 8, 2017) (detecting automobile occupants' annoyance, anger, anxiety, depression, and the degree to which they feel hurried, and altering their mood).

which workers are able and willing to fulfill their tasks—and then putting them in conditions in which they are most likely to do so.[29] Biomanipulation can be used to encourage someone to vote (or not), to work for certain employers (or not), to travel to certain places (or not), or to take to the streets (or not). To the extent that it subverts autonomy, it represents something different in kind, not just degree, from what has come before.

This Article throws down the gauntlet, naming, describing, and challenging the practice of biomanipulation. It begins in Section I.A by establishing what is meant by manipulation: knowingly shaping a target's beliefs, desires, and emotions and/or behavior by covertly exploiting a target's vulnerabilities with the aim of altering the status quo.[30] It encompasses shifting an individual's actions as well as non-actions. Any altered state of belief, desire, emotion, or behavior proves sufficient. Section I.B establishes that biomanipulation, a subset of the broader category, seeks to accomplish the third party's aim by employing biometric data in at least one of four ways: as a measurement of the target's biological features or processes; as insight into the target's emotional, cognitive, or behavioral responses; as a correlative device, associating either of the first two with a particular person, group, or community; and/or as a means of delivery. Section I.C distinguishes biomanipulation from other forms of traditional concern about consumer, market, and political manipulation in two respects. First, it focuses on the highly personalized nature of biologically grounded propensities. Biomanipulation offers the manipulator an opportunity to sidestep rational thought. It can be a highly effective means of getting targets to adopt the desired beliefs, desires, sentiments, and actions. Because biometric feedback systems offer a way to bypass conscious decisionmaking, targets may have less and less agency in their actions and become increasingly subservient to the will of others. Second, Section I.C calls out the immutable nature of biometric data as opposed to other forms of information, with all that it entails—up to, and including, persistent vulnerability throughout a target's lifetime. And it is not just corporate entities or political candidates who have access to this data: private parties, state actors, and others can use the same insights to various ends.

Section II.A recognizes the recent expansion in PBCs, presenting a new taxonomy as a way to understand their breadth.[31] It does the same for BBCs, which I

29. *See, e.g.*, Andrew McStay, *Emotional AI and EdTech: Serving the Public Good?*, 45 LEARNING, MEDIA & TECH. 270 (2020); Manuela Ekowo & Iris Palmer, *The Promise and Perils of Predictive Analytics in Higher Education: A Landscape Analysis*, NEW AM. (Oct. 24, 2016), https://www.newamerica.org/education-policy/policy-papers/promise-and-peril-predictive-analytics-higher-education/[https://perma.cc/R57V-BX89]; Daniel M. Goldstein & Carolina Alonso-Bejarano, *E-Terrify: Securitized Immigration and Biometric Surveillance in the Workplace*, 76 HUM. ORG. 1 (2017); Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735 (2017).

30. *See generally* Robert Noggle, *Manipulative Actions: A Conceptual and Moral Analysis*, 33 AM. PHIL. Q. 43 (1996); *infra* Section I.A.

31. While patents do not necessarily mean that a technology has been adopted, they offer important insight; by some estimates, 80% of the technical information patents contain cannot be obtained elsewhere. FRONTEX, EUR. BORDER & COAST GUARD AGENCY, TECHNOLOGY FORESIGHT ON

define as probabilistic calculations based on actions, habits, or proclivities, grounded in human biology and repeated over time. Section II.B turns to the quality of information PBCs and BBCs yield, noting the remarkable scope as well as the nature of the information and what it says about target vulnerability. It addresses how multimodal systems and the pairing of biometric data with other information, such as education level, social media, playlists, email content, and purchase patterns, expand the quality of information available. Remote access, in turn, allows for collection without a targets' knowledge, as well as environmental monitoring. Sophisticated algorithms and the use of AI/ML now imbue such data with predictive power.[32] By anticipating how targets will react to inputs, information, or contexts, and by providing a feedback loop to check hypotheses, entities increase their ability to shape targets' mental, emotional, and physical states.

The Article in Part III turns to statutory and regulatory provisions, noting the dearth of federal and state measures focused on this area, with the only broad movement being at a national level in the regulatory realm. Only four states have introduced statutes focused on biometrics.[33] Each falls short in critical ways of addressing the challenges posed by biomanipulation. Although some states' broader consumer protection privacy laws mention biometrics, they lack the necessary enforcement mechanisms to address the concerns raised.

While it would be impossible to examine each of the dangers presented by biomanipulation, Part IV highlights some of the most serious ones that stem from the shift in power heralded by these technologies. The implications resonate in risks to democratic governance, individual autonomy, access to certain privileges and rights, and the exploitation of individuals, groups, and communities by private or public actors.

I. DEFINING BIOMANIPULATION

Manipulation entails the knowing alteration of a target's beliefs, desires, emotions, and behavior.[34] Covert in nature, it also involves the exploitation of a target's vulnerabilities with the aim of shifting their mental, emotional, or physical status quo.[35] An individual may (or may not) act on the altered condition. It thus incorporates efforts to alter how an individual thinks, and feels, and what they believe or (ostensibly) "know" to be true, accomplished outside rational discourse. In this way it differs from mere persuasion.

BIOMETRICS FOR THE FUTURE OF TRAVEL, ANNEX II: TAXONOMY OF BIOMETRIC TECHNOLOGIES AND BIOMETRICS-ENABLED TECHNOLOGICAL SYSTEMS 18 (2021). They elucidate corporate commitment, not least because of the cost involved. *Id.* And they often build on other filings, providing insight into the arc of the technology and indicating its evolution. *See id.*

32. *See, e.g.*, McStay, *supra* note 29, at 270, 278.

33. In addition, of the fourteen states that have adopted comprehensive consumer privacy laws, only a few explicitly address biometric data. Even then, it's with minimal protections, failing to take account of the breadth and depth of collection and risk of biomanipulation. *See infra* Part III.

34. These aspects reflect elements highlighted by Professor Robert Noggle in 1996. *See* Noggle, *supra* note 30, at 44.

35. Robert Noggle, *The Ethics of Manipulation*, STAN. ENCYCLOPEDIA PHIL. ARCHIVE (Apr. 21, 2022), https://plato.stanford.edu/archives/sum2022/entries/ethics-manipulation [https://perma.cc/4WQJ-9MRS].

Biomanipulation is a particular form of manipulation which employs biometric data to identify, analyze, predict, and manipulate a person's beliefs, desires, emotions, cognitive processes, and/or behavior. The data on which it relies may narrowly relate to an individual's innate physical characteristics; alternatively, it may generate insight into the inner life of the target, revealing information about not just beliefs, desires, or emotions but also cognitive processes, predilections, sexual identity and preferences, mental and physical health, skills, knowledge, behavioral patterns, and the like, which make the target vulnerable. It thus allows third parties to go well beyond what is typically thought of as manipulative behavior in terms of the potential level of control that can be exercised over the target. Biometric data can also act as an anchor, associating information with a particular person, group, or community. Alternatively, it can be employed as a means of delivering stimuli. While the focus may be on shaping a target's emotional states or cognitive processes, it also may be directed to forcing a target to act in certain ways or to refrain from doing so, the latter of which can be accomplished through direct influence, denial of access to privileges or rights which might otherwise be extended to the target, or exclusion of the target from certain areas or opportunities. At some point, biomanipulation verges on control, dominating the target's response.

Biomanipulation challenges how scholars have traditionally framed consumer, market, and voter manipulation in terms of the target's ability to engage in decisionmaking, as well as the target's knowledge and consent. Unlike other forms of information, such as purchase patterns or political contributions, biometric markers cannot easily be altered: they are innate characteristics. That immutability matters. It creates a vulnerability that persists throughout the target's life. Once captured, moreover, such information can be wielded for innumerable purposes by a wide range of private and public actors.

A. BASELINE: MANIPULATION

Unlike some of its close cousins (such as "free will," "virtue," "knowledge," and "belief"), until relatively recently, philosophical and legal scholarship largely ignored "manipulation."[36] In 1978, Professor Joel Rudinow engaged in one of the earliest discussions, distinguishing it from persuasion and coercion.[37] While the latter two also sought to influence a target's behavior, manipulation entailed something more: it impacted an individual's motivation to act, and it did so "by

36. *See id.* ("Until recently, ordinary manipulation has seldom been the subject of philosophical inquiry in its own right."); Joel Rudinow, *Manipulation*, 88 ETHICS 338, 338 (1978) ("In discussing informally the topic and contents of the following paper, I have encountered no one who has not immediately known what sort of thing I have in mind when I talk about manipulation between persons and who has not also had examples of it ready at hand. Strange, then, to find so little in the way of a systematic account of the concept of interpersonal manipulation, distinguishing it from other means of eliciting behavior. . . .").

37. *See* Rudinow, *supra* note 36, at 338–39.

means of deception or by playing on a supposed weakness."[38] What made coercion more transparent ("and therefore crude by comparison") was the presence of "irresistible incentives."[39] He reasoned that if something was resistible, then it was *only* by playing on weaknesses that an individual could be brought around. Moral opprobrium thus attached to the manipulator's willingness to elicit certain behavior "without regard for—and with a will to interfere with" a target's "operative goals."[40] Rudinow applied a Kantian framing: "Insofar as a person regards the selection of goals as rightfully within his sphere of autonomy and the freedom to pursue his goals as a prima facie right, it is little wonder that he finds attempts to manipulate him objectionable."[41] The manipulator has treated the target as a means, rather than an end.

Rudinow is not alone in considering the element of deception as part and parcel of what we mean by manipulation. Professor of Philosophy Robert Goodin in 1980, for instance, applying it to the political context, offered a two-part test to ascertain whether something constituted manipulation: "1. Is the interference deceptive? 2. Is the interference contrary to the putative will of those subject to it?"[42] In a similar vein, Professor Vance Kasten suggested that "manipulation occurs when there is a difference in kind between what one intends to do and what one actually does, when that difference is traceable to another in such a way that the victim may be said to have been misled."[43]

These approaches have the virtue of capturing the covert quality of what we mean by manipulation, as well as the concept of a shift in the target's actions and (in the case of Rudinow) the sense of playing on an individual's weaknesses to accomplish the aim. Where these theorists fall short is in assuming that the direction adopted is contrary to the target's will or legitimate interests.[44] It may be that the direction chosen entirely comports with what an individual would like to do (indeed, in some cases *ought* to do), based on the effect of the manipulative behavior. The target is not so much being *mis*led as being led to act in a particular manner. Nor is it necessarily just weaknesses that can be exploited. An individual's strengths, too, can prove effective as a means of manipulation. It is thus not so much a weakness as a vulnerability—something that makes the individual susceptible to manipulation. Rudinow, Goodin, and Kasten further miss that it is not

38. *Id.* at 346 ("A attempts to manipulate S iff [sic] A attempts the complex motivation of S's behavior by means of deception or by playing on a supposed weakness of S.").

39. *Id.*

40. *Id.* at 347.

41. *Id.*

42. ROBERT E. GOODIN, MANIPULATORY POLITICS 35 (1980).

43. Vance Kasten, *Manipulation and Teaching*, 14 J. PHIL. EDUC. 53, 54 (1980).

44. I depart here from theorists who consider manipulation to result in behavior not in the target's best interests. *See, e.g.*, Anne Barnhill, *What Is Manipulation?*, *in* MANIPULATION: THEORY AND PRACTICE 51, 52 (Christian Coons & Michael Weber eds., 2014) (defining manipulation as "directly influencing someone's beliefs, desires, or emotions such that she falls short of ideals for belief, desire, or emotion in ways typically not in her self-interest or likely not in her self-interest in the present context").

just the target's goals that may be altered, but the state of being of the target: the mind itself may be shaped by the manipulator.

In 1996, Professor Robert Noggle tackled this last aspect of manipulation, proposing as a central element the objectification of the target, i.e., treating them as though they "were some sort of object or machine."[45] He explained, "It's as though the manipulator controls his victim by 'adjusting her psychological levers.'"[46] He isolated three in particular—belief, desire, and emotion—noting that by operating directly on each of these, a manipulator can get a target to deviate from certain norms or ideals. He thus preserved the idea of an altered course while building out how such influence could occur.[47]

For Noggle, different approaches marked each lever. For the first, belief, deception (i.e., conveying knowingly false information) was just one way in which the status quo could be changed.[48] Irrelevant information meant to distract a target (even if true), as well as insinuations, could also undermine belief.[49] Conditioning an individual to instill desires that they otherwise would not hold constituted the second lever, while efforts to incite certain forms of emotion marked the third.[50] Noggle pointed to the importance of emotion in making salient whatever is most important in any given context.[51] Manipulation thus interferes in this process by elevating certain emotions which highlight information that may be less salient, attention to which is engineered by others.[52] In sum, for Noggle, direct and indirect deception, tempting others, conditioning them to have desires that do not conform to their beliefs, and inciting what he termed "inappropriate" emotion (i.e., a departure from the ideal emotions a target might otherwise hold as indicative of salient details) all contribute to manipulative behavior. Like Rudinow, Noggle underscored the moral opprobrium that attaches: because rational moral agency is crucial to personhood, such actions treat the individual as less than a person, making manipulation morally wrong.

Noggle's insights are important. They highlight that it is not just getting an individual to act or refrain from acting that constitutes manipulation, but also getting a target to believe, want, or feel in a particular way. His approach calls out

45. Noggle, *supra* note 30, at 44.

46. *Id.*

47. *See id.* at 44–47.

48. *See id.* at 44; *see also* Marcia Baron, *Manipulativeness*, PROC. & ADDRESSES AM. PHIL. ASS'N, Nov. 2003, at 37, 44 (2003) (isolating "deception, pressure of one kind or another that wears down the victim's resistance, and manipulation of the situation so as to artificially limit the other person's options," as well as "taking advantage of another's emotions or emotional needs" as different forms of manipulation).

49. Noggle, *supra* note 30, at 44–45.

50. *Id.* at 45–46.

51. *Id.*

52. *Id.*

the value of each in and of themselves, as well as the role played by each as a precursor for action. Where Noggle falls short, though, is in sidestepping how shaping the target's worldview interacts with rational decisionmaking. That is, it is one thing for an individual merely to see the world, or oneself, differently. It is another thing altogether the extent to which the individual is aware of the shifts occurring, much less is able to exercise control over whether and how to act upon the altered conditions.

This last set of considerations raises questions about the relationship between manipulation and rationality. Some scholars highlight ways in which manipulation appeals to non-conscious motivations—what Professor Eric Cave refers to as "motive manipulation."[53] Strategic use, for instance, of seduction techniques developed to evoke psychological and physical responses may depend little on rational thought. Subliminal stimuli may do the same. Setting up conditions requiring significant restraint, in turn, may lead to what Professor Michael Cholbi terms "ego depletion," wherein irrational behavior results.[54] But manipulative behavior may also take advantage of conscious motivations, as well as *use* a target's rational thought to accomplish the objective. That is, rational deliberation may very much be part of the ultimate outcome which then drives an individual's behavior. It is not so much then that rational decisionmaking necessarily is not present, but that rational decisionmaking itself can be directed to accomplishing a certain end by the shaping of the target's beliefs, desires, emotions, and knowledge (as distinct from belief, i.e., what an individual "knows" to be "true"). The influence is hidden and instrumental, even if the target then acts rationally in a manner that ultimately accomplishes the manipulator's aim.[55]

53. Eric M. Cave, *What's Wrong with Motive Manipulation?*, 10 ETHICAL THEORY & MORAL PRAC. 129, 132 (2007); *see* Eric M. Cave, *Unsavory Seduction and Manipulation*, *in* MANIPULATION: THEORY AND PRACTICE, *supra* note 44, at 176, 178–79.

54. *See* Michael Cholbi, *The Implications of Ego Depletion for the Ethics and Politics of Manipulation*, *in* MANIPULATION: THEORY AND PRACTICE, *supra* note 44, at 201, 206.

55. For Professor Allen Wood, both manipulation and coercion rely upon rationality. *See* Allen W. Wood, *Coercion, Manipulation, Exploitation*, *in* MANIPULATION: THEORY AND PRACTICE, *supra* note 44, at 17, 31 ("'Manipulation' refers to a way of interfering with or usurping someone's free agency that does not limit or destroy free choice but, rather, influences it in certain ways that promote the outcome sought by the manipulator."). Coercion, in contrast, is the elimination of other possible courses of action. Nevertheless, rationality persists. Wood explains, "Even in the case of external coercion, where all alternatives but one have been rendered unacceptable by the threat of what will happen if the agent takes them, the coercion operates through the agent's choice of the only acceptable alternative over these others." *Id.* at 24. Wood therefore sees manipulation and coercion as two points on a continuum, with coercion an extreme form of manipulation. *Id.* at 31; *see also* Susser et al., *supra* note 15, at 15–16 ("[C]oercing someone deprives them of choice. . . . When coerced, a person is forced to abandon their self-chosen ends (the destination, say), but it is still the coerced person who does the abandoning. They understand what is happening; they recognize it as the only acceptable option.").

In 2019, Professors Daniel Susser, Beate Roessler, and Helen Nissenbaum underscored the interplay between manipulation and rational thought by picking up on the Razian concept of authorship, suggesting that in the case of manipulation, the target has diminished authorship over subsequent actions.[56] It is more than just making less than ideal decisions, regardless of whether they are based on good (or bad) information.[57] For Susser et al., the manipulator has covertly shaped the decisionmaking process, reducing individual autonomy. This is the difference between feeling "used" (in the context of coercion) and being "played" (in the case of manipulation).[58] It is the instrumentality of the action that deprives the target of authorship, making the question one of degree. They write:

> Whereas persuasion and coercion work by appealing to the target's capacity for conscious decision-making, manipulation attempts to subvert that capacity. It neither convinces the target (leaving all options open) nor compels the target (eliminating all options but one). Instead, it interferes with the target's decision-making process in order to steer them toward the manipulator's ends.[59]

They define manipulation as "a kind of influence—an attempt to change the way someone would behave absent the manipulator's interventions."[60] Instead of convincing the target, or even compelling the target to act in a particular way, it interferes with the decisionmaking process itself.[61]

Their insights are important in that they bring out the qualities of autonomy which present in the context of manipulation. To say that an individual has been manipulated in some sense acknowledges that the target is not entirely responsible for the outcome and therefore cannot be said to have had full authorship over their actions. But a critical point which Susser et al. do not draw to the fore relates to the deep liberty interests at stake.

In the centuries-old debate between positive and negative freedom, writers in the last few decades have focused on liberty as freedom from the will of others: i.e., "non-domination."[62] As Professor Philip Pettit observes, this is something more than just non-interference. In the latter case, a power structure may exist, but the external entity has simply refrained from interfering. Non-domination, in contrast, means that an individual is not subject to others' capacity for arbitrary

---

56. *See* Susser et al., *supra* note 15, at 16–18 (critiquing Noggle for "fail[ing] to capture what is distinctive about manipulation—that it undermines our sense of authorship over our decisions"); *see also* JOSEPH RAZ, THE MORALITY OF FREEDOM 385–87 (1986) (detailing constituent elements for authorship over one's actions).

57. *See* Susser et al., *supra* note 15, at 19.

58. *Id.* at 16–17 (emphasis omitted).

59. *Id.* at 17.

60. *Id.* at 13.

61. *Id.* at 17.

62. *See, e.g.*, Quentin Skinner, *The Republican Ideal of Political Liberty*, *in* MACHIAVELLI AND REPUBLICANISM 293, 302 (Gisela Bock et al. eds., 1990). *See generally* PHILIP PETTIT, REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT (1997).

interference.[63] This is freedom in a fuller sense, as it carries with it greater security for both immediate and future liberty. In the case of manipulation, the target's liberty interest has been harmed by the domination of the will of the external actor over that of the target. Additionally, Susser et al. do not acknowledge that it is not necessarily the decisionmaking ability of the target that has been hampered (although this too may be the object of manipulative behavior), but that the *ground* on which a decision is based has been covertly shaped by others. Manipulation may therefore appeal directly to the target's capacity for conscious decisionmaking. But that determination is made based on variables controlled by the manipulator.

Thus far, the emphasis has been on the target. But manipulative behavior may also shape external environments or the broader context in which the target operates—in ways that play to an individual's vulnerabilities—to alter the target's beliefs, desires, emotions, behavior, or some combination thereof. With regard to behavior, moreover, action and non-action matter. It may be that a third party influences the target *not* to take certain steps. Alternatively, a manipulator can use insight into the target to deny the target access to privileges or rights, or to exclude the target from certain opportunities, events, geographic regions, or experiences. It does so by shaping an environment in which non-action is reinforced. To the extent that the target is unaware that this is being done, such behavior can be considered manipulative.

With these elements in mind, for purposes of this Article manipulation entails the knowing alteration of a target's beliefs (which can be shaped through deception, insinuation, information, or distraction), desires (through conditioning a target), or emotions. It involves covert exploitation of a target's vulnerabilities, which may be considered either strengths or weaknesses—what makes them vulnerabilities is their effectiveness. Manipulation may alter a target's rational decisionmaking processes or the grounds on which a decision, impression, or belief is based. The ends are set not by the target but by the entity engaged in the manipulative behavior. What is at stake is a deeper liberty interest: freedom from being subject to the will of others.

B. ROLE PLAYED BY BIOMETRIC DATA

Biomanipulation, a subset of the broader category, can be distinguished by the role biometric data plays in enabling a third party to achieve their ends. Four different mechanisms apply. First, biometric data may be used to evaluate basic biological characteristics, generating insight into a target's vulnerabilities. Second, biometric data can be collected to measure a target's response to certain stimuli or contexts and thereby glean access into an individual's emotional, mental, or physical states and thought processes. Third, it can be employed as an anchor, tying information to a particular individual, group, or community. Fourth, biometric vectors can be used to deliver stimuli in a manner more likely to shape the

63. *See* PETTIT, *supra* note 62, at 24.

target's emotional or mental states or to convince the target to act or refrain from acting in a particular manner. In each of these mechanisms, biometric data is used as a way to subvert individual autonomy. For the first two, it generates insight which can then be exploited to manipulate an individual through more conventional means. For the last, biometrics *is* the vector used to shape behavior.

In the first sense, biometric data can be employed to measure a target's biological features or processes. It is more than just correlating a fingerprint or iris pattern with a particular human being. With the advent of new technologies, biometric markers can reveal a tremendous amount of information. Palm and fingerprint ridges, for instance, have been found to correlate with a range of medical conditions, from hypertension, bronchial asthma, and breast cancer to chromosomal abnormalities and mental illness.[64] The geometry and texture of the iris can convey the target's race and ethnicity.[65] The range of insight that can be gleaned by behavioral biometrics, in turn, is remarkable. They can be used to reveal not just medical conditions, but the target's education level, religious beliefs, desires, fears, fetishes, propensities, likes, and dislikes. Consider, for instance, eye tracking. It has been used to ascertain "gender, age, ethnicity, body weight," and drug use, as well as "personality traits, . . . emotional state[s], skills and abilities, . . . and sexual preferences."[66] Circadian rhythms can, in turn, convey neurodivergence.[67] And so the list continues.

Such information translates into vulnerabilities. Insight into a target's education level, for instance, or whether they are neurotypical or neurodivergent, may change how subsequent information, regardless of whether it is directed to political persuasion, belief formation, conspiracy theory, or some other desired prompt, is delivered.

---

64. *See, e.g.*, Buddhika TB Wijerathne et al., *Dermatoglyphics in Hypertension: A Review*, J. PHYSIOLOGICAL ANTHROPOLOGY, 2015, at 1, 6–8 (citing numerous studies showing certain dermatoglyphic markers are associated with hypertension and general concurrence in regard to the frequency of whorl patterns as well as a higher total ridge count); Sandeep V. Pakhale et al., *Study of the Fingertip Pattern as a Tool for the Identification of the Dermatoglyphic Trait in Bronchial Asthma*, J. CLINICAL & DIAGNOSTIC RSCH. 1397, 1400 (2012) (determining that fingerprints offer a non-invasive anatomical marker of bronchial asthma risk and facilitate early detection); Chintamani et al., *Qualitative and Quantitative Dermatoglyphic Traits in Patients with Breast Cancer: A Prospective Clinical Study*, BMC CANCER, 2007, at 1, 1 (finding, *inter alia*, six or more whorls in the finger print pattern as statistically significant among cancer patients as compared to the control group); Sayee Rajangam et al., *Dermatoglyphics in Down's Syndrome*, 93 J. INDIAN MED. ASS'N 10, 12 (1995) (finding total ridge counts in people with Down's syndrome significantly different from the control group).

65. *See, e.g.*, Xianchao Qiu et al., Global Texture Analysis of Iris Images for Ethnic Classification, *in* ADVANCES IN BIOMETRICS: ICB 2006, at 411, 411 (David Zhang & Anil K. Jain eds., Springer-Verlag Berlin Heidelberg, 2006), https://link.springer.com/book/10.1007/11608288; Stephen Lagree & Kevin W. Bowyer, Predicting Ethnicity and Gender from Iris Texture, *in* IEEE INTERNATIONAL CONFERENCE ON TECHNOLOGIES FOR HOMELAND SECURITY 440, 444–45 (IEEE, 2011), https://ieeexplore.ieee.org/document/6107909.

66. Jacob Leon Kröger, Otto Hans-Martin Lutz & Florian Müller, *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking*, *in* PRIVACY AND IDENTITY MANAGEMENT: DATA FOR BETTER LIVING: AI AND PRIVACY 226, 226 (Michael Friedewald et al. eds., 2020) (surveying the literature on eye tracking and summarizing what information can be gleaned); *see also* Frederike Wenzlaff, Peer Briken & Arne Dekker, *Video-Based Eye Tracking in Sex Research: A Systematic Literature Review*, 53 J. SEX RSCH. (SPECIAL ISSUE) 1008 (2016) (surveying the literature).

67. *See, e.g.*, Ahmed A. Bouteldja et al., *The Circadian System: A Neglected Player in Neurodevelopmental Disorders*, 60 EUR. J. NEUROSCIENCE 3858, 3859 (2024).

The same is true of sexual identity or orientation, cultural heritage, and level of education—all of which, and more, can be ascertained through biometric data.[68] Even as a snapshot in time, especially when paired with contextual information, insight can be gleaned about individuals, groups, and entire communities. By accessing such information, actors can use that knowledge to meet their goals.

The second way that biometrics can be employed amounts to a deeper analysis of the first path, in that collection over time can generate further insight. How an individual's gait, heart or respiratory rate, typing patterns, or mouse movements (all BBCs) adapt to different contexts provides information about a target's emotional state, cognition, and mobility. Once a biometric base is established, the delta can be analyzed. Knowing, for instance, that a player in a video game tends to embrace certain strategies and hierarchical structures can be used as a tool to identify and recruit individuals into violent movements. Oppositional thinkers can be presented with counterarguments to sway their thinking, while individuals demonstrating a high degree of rationality may be more responsive to a structure emphasizing a hypothesis, example, evidence, anticipation of objections, and response—or an approach that emphasizes the opposite position's fallacious thinking.

A third party, moreover, can deliberately deliver a certain input, triggering the subject's response. There may thus be an element of premeditation in that the subject is essentially prompted, or stimulated, and the response is observed and/or recorded and analyzed to generate deeper insight into the target's personhood. Used in this way, biometrics enable a form of human testing: the third party can hypothesize how the individual, group, or community will react (based in part on biometric data), with the response then observed, collected, and analyzed.

If a high technology company, for instance, were to use eye tracking technology to register the varying levels of attentiveness of individuals present in a room with a television, and then play an advertisement on each individual's personal device that correlates with demonstrated search interests of those present, pupil dilation picked up by the television camera or other visual sensors could reveal the level of interest in the items (or ideas, beliefs, people, groups, or political candidates) presented. The same would be true of models used to display clothes, or contextual imagery, for instance, displaying sports clothing in relation to weightlifting versus a social outing. By measuring the consumer's biometric response, the third party can ascertain how successfully they captured the individual's attention, as well as the target's emotional state and predilections. Subsequent purchase of an item, a contribution to a non-governmental organization, or an email sent to a friend noting support for a particular candidate would merely confirm it further. The same approach could be used for any number of aims: convincing individuals to eschew or approve of abortion, to convert to a particular religion, to enroll at a university, to join the flat earth society, or to try to overthrow the government. The mechanism and role of biometrics in the process is similar.

68. *See infra* Section II.B.2.

Testing can also be applied to mental or emotional states. Predictive analytics can provide an assessment of whether certain olfactory stimuli, for instance, may help to alleviate depression or inculcate sadness. Others may evaluate levels of fear when presented with certain images. Yet more may emphasize auditory reception, taste, or texture, measuring the target's response. The strength of an individual's grip on a mobile device following the delivery of news feeds, or the receipt of certain phone calls or texts, can generate more information. It is the combination of predictive analytics and subsequent testing that allows for measurement and modification to the predictive model. Biometrics provides the key.

In the third category, biometrics may serve as a corollary device. It can anchor a range of data to a particular individual, group, or entity. It may tie the type of information gleaned from the first two mechanisms already discussed to the target, or it could be completely different information, such as the fact that an individual stops in front of a particular window, meets certain people, dresses a certain way, drinks alcohol, laughs at a comedian's jokes, or cries at the end of a movie. Biometrics here allows third parties to associate other information with a particular person.

This role is the latest in the evolution of biometrics writ large. Traditionally, biometrics provided a form of identification. Its function, though, has progressed. It has become a method of authentication, verifying that *X* person has been approved to gain access to certain information, equipment, or physical space.[69] In the early twenty-first century, authentication further expanded to incorporate access to services, such as payment systems or shopper identification for loyalty programs and access to discounts.

Most recently, biometrics have become a way of anchoring data: i.e., associating certain information with particular individuals, groups, or communities. In this manifestation, the name, address, and other more standard personally identifying information becomes irrelevant. So does formal enrollment, which in the past has been part of authentication. Instead, all a third party needs to know is that the information being collected relates to *this* human being, i.e., the same person to whom other information pertains. Thus, whenever any new information attaches to the target, the profile deepens, and to the extent that it is digitized, it does so instantaneously, with the result that anyone with access to the data tranche can instantaneously associate it with that particular person (or group or community).

The fourth and final way in which biometric data may enter into biomanipulation is while being used as a means of delivery. It is in some ways the fruition of the first two senses in that not only is the information being used, but it becomes an avenue for delivering stimuli to convince individuals to believe, want, feel, or act in certain ways. Knowing, for instance, that individuals routinely employ abductive versus analogical reasoning or tend to use heuristics (each of which can be gleaned through

69. *See, e.g.*, Biometric Authentication Device, Biometric Authentication Method, & Storage Medium, U.S. Patent No. 8,542,095 B2 (filed Jan. 19, 2009) (issued Sept. 24, 2013) (submitted by NEC Corporation); Sys. for Multiple Algorithm Processing of Biometric Data, U.S. Patent Application No. 17/329,646 (filed May 25, 2021) (applied for by Fusionarc, Inc.).

biometric data) may alter how information is presented to them. A third party can base delivery on how a target is hardwired, such as susceptibility to social pressure (versus logical argument, for instance) to shape them. Packaging what a target's private contacts have said about a candidate may be far more persuasive for the former, whereas a logical argument as to why a person should vote a certain way in light of their ethnic background (which also can be determined from biometric data) may be more convincing to the latter. Outside of prior notification and consent, an individual may have considerably less agency in acquiescing (or rejecting the effort by others to manipulate them) to the extent that the manipulation stems from innate traits. To the extent that biometric responses are unconscious, using them to alter mental, emotional, or physical states, or to cause an individual to take or to refrain from taking certain actions, makes it possible to short circuit—or at least severely cabin—rationality, knowledge, and consent.[70]

While we tend to think about manipulation in terms of getting targets to hold certain beliefs or desires, evince specific emotions, or engage in particular behaviors, biomanipulation also can be used to deny targets access to certain privileges or rights. An insurance company, for example, may determine genetic vulnerabilities from DNA sampling and use this to deny coverage for those diseases or to only offer them at a much higher premium than required of individuals without the genetic predisposition. If this information is made publicly available, a target may be unable to obtain insurance. Their actions, or non-actions in this case, will have been manipulated by the third party with access to the biometric data. Access to jobs or low-interest loans, or any number of other privileges, may be denied.

The same may be true of a target's ability to access a right. Consider, for instance, the right to vote. A third party may determine from biometric data (e.g., dermatoglyphic patterns) that certain individuals have a predisposition to schizophrenia, a mental illness marked by, inter alia, hallucinations, delusions, and impaired cognitive abilities.[71] This insight can then be used to exacerbate the symptoms, generating false beliefs or judgments about reality or stimulating hallucinations to channel the target into other activities.

---

70. *See infra* Section I.C.

71. *See, e.g.*, Oyunchimeg Norovsambuu et al., *Main Characteristics of Dermatoglyphics Associated with Schizophrenia and its Clinical Subtypes*, PLOS ONE, June 10, 2021, at 1, 6 (finding a significant difference in the fingerprints and palm prints between patients with schizophrenia and participants in a control group); Shana Golembo-Smith et al., *The Presentation of Dermatoglyphic Abnormalities in Schizophrenia: A Meta-Analytic Review*, 142 SCHIZOPHRENIA RSCH. 1, 6 (finding some dermatoglyphic differences between those with and without schizophrenia); Fereshteh Shakibaei et al., *Dermatoglyphics in Patients with Schizophrenia*, 16 J. RSCH. MED. SCI. 1055, 1055, 1060 (2011) (concluding that finger ridge count presents a potential new biological marker for those with schizophrenia); Jen-Feng Wang et al., *Determining the Association Between Dermatoglyphics and Schizophrenia by Using Fingerprint Asymmetry Measures*, 22 INT'L J. PATTERN RECOGNITION & A.I. 601, 612–13 (2008) (finding "evidence for an association between unusual dermatoglyphic characteristics and genetic vulnerability to schizophrenia"). *But see* Megan Key Gabalda & Michael T. Compton, *Dermatoglyphic Indices and Minor Physical Anomalies in Patients with Schizophrenia and Related Disorders, Their First-Degree Biological Relatives, and Non Psychiatric Controls*, 178 PSYCHIATRY RSCH. 255, 258 (2010) (finding no significant differences between patients and control groups).

C. BIOMANIPULATION IN THE MARKET CONTEXT

Biomanipulation differs in important respects from how scholars have traditionally thought about consumer, market, and voter manipulation. Even academics primed in behavioral market-futurism have failed fully to appreciate the specific challenge posed by the collection and use of biometric data.[72] While there are many distinctions, two in particular present. First, personalized targeting grounded in human biological characteristics and processes gives third parties greater control over a target. It bypasses rational choice in terms of how the information is generated and collected, as well as how subsequent stimuli are employed. Because of the level of accuracy secured, individuals subject to such manipulation may have a significantly narrower opportunity to believe, want, feel, or act other than as the third party directs. Second, the immutable nature of the data differs from other kinds of consumer or voter manipulation in that it does not arise from any action of the target themselves, but merely because they exist. It also can be extremely difficult to alter, if it can be changed at all. This means that its collection creates a persistent vulnerability, which exists for the lifetime of the target. And it can be exercised by any number of actors, for any number of reasons, until the target's death.

1. Traditional Approaches

Scholars have long wrestled with ways in which consumers or markets can be manipulated. At the turn of the last century, Professor Thorstein Veblen called attention to growing corporate power, which could be leveraged to harm consumers.[73] Professor John Kenneth Galbraith later argued for the need to establish countervailing power to offset corporate strength.[74] And in the late 1950s, controversy over subliminal advertising generated significant attention.[75] Vance Packard famously drew attention to the way "many of us are being influenced and manipulated."[76] He pointed to "large-scale efforts . . . to channel our unthinking habits, our purchasing decisions, and our thought processes by the use of insights gleaned from psychiatry and the social sciences."[77] Professor Franklyn Haiman similarly warned that subliminal cues "attempt to make [a target] buy, vote, or believe in a certain way by short-circuiting his conscious thought processes and planting suggestions or exerting pressures on the periphery of his consciousness which are intended to

72. *See, e.g.*, ZUBOFF, *supra* note 15, at 236 (discussing a smart bed's collection of heart rate, breathing, and movement data, and the sharing of that information as evidence of the minimal effectiveness of privacy policies); *id.* at 283–84, 289 (discussing emotion analytics as a way to increase revenues and as part of future data analytics).

73. *See generally* THORSTEIN VEBLEN, THE THEORY OF BUSINESS ENTERPRISE (1904).

74. *See generally* JOHN KENNETH GALBRAITH, AMERICAN CAPITALISM: THE CONCEPT OF COUNTERVAILING POWER (1952).

75. *See, e.g.*, Franklyn S. Haiman, *Democratic Ethics and the Hidden Persuaders*, 44 Q.J. SPEECH 385, 385 (1958); James V. McConnell, Richard L. Cutler & Elton B. McNeil, *Subliminal Stimulation: An Overview*, 13 AM. PSYCH. 229, 229 (1958); VANCE PACKARD, THE HIDDEN PERSUADERS 3–4 (1957).

76. PACKARD, *supra* note 75, at 3.

77. *Id.*

produce automatic, non-reflective behavior."[78] His chief concern was the extent to which such efforts tapped into "[n]on-critical reflex action," bypassing reason.[79] Subjected to greater scrutiny, however, a number of academics discredited the effectiveness of subliminal advertising, concluding not only that the "threshold" of consciousness varied among potential targets, but that even within the same person a significant level of variation occurred, influenced by their particular needs, emotions, alertness, and interests at any particular point in time.[80]

Tracking the growth of behavioral economics, Professors Christine Jolls, Cass Sunstein, and Richard Thaler focused on consumer behavior, considering how rationality, willpower, and self-interest shape human decisionmaking and challenging the assumption that consumers consistently (and narrowly) act in their own self-interests.[81] In 1998, Jolls, Sunstein, and Thaler posited a behavioral approach to economic analyses of law to ensure "more accurate assumptions about human behavior, and more accurate predictions and prescriptions about law."[82] Arguing that bounded rationality and willpower, as well as self-interest, operate to shape human decisionmaking, they challenged the idea that people act narrowly in their own self-interest.[83] All three concepts, "well documented in the literature of other social sciences," had yet to penetrate law and economics.[84] The mere knowledge that human beings often displayed such behaviors opened the door for commercial entities to use this knowledge to encourage consumers to buy their products.[85]

---

78. Haiman, *supra* note 75, at 385.

79. *Id.*

80. *See* McConnell et al., *supra* note 75, at 232–33, 235; *see also* Timothy E. Moore, *Subliminal Advertising: What You See Is What You Get*, J. MKTG., Spring 1982, at 38, 39 (explaining that thresholds vary within individuals and between subjects); Anthony R. Pratkanis, *The Cargo-Cult Science of Subliminal Persuasion*, 16 SKEPTICAL INQUIRER 260, 265 (1992) (citing studies that concluded the threshold of awareness varied "as a function of individual and situational factors").

81. Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1474, 1478–80 (1998). For classic treatments of coercion (as opposed to manipulation), see generally Robert L. Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470 (1923) (arguing that every market transaction is mutually coercive with the result that there is nothing intrinsically wrong with coercion) and ALAN WERTHEIMER, COERCION (Marshall Cohen ed., 1987) (arguing for a "moralized" definition of coercion as prima facie wrong).

82. Jolls et al., *supra* note 81, at 1474.

83. *See id.* at 1479.

84. *Id.* at 1476. Bounded rationality referred to "the obvious fact that human cognitive abilities are not infinite." *Id.* at 1477 (footnote omitted). The authors explained, "We have limited computational skills and seriously flawed memories," which impact judgment and decisionmaking. *Id.* Bounded willpower, in turn, referred "to the fact that human beings often take actions that they know to be in conflict with their own long-term interests." *Id.* at 1479. Bounded self-interest acknowledged that people "care, or act as if they care, about others, even strangers, in some circumstances." *Id.* This includes wanting others to be treated fairly, "if those others are themselves behaving fairly." *Id.* For prior discussion of bounded rationality in the social science literature, see generally Herbert A. Simon, *A Behavioral Model of Rational Choice*, 69 Q.J. ECON. 99 (1955). For discussion of cognitive biases, see Daniel Kahneman & Amos Tversky, *Subjective Probability: A Judgment of Representativeness*, 3 COGNITIVE PSYCH. 430, 431, 452 (1972) and Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263, 265, 271 (1979).

85. *See* Jolls, *supra* note 81, at 1486.

The following year, Professors Jon Hanson and Douglas Kysar launched their theory of market manipulation, advocating for an approach to consumer behavior that takes on board the internal, dynamic impact of cognitive biases in decision-making.[86] "Once one accepts that individuals systematically behave in nonrational ways," they wrote, "it follows from an economic perspective that others will exploit those tendencies for gain."[87] The scholars recognized that market outcomes could be not just influenced, but even determined, by whoever controlled the format in which information was presented, the framing and presentation of choices, and the setting within which transactions occurred.[88] "[P]owerful economic incentives" would drive manufacturers to focus on "non-rational consumer tendencies" to alter "consumer preferences and perceptions for gain."[89] This was true even in the face of efforts by regulators to adopt bias-specific procedures, such as warnings, to ensure consumers had enough information to make informed choices.[90] Hanson and Kysar explained, "Advertising, promotion, and price setting all become means of altering consumer risk perceptions, regardless of mandated hazard warnings. This is what we mean by manipulation—the utilization of cognitive biases to influence peoples' perceptions and, in turn, behavior."[91] Cognitive biases ought to be treated as endogenous features of the economic model in that not only do they influence individuals' behavior, but that "other factors within the model [influence] the presence and force of cognitive biases."[92]

In 2003, Thaler and Sunstein put a positive spin on consumer manipulation, billing it as "libertarian paternalism" and arguing,

> Once it is understood that some organizational decisions are inevitable, that a form of paternalism cannot be avoided, and that the alternatives to paternalism (such as choosing options to make people sick, obese, or generally worse off) are unattractive, we can abandon the less interesting question of whether to be paternalistic or not and turn to the more constructive question of how to choose among paternalistic options.[93]

---

86. *See* Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 HARV. L. REV. 1420, 1564–65 (1999) [hereinafter Hanson & Kysar, *Some Evidence*]; Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630, 747 (1999) [hereinafter Hanson & Kysar, *The Problem*].

87. Hanson & Kysar, *The Problem*, *supra* note 86, at 635.

88. *See id.* at 635 ("[W]e believe that market outcomes frequently will be heavily influenced, if not determined, by the ability of one actor to control the format of information, the presentation of choices, and, in general, the setting within which market transactions occur."); *see also* Hanson & Kysar, *Some Evidence*, *supra* note 86, at 1451 (explaining that one way in which marketers can influence buyer perception "is through the use of framing effects, which refer to the tendency for information format (as opposed to content) to influence perceptions and behavior"); *id.* at 1424–25 ("[B]ecause individuals exhibit systematic and persistent cognitive processes that depart from axioms of rationality, they are susceptible to manipulation by those actors in a position to influence the decisionmaking context.").

89. Hanson & Kysar, *The Problem*, *supra* note 86, at 630.

90. *Id.* at 636–37.

91. *Id.* at 637.

92. *Id.* at 636.

93. Richard H. Thaler & Cass R. Sunstein, *Libertarian Paternalism*, 93 AM. ECON. REV. 175, 175 (2003).

The best way to accomplish the latter was either to conduct a cost–benefit analysis (to measure the full impact of any design choice) or "seek indirect proxies for welfare" (choosing between three methods of welfare-maximizing approaches).[94] Thaler and Sunstein went on to define such behavior as a "nudge," explained as an intervention that "alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, [an] intervention must be easy and cheap to avoid. Nudges are not mandates."[95]

For Thaler and Sunstein, predictability goes in some sense to the legitimacy of the manipulation, but in the context of biometric data, predictability presents very differently. Basing manipulation on inherent traits significantly increases the likelihood of an anticipated outcome. It may be difficult, if not impossible, for the target to refrain from acting (or not acting) according to the input. That quality is precisely what undermines the target's autonomy and liberty interests. In a digital environment, moreover, with 24/7/60/60 access to a target, it may be nearly impossible to avoid. Professor Lauren Willis presaged this concern, questioning—in response to Thaler and Sunstein—whether "nudging" really described corporate conduct, calling out the "stickiness" of default conditions, paired with corporate agility, as closer to a shove.[96]

In 2014, Professor Ryan Calo moved the ball up the field, examining ways in which technology mediates market interactions, allowing for the collection and analysis of massive amounts of information about consumer behavior.[97] Calo noted that data can be used to identify biases and to manipulate individuals into certain purchase patterns.[98] It thus came as little surprise that Microsoft employed the second-largest number of anthropologists in the United States, after the U.S. government.[99] Following Calo's article, scholars began looking more carefully at targeted online manipulation. Sunstein, for instance, posited that it involved attempting to influence individuals' choices to the extent that such efforts did "not sufficiently engage or appeal to their capacity for reflection and deliberation."[100] Ambiguity found root in "the sufficiency of people's capacity to deliberate on the question at hand."[101]

---

94. *Id*. at 178.

95. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008); *see also* SUNSTEIN, *supra* note 15, at 5–6, 20–21, 57–58, 116 (discussing "nudges" in the context of government).

96. Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155, 1160, 1171, 1227 (2013); *see* Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593, 1658 (2014) (describing further the concept of sticky defaults as creating a façade of choice).

97. Calo, *supra* note 15, at 999.

98. *Id*. at 1010–12.

99. *Id*. at 1009 (citing Graeme Wood, *Anthropology Inc*., ATLANTIC, Mar. 2013, at 48, 51, http://www.theatlantic.com/magazine/archive/2013/03/anthropology-inc/309218/).

100. Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 216 (2015) (emphasis omitted).

101. *Id*. (citing Barnhill, *supra* note 44). Sunstein's approach departed from Anne Barnhill, who posited in 2014 that manipulation has to do with "directly influencing someone's beliefs, desires, or emotions such that she falls short of ideals for belief, desire, or emotion in ways typically not in her self-

The same year that Calo wrote, Professor Ira Rubinstein called out the growing field of politically oriented commercial data brokers assembling political dossiers on voters, allowing for microtargeting.[102] He highlighted their reliance on voter registration databases, donor and survey material, website registration, social media, credit scores, state and national voter files, commercial data, and various other sources, noting, "Most voters are ignorant of the steps taken to create these dossiers and know even less about related targeting practices."[103] Around the same time, Professor Neil Richards suggested "that surveillance transcends the public/private divide," calling out the harm: "Surveillance menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination. . . ."[104]

While these scholars addressed big data generally, they did not grapple with the unique challenge posed by biomanipulation. Susser et al. in 2019 came the closest to addressing the types of issues that arise in their treatment of three behaviors associated with technology: Facebook's emotional sentiment analysis, algorithmically nudged labor, and psychographic profiling and election influence.[105] On the first, while the company denied having done so, a leaked Facebook internal report highlighted how advertisers could take advantage of teens at moments of vulnerability. The report noted, "By monitoring posts, pictures, interactions and internet activity in real-time, Facebook can work out when young people feel 'stressed', 'defeated', 'overwhelmed', 'anxious', nervous', 'stupid', 'silly', 'useless', and a 'failure.'"[106] Using Uber as a model for the second behavior—labor nudging—the scholars pointed to the barrage of "texts, emails, popups, and carefully designed graphics to keep [drivers] behind the wheel and to direct them, ostensibly, to areas of highest demand"; Uber also

interest." Barnhill, *supra* note 44, at 52. In her response to Sunstein, Barnhill observed that while manipulation may sometimes undermine the target's reflection and deliberation, in some circumstances, merely "bad inputs" are sufficient—not every decision requires deliberation. Anne Barnhill, *I'd Like to Teach the World to Think: Commercial Advertising and Manipulation*, 1 J. MKTG. BEHAV. 307, 309 (2015).

102. Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 863, 867 (2014); *see also* Daniel Kreiss, *Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data*, 64 STAN. L. REV. ONLINE 70, 71 (2012) (arguing "the sheer expanse of data now gathered and stored about the electorate and the modeling and targeted communications it supports are qualitatively new," and noting "[t]he core of these databases are public data collected from local, state, and federal records, which include information such as party registration, voting history, political donations, vehicle registration, and real estate records. This data is supplemented with commercial information such as magazine subscription records, credit histories, and even grocery 'club-card' purchases").

103. Rubinstein, *supra* note 102, at 867–68, 874, 915.

104. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935–36 (2013) (emphasis omitted); *see also* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 266–67 (2013) (responding to Professor Richards by explaining that focus must also be given to *how* information is being gathered, not just *what* information is being gathered).

105. Susser et al., *supra* note 15, at 2, 6–7, 13, 28.

106. *Id.* at 6 (quoting Darren Davidson, *Facebook Targets 'Insecure' Young People to Sell Ads*, AUSTRALIAN (May 1, 2017), https://theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6 (analyzing internal Facebook report)).

sends push notifications towards the end of shifts to encourage drivers to keep making money.[107] Cambridge Analytica, Exhibit A for the third behavior—psychographic profiling—famously generated user profiles based on a personality quiz administered by a lecturer in the Department of Psychology at the University of Cambridge, while simultaneously appropriating test takers' social networks.[108] Michal Kosinski, a potential inspiration for the Cambridge lecturer administering the quiz, demonstrated that "from Facebook 'likes' alone," a target's "gender, sexual orientation, race, religion, political views, relationship status, substance use [and abuse]" could be ascertained.[109] His research suggested a correlation between "like" patterns, personality profiles (OCEAN), and psychological traits (e.g., intelligence).[110]

By grouping sentiment analysis, labor nudging, and psychographic profiling together, the authors essentially put dark patterns, "likes," and psychological testing on par with each other, missing a critical distinction among mechanisms (like biometric data) which can be employed to similar ends. The extent to which a target has actual agency wildly differs depending on the source and nature of the information used to exploit target vulnerabilities.

2. Biologically Based Personalization

The personalized nature of biomanipulation matters, and its grounding in a target's innate characteristics and biological processes sets it apart from the type of data generally considered in the context of consumer and market manipulation. The information entailed makes it highly effective, allowing third parties to bypass or channel a target's ordinary thought processes in a way that may leave targets with little choice but to acquiesce. A greater liberty interest presents than typically operates in the context of market, or even voter, manipulation.

There is a world of difference between broad efforts to try to convince individuals to act or to see the world in a certain way and using individualized biometric processes to do so. If I were to pick up a book, for instance, and the author were to write persuasively about the looming threats posed by biometrics, I would be perfectly aware that the individual is trying to persuade me of the seriousness of the implications of new and emerging technologies. Assumedly, that is why I decided to access that information: because I wanted to increase my knowledge or challenge my ideas (or perhaps merely occupy myself until supper). The extent to which biological processes underlie my subsequent analysis matters naught:

---

107. *Id.* at 8.

108. *Id.* at 10.

109. *Id.* (citing Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCIS. 5802 (2013)).

110. *Id.* Although the Big Five (or OCEAN) personality traits appear with some frequency, they are not without controversy as either measurable across situations or as a meaningful way to organize personality. *See, e.g.*, Daniel Cervone, *Explanatory Models of Personality: Social-Cognitive Theories and the Knowledge-and-Appraisal Model of Personality Architecture*, *in* 1 THE SAGE HANDBOOK OF PERSONALITY THEORY AND ASSESSMENT 80, 95 (Gregory J. Boyle et al. eds., 2008). There are numerous other tests, however, which offer other ways to get at the same information.

the book itself was not delivered based on the collection of my biometric data, nor did it short-circuit my ability to reflect on the material by tapping into my (unique) brainprint and identifying my cranial processes. So, too, with contemporary advertising: merely the fact that I have bought books and downloaded scholarly articles from JSTOR on the subjects of manipulation, coercion, and exploitation may be sufficient for an advertisement to pop up in my email, suggesting that I read Jane Austen's *Persuasion* (or watch the 2022 adaptation on Netflix) or get up to speed on Simon Sinek's thoughts on manipulation as a way to influence behavior in *Start with Why*.[111] Each would rely on the digital data trail I have created by my actions, indicating a possible interest in the subject matter.

In contrast, say during a video call, a smartphone engages in eye tracking, enabling the phone company to ascertain that the speaker is neurodivergent. It then may begin feeding information about social anxiety into the speaker's news feed, alongside advertisements for sudoku (on the grounds that people on the spectrum often focus on details and patterns).[112] In this case, the material that has been delivered draws from the company's knowledge of how the speaker's brain works. The action is deeply personalized, and the deliberative process cabined by pre-selecting variables that comport with how the speaker processes information. In the hands of a political campaign, the same information could be used to prevent citizens from showing up to vote: articles detailing the voluminous nature of crowds outside polling places or highlighting the chaos inside them could dissuade the target. It is not merely bypassing stages of deliberation where manipulation occurs but changing the breadth of deliberation *based on biometric processes*.

In a chapter entitled "Fifty Shades of Manipulation," Sunstein distinguishes between efforts to influence people's behavior and manipulation.[113] He offers as the defining feature of the latter the extent to which such behavior sufficiently engages or appeals to a target's capacity for reflection and deliberation.[114] He underscores the role the inherent concept of fairness plays in this construction: the issue is that targets have not "had a fair chance to make a decision on their own."[115]

Sunstein is right that there is a world of difference between information fairly or neutrally presented and the effort to mask such actions to shape how others act.

---

111. *See generally* SIMON SINEK, START WITH WHY: HOW GREAT LEADERS INSPIRE EVERYONE TO TAKE ACTION (2009) (discussing manipulation as a tactic employed by leaders in advertising, politics, and business).

112. *See Apple Announces New Accessibility Features, Including Eye Tracking, Music Haptics, and Vocal Shortcuts*, APPLE NEWSROOM (May 15, 2024), https://www.apple.com/newsroom/2024/05/apple-announces-new-accessibility-features-including-eye-tracking/ [https://perma.cc/A4UE-CS2J]; Shuo Wang et al., *Atypical Visual Saliency in Autism Spectrum Disorder Quantified Through Model-Based Eye Tracking*, 88 NEURON 604, 604–05 (2015); Beth P. Johnson et al., *Ocular Motor Disturbances in Autism Spectrum Disorders: Systematic Review and Comprehensive Meta-Analysis*, 69 NEUROSCIENCE & BIOBEHAVIORAL REVS. 260, 269 (2016) (finding evidence of differences in saccade dysmetria in individuals with ASD). For a discussion of the range of information that can be obtained via eye tracking, see *infra* Section II.A.2.

113. SUNSTEIN, *supra* note 15, at 78–115.

114. *Id.* at 82.

115. *Id.* at 83 (emphasis omitted).

In the context of biomanipulation, however, the concern extends beyond fair presentation. It is not just that an individual has not had (adequate) opportunity to reflect on the information at the point of delivery, but that a person at some level may be inherently *unfree* to do so in two respects.

First, to the extent that the input or stimulus taps into PBCs or BBCs (especially those about which the target is ignorant), the individual may not even be aware that such manipulation is occurring.[116] The delivery of contextualized persuasion has long been a standard feature of advertising: a commercial depicting a man in his mid-forties driving a Lexus with a beautiful woman sitting next to him as the car hugs the curves of a mountain road shapes the imagination of a certain subset of possible customers, regardless of whether the audience is knowingly aware of how it taps into their subconscious. But to the extent that such portrayals play on broad and well-known stereotypes, which may or may not appeal to some percentage of the population, they are different in kind to the sort of individualized messaging that is possible with the collection of biometric data and subsequent delivery of stimuli.

Knowing from pupillometry, for instance, that a target is homosexual, cisgender, has acrophobia, and prefers opera to jazz may completely change the format the commercial takes. Suddenly, two men dressed in tuxedos may be in the vehicle speeding along flat city streets, expertly pulling up in front of a theater announcing the opening night of *La Traviata*. In the second case, not only is the information highly personalized, but there may be no way of knowing that the manipulator obtained insight via eye tracking or that they are using that information to shape decisionmaking. There is a world of difference between images or ideas finding fertile ground, whether they be political candidates giving a speech or a religious leader inveighing a community to love their neighbors, and harvesting an individual's biological information to gain insight into who they are, how they think, and what they are likely to do to manipulate them into believing, wanting, feeling, or acting a certain way.

Admittedly, some of this information may also be obtainable via patterns in consumer behavior: magazine purchases, Spotify playlists, clothing choices, and other preferences could be obtained from data aggregators yielding insight into sexual identity, sexual orientation, and musical preferences. Such information could be employed via 24/7/60/60 online access to consumers. However, a key distinction is that in the latter case, information relies on consumer behavior. Biometrics does not. It can be gleaned simply by the nature of an individual *existing*. That is, the target does not need to *do* anything for the collector to gain such

116. One possible objection might be merely to note that all the third party did was use the target's data to figure out what articles were most likely to interest the target and then forward the appropriate links. The target still has the option of deciding whether or not to click on them and to read the text. Beyond this, the individual is still free to form their own opinion about the material. By way of response, what is concerning about this behavior is not whether an individual would or would not have found the material on their own, but the extent to which the company is using how the subject is hardwired to manipulate them into acting and doing so in a surreptitious manner.

insight. Instead, information can be collected without their knowledge or consent. There is no necessary step the individual takes that could rationally be said to reveal such information to anyone. There is no inference from other decisions the individual has made. Nor may the target be aware that they are being manipulated based on this data.

Second, even if aware that such efforts are occurring, the target's hardwiring may lead to diminished capacity to withstand the manipulation. This gives rise to distinct questions about voluntariness related to each of the ways in which manipulation works: namely, how voluntarily is the individual (a) coming to the belief, (b) adopting the desire, (c) assuming the emotion, or (d) engaging (or not) in the subsequent action? There are operative differences among these with respect to biomanipulation, as opposed to manipulation writ large.

Regarding (a), the extent to which the stimulus interacts with previously held beliefs, the analytical process employed by an individual to reach a belief, the level of assuredness in truth conveyed or received, and other factors may come into account. In the case of typical consumer or voter manipulation, beliefs may be ascertained from external behaviors: geolocational data may show whether a target attends a church, mosque, or synagogue—or not. But it will not reveal precisely *why* the individual is there. Is it habit? Social pressure? Guilt? Or what one might call true belief? Biometric data *can* give an answer to these questions, making it far more invasive and increasing the likelihood that the prompting can be specifically tailored in a way more likely to broker the desired mindset—whether it be bolstering, redirecting, or undermining belief.

For (b), desire, and (c), emotion, to the extent that the stimuli employ an individual's hardwiring, there may be significantly less time for such intervening qualities to come into play. Knowing, for instance, that an individual is attracted to a particular actor or is quick to anger when confronted by images of animals being harmed may be enough to quickly shift their desire to see the latest movie or to become incensed when confronted by certain images. Intervening information or events might prevent acting on the desires or emotions, but the immediate shaping has occurred. The level of intrusion and reliability of effect can differ significantly from aggregating consumer behavior and even personally identifiable information. It can provide relative weighting. Biometrics, for instance, can reveal *which* of different stimuli causes the greatest fear, joy, or anger, and in what contexts, allowing the manipulator to fine-tune the target's response to get them to reach the desired goal. In part this is possible through persistent monitoring, allowing for a feedback device. As the next Part notes, biomanipulation provides for a feedback mechanism over time. It can record a base state and then a target's response, resulting in a form of human experimentation into the inner life of the subject.

For (d), actions, access to an individual's hardwiring may generate a firm grasp of the target's social, emotional, or cognitive processes, in contrast to ordinary consumer manipulation, which is built on past behavior. This places the manipulator in a better position to predict how an individual will act, allowing them to impose their

will on that of the target. In each of these manifestations, what is at stake is the degree of autonomy enjoyed by the target, as well as their liberty in relation to being subject to another's will. It can be wielded to any number of effects which extend well beyond the concerns that present in the market or voter context.

3. Immutability and Persistent Vulnerability

The immutable nature of biometric markers also sets them apart from ordinary consumer, market, and voter behavior modification. It can be very difficult, if not impossible, to alter an individual's biometric data. PBCs, after all, are simply innate characteristics. Retinal patterns and vascular systems do not change. Outside of surgery, face geometry remains consistent, with algorithms able to adjust to age (both forward and backward).[117] Even if finger, palm, or earprints can be surgically altered, the new print then becomes the biometric marker, with an equally high barrier to future changes. Thus, while it might be possible to bypass some markers (e.g., using special contacts to thwart iris detection or employing a limp to bypass gait recognition), others, like vascular networks, blood flows associated with cognitive processing, pupil dilation, and DNA, are more permanent. This makes them rather more reliable than other forms of information, both as a means of gleaning insight and as a way of using biology for stimuli to find fertile ground.

That data, in turn, can be used for any number of purposes, not just the reason for which it is initially collected. One of the features of many of the BBC systems that has largely escaped notice is that they are multi-use. Retinal imaging or scanning, for instance, can be employed for physicians and psychologists to diagnose and treat diseases.[118] The attendant emotional and physiological data though allows for broader application. The same system can be directed to "market, sociological, political, and psychological studies."[119] As conveyed in one patent, "[e]valuating images of the retina and other parts of the eye can reveal excitement, sadness, other emotional responses, non-emotional responses such as pain, and physiological responses."[120] The "person or processor controlling the stimuli could receive reports of reactions in real time and adjust stimuli to select content for a subject or group based on reactions to the previous content."[121] *Pari passu*, the system could be employed to recommend content and select advertisements. The document explains:

> [S]ome embodiments could go even further through continual monitoring via retinal imaging and evaluation. The data could be used to determine whether a

117. *See* Nagesh Kumar M. & M.N. Shanmukha Swamy, An Efficient Multimodal Biometric Face Recognition Using Speech Signal, *in* INT'L CONF. ON SIGNAL & IMAGE PROCESSING 201, 201 (IEEE, 2010), https://ieeexplore.ieee.org/abstract/document/5697469.

118. *See* A.I. &/or Virtual Reality for Activity Optimization/Personalization, U.S. Patent Application No. 17/395,177, para. [0006].

119. *Id.* para. [0219].

120. *Id.*

121. *Id.*

> user wants to skip the intro of his favorite show, estimate how much content the user wants to have suggested, and estimate when ads can be shown for maximum attention or for minimum annoyance by tracking the user's reaction as he sees ads at different times. It would also . . . watch[] his reaction as he sees the ads. For example, if he gets excited often by trucks, then he would see more trucks, and which trucks excited him would be tracked to allow more targeted advertising. Recording such reactions could also be used for advertising via other media including phone, email, or traditional mail.[122]

The patent centers on using stimuli and immediately ascertaining the target's response. It states,

> For example, if the user finds it funny instead of thrilling, that information may help understand what users want. Understanding whether the user is laughing, on the edge of his seat, or fascinated can help sort through which Reaction Triggers are driving his reaction as well if several happen at about the same time. Additionally, preexisting Like Factors can be consulted in generating like factors.[123]

The system contemplates continuous or intermittent retinal imaging to collect the target's reaction to content.[124] It combines this information with data from other devices. Where there is a delta between them, the system can be adjusted for delivery of more information in the future.[125]

This example reaches a related distinguishing characteristic: the vulnerability created by initial collection persists for the target's lifetime. That is, it is not just their freedom at the moment that is compromised. They become vulnerable to being subject to the will of another for as long as they live, without regard to any specific ends. From employment and education, to housing, politics, rebellion, and even war, that individual becomes susceptible to direction from others. Biomanipulation is thus related to, but a distinct form of, manipulation.

II. ENABLING FACTORS

The rapid expansion in the range and depth of biometric information available has paved the way for biomanipulation. PBCs and BBCs now extend well beyond the traditional categories of finger/handprinting, FRT, and voiceprints. Associated data reveals: vulnerabilities as well as processes ripe for exploitation. Biometric systems increasingly draw from multimodal sources and often pair the data with demographic, financial records, email content and traffic, location data, and other information, creating deeper insights into the target's past and likely future behaviors. Collection from afar, in turn, which I refer to as "remote access," provides for continual monitoring, as well as collection from multiple people simultaneously, which I understand as "environmental monitoring."

122. *Id*. para. [0222].
123. *Id*. para. [0224].
124. *Id*.
125. *See id*. para. [0025].

Finally, advances in algorithmic sciences, the advent of big data analytics, and the growth of AI and machine learning (ML) now allow for predictive analytics.[126] Systems increasingly incorporate feedback loops, allowing users to refine their processes to achieve their desired goals. The approach mimics a form of human subject experimentation, targeting individuals based on their innate biological properties and habitual practices.

A. BIOMETRIC TAXONOMIES

The recent commercial and scholarly emphasis on biometrics means that new and varied types of information can be obtained. There are no comprehensive taxonomies, however, which lay out the range of PBCs and BBCs available. This Section addresses the gap, noting in the process that the PBCs and BBCs that can be collected convey information beyond the features in question. Yet more information can be inferred based on the collection of such information in relation to space and time. The unique nature of the data, as aforementioned, transforms the act of identification to a way to enable correlation. It can convey intimate details about an individual. That BBCs are biometrically determined, moreover, makes the target vulnerable to exploitation through the very mechanisms used to gain insight in the first place.

1. Physiological Biometric Characteristics (PBCs)

Physiological biometric characteristics (PBCs) include images, measurements, or calculations derived from, and correlated with, an individual's innate traits.[127] Although relatively stable, they may be damaged, altered, degraded, or destroyed through age, repetitive actions, sickness, accident, or medical procedures.[128] Nevertheless, their status persists: once altered, the new image, calculation, or measurement (or absence thereof) forms a new PBC. In the contemporary legal literature, the PBCs that have garnered the most attention include finger/hand/

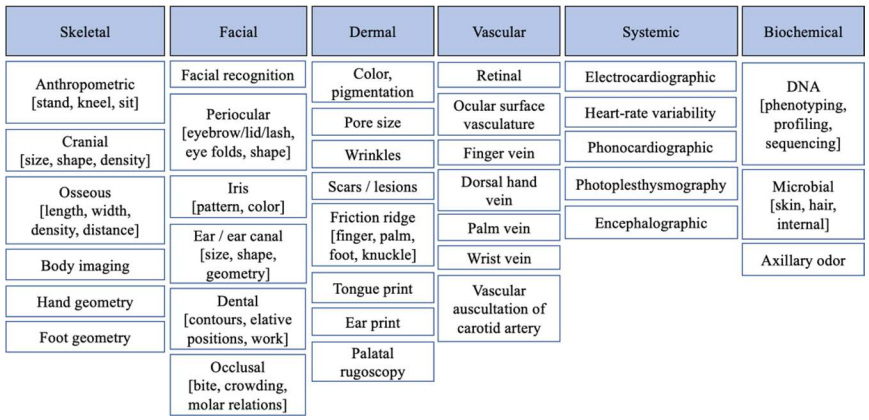
126. *See* STANFORD U., GATHERING STRENGTH, GATHERING STORMS: THE ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE (AI100) 2021 STUDY PANEL REPORT 12 (2021), https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/AI100Report_MT_10.pdf [https://perma.cc/BMR9-228U] ("In the last five years, the field of AI has made major progress in almost all its standard sub-areas, including vision, speech recognition and generation, natural language processing (understanding and generation), image and video generation, multi-agent systems, planning, decision-making, and integration of vision and motor control for robotics. . . . The core technology behind most of the most visible advances is *machine learning*, especially deep learning (including generative adversarial networks or GANs) and reinforcement learning powered by large-scale data and computing resources."); S. C. Olhede & P. J. Wolfe, *The Growing Ubiquity of Algorithms in Society: Implications, Impacts, and Innovations*, PHIL. TRANSACTIONS ROYAL SOC'Y A: MATH, PHYSICAL & ENG'G SCIS., Sept. 13, 2018, at 1, 2 ("The large-scale availability of data, coupled with rapid technological advances in algorithms, is changing society markedly."). Innumerable scientific articles similarly emphasize the impact algorithms and deep learning have had on discrete biometric subfields. *See, e.g.*, Luiz A. Zanlorensi et al., *A New Periocular Dataset Collected by Mobile Devices in Unconstrained Scenarios*, SCI. REPS., 2022, at 1, 1; Cides S. Bezerra et al., Robust Iris Segmentation Based on Fully Convolutional Networks and Generative Adversarial Networks, *in* 31st SIBGRAPI CONF. ON GRAPHICS, PATTERNS & IMAGES 281, 282 (SIBGRAPI 2018), https://arxiv.org/abs/1809.00769.

127. *See Physiological and Behavioural Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/physiological-and-behavioural-biometrics/ [https://perma.cc/G8TN-LWCR] (last visited Dec. 31, 2024).

128. *Id.*

footprints, iris analytics, and FRT.[129] For each, the framing almost always considers such markers in relation to identification. This narrow emphasis, however, misses the many other reasons for which data may be gathered and the ways in which it can be used, as well as the myriad traits which populate the PBC category and aid in target exploitation.[130] For purposes of this Article—and to illustrate the breadth of information that can be obtained, I divide PBCs into six trait categories: skeletal, facial, dermal, vascular, systemic, and biochemical.[131] Each can be partitioned by the different types of data which can be obtained.

Figure 2. Physiological Biometric Characteristics



129. *See generally, e.g.*, SELFIE BIOMETRICS: ADVANCES AND CHALLENGES (Ajita Rattani et al. eds., 2019) (focusing almost exclusively on FRT and iris recognition); ANIL K. JAIN, ARUN A. ROSS & KARTHIK NANDAKUMAR, INTRODUCTION TO BIOMETRICS (2011) (textbook with three chapters on fingerprint, face, and iris recognition, and only one covering "additional biometric traits").

130. In 2021, the European Border and Coast Guard Agency (Frontex) undertook a study of *Biometric Technologies and Biometrics-Enabled Technological Systems*, as well as *Patentometric and Bibliometric Analyses of Biometric Technologies*. While the initiative contains some interesting information, it employs automated analysis focused on EU research funding, EU patents, and European research. Its primary emphasis, moreover, was on border identification, not biometric technologies across the board. Even then, it excluded border surveillance and emotion and behavior detection. The model it offers thus falls significantly short of what is needed to grasp the current context of biometric collection in the United States. *See* FRONTEX, *supra* note 31, at 13; FRONTEX: EUR. BORDER & COAST GUARD AGENCY, TECHNOLOGY FORESIGHT ON BIOMETRICS FOR THE FUTURE OF TRAVEL, ANNEX III: PATENTOMETRIC AND BIBLIOMETRIC ANALYSES OF BIOMETRIC TECHNOLOGIES 22–23 (2021) [https://perma.cc/Z4J3-AYWU].

131. *See infra* fig. 2. I have developed this chart based on broad reading of primary source documents. Although I have tried to be as comprehensive as possible, there may be additional PBCs which I have simply missed.

The first category, skeletal data, emphasizes measurement, proportions, and characteristics of the corporal form. It includes anthropometric traits, such as height (standing, kneeling, or sitting). Cranial measurements convey the size, shape, and density of the skull. The category includes osseous matter, such as the length, width, and density of bones (in isolation or together) and the distance between parts of the body (e.g., fingertip-to-fingertip, or "wingspan"). A newer addition is the full body scan.[132] It also incorporates hand and foot geometry, which use markers like shape, texture, pressure distribution, and ridge characteristics.[133]

The second category, PBCs associated with the face and head, incorporates FRT, which uses mathematical patterns to verify face pairing. Facial landmark detection isolates structural points (e.g., forehead, eyes, nose, lips, cheeks, and chin), measuring size and distance between each point. FRT can be applied to frontal or side profiles to extract data from still images, video sequences, or multiple feeds, as well as three-dimensional information.[134] While FRT previously relied on images, which partial facial covering (i.e., masks, hair, or glasses) could obscure, more recently

132. *See, e.g.*, Elec. Devices with Body Composition Analysis Circuitry, U.S. Patent Application No. 17/865,194, at [57] (filed July 14, 2022) (describing an electronic device using image sensors to capture body composition and a deep learning model which takes account of facial expressions and different body poses in a patent application created by Apple).

133. *See, e.g.*, Alberto de-Santos-Sierra et al., *Unconstrained and Contactless Hand Geometry Biometrics*, 11 SENSORS 10143, 10143, 10145 (2011). While much of the research in the early twenty-first century focused on contact-based systems, by 2007 the emphasis had shifted to contactless platforms. *Compare, e.g.*, Anil K. Jain & Nicolae Duta, Deformable Matching of Hand Shapes for User Verification, *in* PROC. 1999 INT'L CONF. ON IMAGE PROCESSING 857, 859 (IEEE, 1999), https://ieeexplore.ieee.org/document/823019 (utilizing images "acquired by a hand scanner"), *and* Raul Sanchez-Reillo et al., *Biometric Identification Through Hand Geometry Measurements*, 22 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACH. INTEL. 1168, 1168 (2000), https://ieeexplore.ieee.org/document/879796 (extracting "[h]and features" from a photograph taken on a platform), *with* Xiaoqian Jiang et al., New Directions in Contact Free Hand Recognition, *in* IEEE INT'L CONF. ON IMAGE PROCESSING 389, 389 (IEEE, 2007), https://ieeexplore.ieee.org/document/4379174 ("[C]omputing hand geometry measurements from frontal views of freely posed hands."), *and* Gholamreza Amayeh et al., Improving Hand-Based Verification Through Online Finger Template Update Based on Fused Confidences, *in* IEEE 3RD INT'L CONF. ON BIOMETRICS: THEORY, APPLICATIONS, & SYS. 1, 1 (IEEE, 2009), https://ieeexplore.ieee.org/document/5339044 (using freestanding photographs of hands); Andreas Uhl & Peter Wild, Personal Identification Using Eigenfeet, Ballprint and Foot Geometry Biometrics, *in* FIRST IEEE INT'L CONF. ON BIOMETRICS: THEORY, APPLICATIONS, & SYS. 1, 1 (IEEE, 2007), https://ieeexplore.ieee.org/document/4401924 (identifying persons using shape, texture, ballprint, and foot width); Kazuki Nakajima et al., *Footprint-Based Personal Recognition*, 47 IEEE TRANSACTIONS ON BIOMEDICAL ENG'G 1534, 1534 (2000) (measuring pressure distribution of footprint); Jin-Woo Jung et al., Unconstrained Person Recognition Method Using Dynamic Partial Footprints from Floor-Type Pressure Sensor, *in* PROC. 18TH HUNGARIAN-KOREAN SEMINAR 85, 85 (2002) (recognizing persons using static foot shape); Jin-Woo Jung et al., *Dynamic Footprint-Based Person Recognition Method Using a Hidden Markov Model and a Neural Network*, 19 INT'L J. INTELLIGENT SYS. 1127, 1127 (2004) (suggesting a new person-recognition scheme based on center of pressure trajectory in dynamic footprints).

134. *See generally What Is Facial Recognition?*, AWS: CLOUD COMPUTING CONCEPTS HUB, https://aws.amazon.com/what-is/facial-recognition/ [https://perma.cc/KDA8-DPC5] (last visited Dec. 31, 2024). Over the past fifteen years, there has been a significant increase in the number of FRT patents filed. Apple, for instance, which filed only seven such patents from 2000–2009, filed eighty-three FRT patents from 2010–2020. *See Apple Facial Recognition Patents*, INSIGHTS BY GREYB (Sept. 23, 2024), https://insights.greyb.com/apple-facial-recognition-patents/ [https://perma.cc/38NC-KKK7].

companies have turned to new technologies like heat mapping, with the advantage that more consistent measurements can be obtained.[135] Periocular recognition (PR), another type of facial biometric, focuses more narrowly on the area around the eye, such as the eyebrows, eyelids, eyelashes, and eye folds.[136] It includes the sclera (i.e., the white outer layer of the eyeball) and the shape of the eye.[137] PR has an advantage over full facial recognition in that age, emotions and expressions, partial face coverings, and facial hair affect accuracy less in PR than in FRT.[138] Although still in its infancy, the advantages it has over FRT (as well as iris recognition, which requires both closer access and high resolution images),[139] make it likely to quickly gain ground.[140] Numerous other facial features exhibit unique characteristics. In the late twentieth century, as aforementioned, iris identification techniques became more advanced, allowing for identity to be established based on color and patterns.[141] Ear and ear canal size, shape, and geometry also can be associated with individuals.[142] Dental biometrics focuses on the contours of the teeth, relative positions of teeth, and work which has been carried out, such as fillings, bridges, implants, and extractions.[143] Occlusal analyses look at the interior and posterior bite, abrasion, crowding of the teeth, and molar relations.[144]

The third category focuses on variations in the skin. Color and pigmentation provide one of the oldest and most common biometric markers.[145] They can be supplemented by pore size, wrinkles, and the presence of scars or lesions.[146] Fingerprinting is perhaps the most well-known PBC. Friction ridge analyses related to the finger, palm, or foot reach back hundreds of years.[147] It was not until 1963, however, that the first scientific paper on automated fingerprint matching

135. *See* Occlusion Detection for Facial Recognition Processes, U.S. Patent Application No. 15/934,559 paras. [0004–05] (filed Mar. 23, 2018).

136. Renu Sharma & Arun Ross, *Periocular Biometrics and Its Relevance to Partially Masked Faces: A Survey*, COMPUT. VISION & IMAGE UNDERSTANDING, 2023, at 1, 1; *see also* Zanlorensi et al., *supra* note 126, at 1.

137. *See* Sharma & Ross, *supra* note 136, at 1.

138. FRONTEX, *supra* note 130, at 135.

139. Daugman, *supra* note 6, at 329.

140. FRONTEX, *supra* note 130, at 164–65.

141. Daugman, *supra* note 6, at 326, 329.

142. *See* Mazumdar & Nirmala, *supra* note 11, at 711; Auden P. Balouch et al., *Measurements of Ear-Canal Geometry from High-Resolution CT Scans of Human Adult Ears*, HEARING RSCH., 2023, at 1, 1.

143. *See* Hong Chen & Anil K. Jain, *Dental Biometrics: Alignment and Matching of Dental Radiographs*, 27 IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACH. INTEL. 1319, 1319 (2005); Vijayakumari Pushparaj et al., *An Effective Dental Shape Extraction Algorithm Using Contour Information and Matching by Mahalanobis Distance*, 26 J. DIGIT. IMAGING 259, 260 (2013).

144. *See generally* Philip L. Millstein & Carlos E. Sabrosa, *Occlusal Contact Prints; A Biometric Means for Identification*, J. ADVANCED FORENSIC SCIS. 2022, at 1 (comparing dental prints and occlusal analysis with fingerprinting as a form of biometric identification).

145. *See* HANDBOOK OF BIOMETRICS 211 (Anil K. Jain et al. eds., 2008).

146. *See id.* at 347, 449.

147. *See* Jeffrey G. Barnes, *History*, *in* THE FINGERPRINT SOURCEBOOK 5, 9 (Alan McRoberts ed., 2011); FRANCIS GALTON, FINGER PRINTS 1–2 (1892).

surfaced.[148] Since then, automated print matching has become standard.[149] Inner- and dorsal-knuckle print recognition, a relative newcomer to the scene, is also employed in identification systems.[150] Advances in high resolution photography and duplication methods, however, made it easier to bypass controls and decreased the power of fingerprinting as a means of authentication.[151] Like hands and feet, the color, shape, and surface features of the tongue (relatively stable in light of protection offered by the oral cavity) similarly evince a distinct pattern.[152] Ear prints, two-dimensional reproductions of the outer ear, contain specific and unique anatomical markers, which similarly can be used to identify individuals.[153] In addition, palatal rugae—irregular, asymmetric ridges which mark the top of the mouth—are unique to each person.[154]

The fourth category relates to the vascular system, which represents a fairly recent evolution in biometrics. The first scientific papers on its use began appearing at the end of the twentieth and early twenty-first century, at which time Fujitsu Lab, Advanced Biometrics, Inc., and others began working on circulatory system identification.[155] Vascular patterns, which are also unique, demonstrate a remarkable degree of stability over an individual's life, and the information can be obtained remotely.[156] Associated systems focus on different areas of the

148. *See* Mitchell Trauring, *Automatic Comparison of Finger-Ridge Patterns*, 197 NATURE 938, 938 (1963) (stating as the purpose of the article to put forward "a method by which decentralized automatic identity verification, such as might be desired for credit, banking or security purposes, can be accomplished through automatic comparison of the minutiae in finger-ridge patterns").

149. *See, e.g.*, HANDBOOK OF BIOMETRICS, *supra* note 145, at 474, 478; Shriram D. Raut & Vikas T. Humbe, *Biometric Palm Prints Feature Matching for Person Identification*, 11 INT'L J. MOD. EDUC. & COMPUT. SCI. 61, 61 (2012).

150. *See* Gaurav Jaswal et al., *Knuckle Print Biometrics and Fusion Schemes – Overview, Challenges, and Solutions*, ACM COMPUTING SURVS., Nov. 2016, at 1, 7; Christian Holz et al., Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts, *in* CHI '15: PROC. OF THE 33RD ANN. ACM CONF. ON HUM. FACTORS IN COMPUTING SYS. 3011, 3012 (Ass'n for Computing Mach., 2015), https://dl.acm.org/doi/10.1145/2702123.2702518 (identifying dorsal knuckle imaging as a component of bodyprinting).

151. *See, e.g.*, Alex Hern, *Hacker Fakes German Minister's Fingerprints Using Photos of Her Hands*, GUARDIAN (Dec. 30, 2014, 6:43 AM), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands [https://perma.cc/HTE8-GNBK].

152. *See* T. Radhika et al., *Tongue Prints: A Novel Biometric and Potential Forensic Tool*, 8 J. FORENSIC DENTAL SCIS. 117, 118 (2016).

153. *See Ear Print Analysis*, ENCYCLOPEDIA.COM, https://www.encyclopedia.com/science/encyclopedias-almanacs-transcripts-and-maps/ear-print-analysis [https://perma.cc/ZL5K-VKCU] (last visited Dec. 31, 2024). Ear prints differ from 3D imaging of the ear in that the former are limited to skin patterns and anatomical markers. *See id.*

154. *See* Aparna Paliwal et al., *Palatal Rugoscopy: Establishing Identity*, 2 J. FORENSIC DENTAL SCIS. 27, 27 (2010); Inês Morais Caldas et al., *Establishing Identity Using Chieloscopy and Palatoscopy*, 165 FORENSIC SCI. INT'L 1, 2 (2007); William R. English et al., *Individuality of Human Palatal Rugae*, 33 J. FORENSIC SCIS. 718, 722 (1988); *see also* Jun Ai Chong et al., *Morphological Patterns of the Palatal Rugae: A Review*, 62 J. ORAL BIOSCIENCES 249, 249–51 (2020) (finding seventy-three articles in PubMed and ScienceDirect databases focusing on the stability of palatal rugae).

155. *See, e.g.*, Sang-Kyun Im et al., *An Biometric Identification System by Extracting Hand Vein Patterns*, 38 J. KOREAN PHYSICAL SOC'Y 268, 268 (2001); Takashi Shinzaki, *Use Case of Palm Vein Authentication*, *in* HANDBOOK OF VASCULAR BIOMETRICS 145, 146 (Andreas Uhl et al. eds., 2020).

156. *See* Shinzaki, *supra* note 155, at 146–47.

body.[157] Retinal vasculature, for instance, resides behind the eye.[158] Unlike some (non-vascular) PBCs, such as fingerprints or iris recognition—which can be circumvented through use of artificial fingers or contact lenses—retinal blood vessel patterns cannot be forged.[159] Ocular surface vasculature (blood vessel patterns on the white of the eye in the conjunctival and episcleral layers) and texture provide another unique marker.[160] It has the advantage over iris recognition in that the eye gaze does not have to be directed at the device for information to be obtained; and while iris patterns are more easily obtained in the near infrared spectrum, vasculature patterns can be captured in the visible spectrum.[161] Finger vein recognition employs near-infrared light to detect blood vessel patterns visible from the surface of the skin.[162] Along with dorsal (on the backside of the hand) and palm vein recognition, targets must be both real and alive.[163] These vein patterns are remarkably stable: outside of youth (ages 0–15 years), the pattern remains unchanged unless serious accident or medical intervention occurs.[164] Wrist vasculature, marked by the same level of stability, has the advantage of wider veins, making it easier to identify associated patterns.[165] Some vascular systems extend beyond mere patterns to include auditory information. Recently, for instance, research has emerged on how to employ the blood flow sounds in the carotid artery for biometric identification.[166]

The fifth area focuses on metabolic and cardiovascular systems.[167] The Electrocardiogram (ECG) is more than a diagnostic tool.[168] It captures patterns

157. *See* Andreas Uhl, *State of the Art in Vascular Biometrics*, *in* HANDBOOK OF VASCULAR BIOMETRICS, *supra* note 155, at 3, 3.

158. *See* Mazumdar & Nirmala, *supra* note 11, at 711.

159. *See id.*

160. *See* Simona Crihalmeanu & Arun Ross, *Multispectral Scleral Patterns for Ocular Biometric Recognition*, 33 PATTERN RECOGNITION LETTERS 1860, 1860 (2012); Sriram Pavan Tankasala et al., *Ocular Surface Vasculature Recognition Using Curvelet Transform*, 6 INST. ENG'G. & TECH. 97, 97 (2017).

161. Crihalmeanu & Ross, *supra* note 160, at 1861.

162. *See* Borui Hou et al., *Finger-Vein Biometric Recognition: A Review*, IEEE TRANSACTIONS ON INSTRUMENTATION & MEASUREMENT, 2022, at 1, 1.

163. *See id.* at 22; Waheed Ali Laghari et al., *Dorsal Hand Vein Pattern Recognition: A Comparison Between Manual and Automatic Segmentation Methods*, 29 HEALTHCARE INFORMATICS RSCH. 152, 153 (2023).

164. *See* M. Rajalakshmi et al., *Palm-Dorsal Vein Pattern Authentication Using Convoluted Neural Network (CNN)*, 116 INT'L J. PURE & APPLIED MATHEMATICS 525, 525–26 (2017); Rajendra Kumar et al., Dorsal Hand Vein-Biometric Recognition Using Convolution Neural Network, *in* INT'L CONF. ON INNOVATIVE COMPUTING & COMMC'NS 1087, 1087 (Springer, 2021), https://link.springer.com/chapter/10.1007/978-981-15-5113-0_92 ("[N]o such study is available to ensure whether the vein patterns of kids are changed with age from infants to 15 years of age. . . .").

165. *See* Raul Garcia-Martin & Raul Sanchez-Reillo, *Wrist Vascular Biometric Recognition Using a Portable Contactless System*, 20 SENSORS 1469, 1469 (2020).

166. *See, e.g.*, Rutuja Salvi et al., *Vascular Auscultation of Carotid Artery: Towards Biometric Identification and Verification of Individuals*, 21 SENSORS 6656, 6658, 6667 (2021).

167. When variance in response to stimuli or altered contextual conditions is involved, systemic measurements would be considered BBCs, as discussed below.

168. *See* Priatna Ahmad Budiman et al., *Study for Integration of Multi Modal Biometric Personal Identification Using Heart Rate Variability (HRV) Parameter*, J. PHYSICS: CONF. SERIES, 2019, at 1, 1; Maryamsadat Hejazi et al., Non-Fiducial Based ECG Biometric Authentication Using One-Class

unique to an individual. Phonocardiograms, high-fidelity recordings of heart murmurs and other sounds resulting from the opening and closing of the heart valves and alterations in blood flow and pressure, similarly correlate to particular persons.[169] Photoplethysmography (PPG) employs illumination-based sensors, which pick up volumetric changes as blood courses around the body.[170] Sensors with light-emitting diodes and photodiodes attached to the fingertip or earlobe can collect heart rate and heart rate variability.[171] Although less information can be obtained through this system than through ECGs (their electromagnetic counterparts), PPG-based systems can be used to provide authentication, regardless of the emotional state of the subject.[172] Researchers claim up to a 99.95% recognition rate using this approach.[173] EEG signals, which show the functional connectivity among parts of the brain, similarly provide information unique to individuals, as there is a significant amount of variability among brain structures and basic and high cognitive functions.[174] EEGs can be used to provide a picture of an individual's basal state, illuminating essentially how the brain is connected.[175] While some data may be collected in response to certain sensory stimulation (and thus be considered within the BBC designation, below), other information can be gleaned from spontaneous signals continuously produced by the brain in a resting state.[176]

The sixth and final category has to do with biochemical markers, encompassing biomolecular, genetic, hormonal, and chemical traits. DNA phenotyping is an emerging technique for predicting an individual's externally visible characteristics (e.g., hair and skin color), ancestry, and age.[177] DNA sequencing, in turn, allows for identification based on short tandem repeat sequences in the nuclear or

---

Support Vector Machine, *in* SIGNAL PROCESSING: ALGORITHMS, ARCHITECTURES, ARRANGEMENTS, & APPLICATIONS 190, 190 (IEEE, 2017), https://ieeexplore.ieee.org/document/8166862.

169. *See*, *e.g.*, Abuagla Babiker et al., *Heart Sounds Biometric System*, J. BIOMEDICAL ENG'G. & MED. DEVICES, 2017, at 1, 1–2; Nazneen Akhter et al., *Heart-Based Biometrics and Possible Use of Heart Rate Variability in Biometric Recognition Systems*, *in* 1 ADVANCED COMPUTING AND SYSTEMS FOR SECURITY 15, 16 (Rituparna Chaki et al. eds., 2016).

170. *See* Abhijit Sarkar et al., Biometric Authentication Using Photoplethysmography Signals, *in* 2016 IEEE 8TH INT'L CONF. ON BIOMETRICS THEORY, APPLICATIONS & SYS. 1, 1 (IEEE, 2016), https://ieeexplore.ieee.org/document/7791193.

171. *See id.*; Junfeng Yang et al., *Photoplethysmography Biometric Recognition Model Based on Sparse Softmax Vector and* k*-Nearest Neighbor*, J. ELEC. & COMPUT. ENG'G., Oct. 2020, at 1, 1.

172. *See* Sarkar et al., *supra* note 170, at 1.

173. Yang et al., *supra* note 171, at 8.

174. *See*, *e.g.*, Min Wang et al., *BrainPrint: EEG Biometric Identification Based on Analyzing Brain Connectivity Graphs*, PATTERN RECOGNITION, Sept. 2020, at 1, 8; Ryota Kanai & Geraint Rees, *The Structural Basis of Inter-Individual Differences in Human Behaviour and Cognition*, 12 NATURE REVS.: NEUROSCIENCE 231, 231 (2011); Yu Zhang et al., *Strength and Similarity Guided Group-Level Brain Functional Network Construction for MCI Diagnosis*, 88 PATTERN RECOGNITION 421, 429 (2019); Sophia Mueller et al., *Individual Variability in Functional Connectivity Architecture of the Human Brain*, 77 NEURON 586, 586 (2013).

175. *See* Wang et al., *supra* note 174, at 1–2.

176. *See id.* at 2; Maria V. Ruiz-Blondet et al., *CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification*, 11 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 1618, 1619 (2016).

177. *See* Aurora Canales Serrano, *Forensic DNA Phenotyping: A Promising Tool to Aid Forensic Investigation. Current Situation*, 46 SPANISH J. LEGAL MED. 183, 184 (2020); Peter M. Schneider et al.,

mitochondrial DNA, which vary from person to person.[178] Bodily fluids, skin, and live hair follicles all contain DNA from which samples can be drawn.[179] Over the past fifteen years, research into the human microbiome (i.e., microbial communities which live on and inside the body) has revealed significant diversity of skin- and gut-associated bacterial communities, as well as a high degree of variability among individuals.[180] The findings prompted scholars to examine whether such variation might reflect unique microbial fingerprints—with the result that a new branch of biometric identification is now emerging.[181] Skin-associated bacteria can be readily obtained; they are left on keyboards, door handles, mobile devices, or anything an individual touches, where they remain for up to two weeks at room temperature.[182] Microbial biometrics surpasses certain aspects of DNA: while the latter, for instance, requires that a live follicle of hair be obtained, the former can be used on any strand of hair.[183] Advances in sensor technologies have made it possible to use molecular signatures to undertake rapid human identification.[184] Odor sensing provides yet another approach. While an individual's scent, to some degree, can change due to factors like emotional state, menstrual cycle, or medication, individuals retain their own signature.[185] Enzymes in microorganisms of the axillary microbiome, for instance, combined with genetic considerations can impact body odor.[186] Unique biochemical markers obtained from sweat, saliva, and urine can be extracted, revealing further biochemical information about the subject.[187] Distinctions in the scents produced by hands alone are sufficient to distinguish among individuals.[188]

The Use of Forensic DNA Phenotyping in Predicting Appearance and Biogeographic Ancestry, 116 DEUTSCHES ÄRZTEBLATT INT'L 873, 873 (2019).

178. *See* Schneider et al., *supra* note 177, at 873; S. Panneerchelvam & M.N. Norazmi, *Forensic DNA Profiling and Database*, 10 MALAYSIAN J. MED. SCIS. 20, 20–23 (2003).

179. *Id.* Although at first DNA biometric collection operated in the context of forensic sciences, its reliability, paired with the speed of verification and advances in big data and algorithmic sciences, has catapulted it to the public sphere. *See* Corinna Schindler, *With DNA Comes a New Level of Security*, BIOMETRIC UPDATE.COM (July 4, 2023, 4:33 PM), https://www.biometricupdate.com/202307/with-dna-comes-a-new-level-of-security [https://perma.cc/8VRT-DC26].

180. Noah Fierer et al., *Forensic Identification Using Skin Bacterial Communities*, 107 PROC. NAT'L ACAD. SCIS. 6477, 6479 (2010); Eric A. Franzosa et al., *Identifying Personal Microbiomes Using Metagenomic Codes*, 112 PROC. NAT'L ACAD. SCIS. E2930, E2930 (2015).

181. *See* Franzosa et al., *supra* note 180, at E2936.

182. Fierer et al., *supra* note 180, at 6477–78; Simon Lax et al., *Forensic Analysis of the Microbiome of Phones and Shoes*, MICROBIOME, 2015, at 1, 1.

183. *See* Silvana R Tridico et al., *Metagenomic Analyses of Bacteria on Human Hairs: A Qualitative Assessment for Applications in Forensic Science*, INVESTIGATIVE GENETICS, 2014, at 1, 2.

184. *See* Anirban Sengupta et al., *Robust Security of Hardware Accelerators Using Protein Molecular Biometric Signature and Facial Biometric Encryption Key*, 31 IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYS. 826, 835 (2023).

185. *See* Dustin J. Penn et al., *Individual and Gender Fingerprints in Human Body Odour*, 4 J. ROYAL SOC'Y INTERFACE 331, 331–32, 335 (2006).

186. *See* Andreas Natsch & Roger Emter, *The Specific Biochemistry of Human Axilla Odour Formation Viewed in an Evolutionary Context*, PHIL. TRANSACTIONS ROYAL SOC'Y. B, June 8, 2020, at 1, 1, 9 (2020).

187. Penn et al., *supra* note 185, at 332.

188. *See* Irene Rodriguez-Lujan et al., *Analysis of Pattern Recognition and Dimensionality Reduction Techniques for Odor Biometrics*, 52 KNOWLEDGE-BASED SYS. 279, 280, 288 (2013).

Each sub-category of PBCs (skeletal, facial, dermal, vascular, systemic, and biochemical) has witnessed a sudden expansion in the number and range of associated patents.[189] Part of the reason has to do with prior perceived weaknesses: the viability of using biometrics requires that the disparity between two people be greater than the variation obtained from an individual. Some traditional markers prove problematic. FRT may fail in the face of simple emotion: laughter or anguish may alter expressions and measurement of the distance between facial features. The face may be obscured by glasses or masks, just as beards or mustaches may alter contours. Different people, moreover, may have common features, making it difficult to distinguish them. For identical twins, even DNA may fail to accurately identify the target some percent of the time.[190] Advances in science and technology have filled the gap.

2. Behavioral Biometric Characteristics (BBCs)

In 1953, B. F. Skinner, in his work *Science and Human Behavior*, posited that despite the complexity of human nature, it may be possible to use science to understand the causes of human behavior.[191] He nevertheless questioned explanations grounded in "[t]he proportions of the body, the shape of the head, the color of the eyes, skin, or hair, the marks on the palms of the hands, and the features of the face," to which others had ascribed predictive qualities.[192] "Valid relations between behavior and body type must, of course, be taken into account in a science of behavior," he wrote, "but these should not be confused with the relations invoked in the uncritical practice of the layman."[193] No more so could "information about . . . chemical and electrical processes in the nervous system" be "necessarily inferential or fictional."[194] Correlation was not the same as causation. He sought, instead, "a science of the nervous system based upon direct observation rather than inference," an inquiry which would drive scientists to "events outside the nervous system and, eventually, outside the organism."[195] Behavioral biometrics has since walked the path laid out by Skinner.

---

189. *See, e.g.*, Image Based Detection of Fit for a Head Mounted Wearable Computing Device, U.S. Patent Application No. 17/444,963, at [57], paras. [0032], [0046–47] (filed Aug. 12, 2021) (skeletal, cranial); Sys. & Methods of Detecting & Responding to a Visitor to a Smart Home Env't, U.S. Patent No. 10,664,688 B2, at [57] (filed Nov. 10, 2017) (issued May 26, 2020) (facial); Liveness Detection in an Interactive Video Session, U.S. Patent Application No. 17/136,053, at [57] (filed Dec. 29, 2020) (dermal, wrinkles); Adjusting Security in Response to Alert Communications, U.S. Patent No. 10,165,401 B2 col. 15 ll. 65–67 (filed Oct. 19, 2017) (issued Dec. 25, 2018) (retinal); Sys. & Method for Multi-Node PPG on Wearable Devices, U.S. Patent Application No. 18/025,585, at [57] (filed Oct. 20, 2020) (systemic, heart rate variability); Info. Processing Apparatus, Suspect Info. Generation Method & Program, U.S. Patent Application No. 16/079,796, at [57] (filed Feb. 24, 2017) (DNA matching).

190. This is part of why iris recognition gained ground so quickly, as algorithmic analyses of the unique patterns demonstrated near perfect identification. *See* Daugman, *supra* note 6, at 326, 328–29, 333.

191. B. F. SKINNER, SCIENCE AND HUMAN BEHAVIOR 14–15, 23 (1953).

192. *Id.* at 25.

193. *Id.*

194. *Id.* at 28.

195. *Id.*

BBCs, which I define as probabilistic calculations based on actions, habits, or proclivities grounded in human biology and repeated over time, appeared as early as World War II.[196] In the 1960s, Gunnar Fant and Kenneth Stevens began tying biology to speech patterns—a model developed by Joseph Perkell into a tool of biometric identification.[197] For decades, however, the sheer volume of information and complex analysis required limited what could be done. But big data analytics, advanced algorithmic sciences, and AI/ML altered the landscape, making it possible to assemble massive amounts of information and break it down into patterns. Further enabled by the growth of PBCs, BBCs are becoming increasingly prevalent.[198] While some can be shaped by conscious behaviors—such as working out, practicing, or taking medication—to the extent that they are habitual and reactive, they can be remarkably stable over time. Variation is offset by the probability that an individual will act within certain parameters derived from past behavior in similar contexts or in response to similar stimuli. Models can be altered and refined. To help illustrate the breadth of information that can be collected, I divide BBCs into six trait categories: locomotor, mental or emotional states, systemic data, and task-, strategy-, and preference-based systems. The latter two closely relate to an individual's logic and decisionmaking. All six can be used to anticipate a person's predilections. While some overlap exists, their central emphases differ.[199]

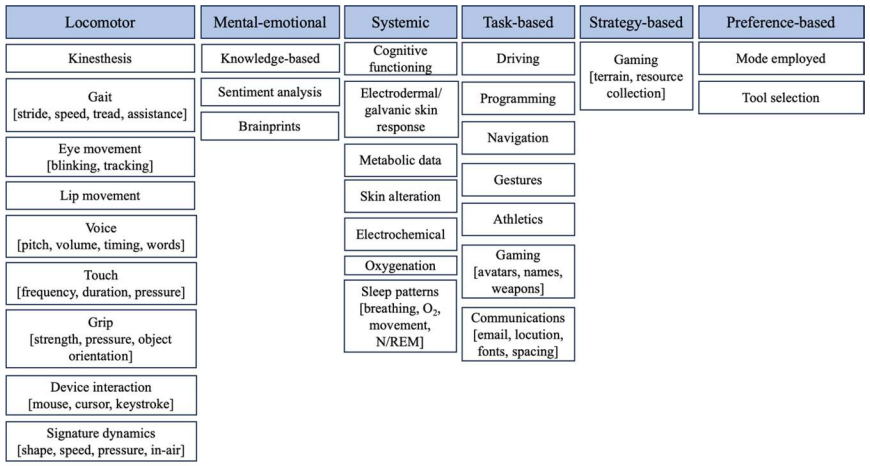
196. The military's "Fist of the Sender" strategy identified Morse code operators based upon each person's unique rhythms, enabling the Allies to track troops and vehicles with whom the operators travelled. *See* David Guy Brizan et al., *Utilizing Linguistically Enhanced Keystroke Dynamics to Predict Typist Cognition and Demographics*, 82 INT'L J. HUM.-COMPUT. STUD. 57, 57 (2015).

197. *See* G. Fant & K. N. Stevens, *Systems for Speech Compression*, 5 FORTSCHRITTE DER HOCHFREQUENZTECHNIK 229, 230 (1960); Joseph Shaile Perkell, A Physiologically-Oriented Model of Tongue Activity in Speech Production 2 (Sept. 1974) (Ph.D. dissertation, Massachusetts Institute of Technology), https://dspace.mit.edu/handle/1721.1/29190 [https://perma.cc/SLB3-AVVS]; Joseph S. Perkell, Models, Theory and Data in Speech Production, *in* PROC. OF THE 12TH INT'L CONG. OF PHONETIC SCIS. 182, 182, 189 (1991).

198. The market for BBCs is rapidly growing: as of 2022, the global market was valued at $1.45 billion. With a compound annual growth rate of 27.3%, by 2027, it is expected to reach $4.62 billion. GRAND VIEW RSCH., *Behavioral Biometrics Market Size & Trends*, https://www.grandviewresearch.com/industry-analysis/behavioral-biometrics-market [https://perma.cc/XRZ2-V62N] (last visited Jan. 1, 2025).

199. *See infra* fig. 3.

Figure 3. Behavioral Biometric Characteristics



The first category focuses on muscle-controlled patterns exhibited by a subject when placed into a known context. Grounded in muscle memory and the nervous system, they tend to be unconscious and thus have a high degree of consistency and stability over time. They present in the three-dimensional world and online, with the result being that data can be gleaned in a range of contexts, from the local grocery store to the gaming world. In the former, cameras or non-visual sensors may be employed. In the latter, VR headsets, multidirectional platforms, and haptic gear make collection and analysis possible. Multiple types of biometrics reside in the locomotor category.

Kinesthesis constitutes the first.[200] On- and off-line, physical movements like walking, grabbing, rotating, and dropping can be decomposed into unique patterns.[201] Using machine learning and other forms of BBCs, such as eye movement, researchers have obtained up to 98.6% accuracy using kinesthesis for biometric identification.[202] Gait biometrics, a specialized form of kinesthesis, looks at characteristics such as the upper-body posture, stride length, speed of travel, the direction and weight of tread, and interaction with mobility assistance devices such as a cane.[203] Neural networks employed to extract features and

200. *See* Ilesanmi Olade et al., *BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems*, 20 SENSORS 2944, 2944 (2020); *see also* Marco Santello et al., *Patterns of Hand Motion During Grasping and the Influence of Sensory Guidance*, 22 J. NEUROSCIENCE 1426, 1426, 1434 (2002) (finding that vision of the object during the reaching moment has no influence on kinematics and that the effect of the physical presence manifests upon contact).

201. *See, e.g.*, Olade et al., *supra* note 200, at 2944, 2950.

202. *Id.* at 2958.

203. *See, e.g.*, Jonathan L. Geisheimer et al., A Continuous-Wave (CW) Radar for Gait Analysis, *in* CONF. RECORD OF 35TH ASILOMAR CONF. ON SIGNALS, SYS. & COMPUTS. 834, 834 (IEEE, 2001), https://ieeexplore.ieee.org/document/987041; Moeness G. Amin et al., *Human Gait Recognition with Cane*

identify the target can reach up to 90% accuracy based solely on stepping patterns (i.e., dynamic footprints).[204] Like many of the BBCs considered in this Article, hardware already built into mobile devices can be used to obtain relevant information. Accelerometers, global positioning systems (GPS), and compass sensors, for instance, can reveal location, speed, and direction. Gyroscopes, which enable users to rotate the screen on a mobile device, can be used to convey the device's relative position for other purposes as well—such as when the phone moves up and down as the user walks, jogs, runs, or skips along.[205] That information can then be used to build a gait signature, identifying who is in possession of the device.

Other locomotor BBCs focus on eye movements.[206] Such systems capture a range of parameters, such as fixation, saccades (rapid eye movement between two points), and smooth pursuit eye movements (which follow moving targets).[207] In addition to motion data, such as the duration, amplitude, velocity, and sequencing of eye movement, eye trackers may monitor blinking, microtremors, and pupil size and reactivity.[208] Common capture is through video (via head-mounted units like VR headsets or smart glasses) or cameras in laptops or mobile devices.[209] Gaze

Assistive Device Using Quadratic Time-Frequency Distributions, 9 IET RADAR, SONAR & NAVIGATION 1224, 1224 (2015); Bruhtesfa E. Godana, Human Movement Characterization in Indoor Environment Using GNU Radio Based Radar 5 (June 19, 2009) (M.Sc. thesis, Delft University of Technology) (on file with Delft University of Technology), https://repository.tudelft.nl/record/uuid:414e1868-dd00-4113-9989-4c213f1f7094 [https://perma.cc/36CC-777K]; *Types of Biometrics – Gait*, BIOMETRICS INST., https://www.biometricsinstitute.org/types-of-biometrics-gait/ [https://perma.cc/UT7D-QZ9A] (last visited Jan. 1, 2025); User Identification & Acct. Access Using Gait Analysis, U.S. Patent No. 10, 929,829 B1, at [57] (filed May 4, 2017) (issued Feb. 23, 2021).

204. *See* Jaeseok Yun et al., Biometric User Identification with Dynamic Footprint, *in* SECOND INT'L CONF. ON BIO-INSPIRED COMPUTING: THEORIES & APPLICATIONS 225, 229 (IEEE, 2007), https://ieeexplore.ieee.org/document/4806456.

205. *See*, *e.g.*, Andrew H. Johnston & Gary M. Weiss, Smartwatch-Based Biometric Gait Recognition, *in* 7TH INT'L CONF. ON BIOMETRICS THEORY, APPLICATIONS & SYS. (BTAS) 1, 1 (IEEE, 2015) https://ieeexplore.ieee.org/document/7358794.

206. *See, e.g.*, Paweł Kasprowski & Józef Ober, Eye Movements in Biometrics, *in* BIOMETRIC AUTHENTICATION: ECCV 2004 INT'L WORKSHOP, BIOAW, PRAGUE, CZECH REPUBLIC, PROC. 248, 248 (Davide Maltoni & Anil K. Jain eds., Springer, 2004), https://link.springer.com/chapter/10.1007/978-3-540-25976-3_23.

207. Mélodie Vidal et al., *Wearable Eye Tracking for Mental Health Monitoring*, 35 COMPUT. COMMC'NS 1306, 1306–07 (2012).

208. Maria K. Eckstein et al., *Beyond Eye Gaze: What Else Can Eyetracking Reveal About Cognition and Cognitive Development?*, 25 DEVELOPMENTAL COGNITIVE NEUROSCIENCE 69, 79, 84, 87 (2017). They also might collect PBCs like the color or texture of the iris or the size or shape of the eye. *See* Brendan John et al., EyeVEIL: Degrading Iris Authentication in Eye Tracking Headsets, *in* ETRA '19: PROC. OF THE 11TH ACM SYMP. ON EYE TRACKING RSCH. & APPLICATIONS 1, 1–2 (Ass'n for Computing Mach., 2019), https://dl.acm.org/doi/10.1145/3314111.3319816.

209. *See Eye Tracking Virtual Reality*, IMOTIONS, https://imotions.com/products/imotions-lab/modules/eye-tracking-virtual-reality [https://perma.cc/93J6-F6PL] (last visited Jan. 1, 2025) (detailing a VR headset incorporating eye tracking technologies); Yixuan Li et al., Towards Measuring and Inferring User Interest from Gaze, *in* PROC. OF THE 26TH INT'L CONF. ON WORLD WIDE WEB COMPANION 525, 525–26 (Ass'n for Computing Mach., 2017), https://dl.acm.org/doi/10.1145/3041021.3054182 (obtaining eye tracking data from front-facing cameras embedded in mobile devices); Kyle Krafka et al., Eye Tracking for Everyone, *in* IEEE CONF. ON COMPUT. VISION & PATTERN RECOGNITION 2176, 2176 (IEEE, 2016), https://ieeexplore.ieee.org/document/7780608 (finding the cameras installed in mobile phones and tablets, without any additional sensors or devices, sufficient for comprehensive eye

fixations can be aggregated into heat maps which reveal particular areas of interest. Eye tracking technologies have started to appear in everything from gaming and military operations to automobiles, healthcare, and marketing.[210] Lip-based biometric authentication (LBBA) focuses on an individual's lip qualities and movements while speaking.[211] The hardware required (i.e., a camera or video capabilities) is commonly already installed in computing and mobile devices.[212] LBBA has the edge over voice recognition systems by being able to operate in noisy environments while still capturing the substance of what is being uttered.[213] Voice biometrics, in turn, relates to pitch, tone, and timing, as well as the selection of particular words or clauses.[214] While a speaker's anatomy and physiology provide a basic structure, where people were born, where they live, and their social groups influence how they convey meaning.[215] Touch (frequency, duration, pressure, and micromovements) and grip (strength, pressure distribution, and object orientation) tend to be relatively constant as well as distinct among individuals.[216] By using motion sensors (already integrated into most smartphones), touch biometrics can be continuously monitored, with a 99% accuracy rate in identifying the individual using the device.[217] For grip, algorithms can be applied to how an individual holds an object, which turns out to be both relatively distinct and stable over time.[218]

---

tracking); Adjusting Video Rendering Rate of Virtual Reality Content & Processing of a Stereoscopic Image, U.S. Patent Application No. 16/298,441, at [57] (filed Mar. 11, 2019) (monitoring blinking via VR goggles).

210. The U.S. eye tracking market is expected to explode; estimates put the compound annual growth rate at 30.7% per year from 2022–2030. *See Eye Tracking Market Size, Share & Trends Analysis Report by Type (Optical, Eye Attached Tracking), by Application (Healthcare, Consumer Electronics), by Component (Hardware, Software), by Location, and Segment Forecasts, 2022 - 2030*, GRAND VIEW RSCH., https://www.grandviewresearch.com/industry-analysis/eye-tracking-market (last visited Jan. 1, 2025).

211. *See* Brando Koch & Ratko Grbić, *One-Shot Lip-Based Biometric Authentication: Extending Behavioral Features with Authentication Phrase Information*, IMAGE & VISION COMPUTING, 2024, at 1, 1; Carrie Wright & Darryl William Stewart, *Understanding Visual Lip-Based Biometric Authentication for Mobile Devices*, EURASIP J. ON INFO. SEC., 2020, at 1, 1.

212. Wright & Stewart, *supra* note 211, at 1, 5.

213. Petar S. Aleksic, *Lip Movement Recognition*, *in* ENCYCLOPEDIA OF BIOMETRICS 904, 905 (Stan Z. Li & Anil K. Jain eds., 2009).

214. *See* HANDBOOK OF BIOMETRICS, *supra* note 145, at 153–54.

215. *See generally* Peter French et al., The Vocal Tract as a Biometric: Output Measures, Interrelationships, and Efficacy, *in* 18TH INT'L CONG. OF PHONETIC SCIS. (Int'l Phonetic Ass'n, 2015), https://www.internationalphoneticassociation.org/icphs/icphs2015. Since 2019, neural networks have catapulted voice biometrics forward, with myriad products now integrating some form of vocal recognition and authentication systems. For a review of the sudden advances in the field from 2019–2022, see M. K. & Aithal, *supra* note 11, at 202.

216. *See* Cheng Bo et al., *SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics*, ARXIV, 2013, at 1, 1.

217. Cheng Bo et al., Continuous User Identification via Touch and Movement Behavioral Biometrics, *in* IEEE 33RD INT'L PERFORMANCE COMPUTING & COMMC'NS CONF. 1, 1 (IEEE, 2014), https://ieeexplore.ieee.org/document/7017067.

218. *See, e.g.*, Raymond Veldhuis et al., Biometric Verification Based on Grip-Pattern Recognition, *in* PROC. VOL. 5306, SEC., STEGANOGRAPHY & WATERMARKING OF MULTIMEDIA CONTENTS VI, at 1,

Some skill-based biometrics in the first category relate to real-time, continual interaction with devices, such as computer mice, cursor movement, and keystroke dynamics.[219] Despite the relatively compact surface area of a mouse, for instance, the odds of an individual placing their fingers in the same spot and exerting the same amount of pressure are small.[220] Unique to each person, mouse manipulation (and keystroke dynamics) can also be used to identify an individual's emotional state, ranging from happiness and sadness to fear and disgust.[221] Text messaging, which employs typing and swiping, generates insight into not just who is using a device but also whether they are happy, sad, stressed, or relaxed.[222] Signature dynamics, in turn, are based on the shape and speed of signing, pen pressure, and pen-in-air movements.[223]

The second trait category focuses on mental–emotional behavioral characteristics. Human knowledge biometrics emphasize what people understand about the world more generally by employing dynamic and semi-static knowledge.[224] The

---

6–7 (SPIE, 2004), https://doi.org/10.1117/12.530967 (finding that grip patterns "contain[] sufficient information that can be used for verification"); Vrajeshri Patel et al., *Hand Grasping Synergies as Biometrics*, FRONTIERS IN BIOENGINEERING & BIOTECHNOLOGY, 2017, at 1, 1 (describing "hand synergies" as a promising biometric). Grip biometrics has been proposed as a means of protecting against unauthorized use of firearms. *See* Veldhuis et al., *supra*, at 1; Virtual Reality/Augmented Reality Handheld Controller Sensing, U.S. Patent Application No. 16/111,702 (filed Aug. 24, 2018) (creating a method employing several sensors to estimate hand position, force, and pressure while individuals hold a handheld device).

219. *See, e.g.*, Fabian Monrose & Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, 16 FUTURE GEN. COMPUT. SYS. 351, 351, 358 (2000) (calculating parameters based on a user's speed, duration of pressure on different keys, changes for certain sequences, and other patterns); Nan Zheng et al., An Efficient User Verification System via Mouse Movements, *in* PROC. OF THE 18TH ACM CONF. ON COMPUT. & COMMC'NS SEC. 139, 139, 149 (Ass'n for Computing Mach., 2011), dl.acm.org/doi/10.1145/2046707.2046725 (identifying cursor and mouse movement as a potential biometric identifier); Keystroke Dynamics Authentication Techs., U.S. Patent No. 8,332,932 B2 (filed Dec. 7, 2007) (issued Dec. 11, 2012) (constructing a method for users to be identified via their keystroke dynamics).

220. *See* Biometric Pressure Grip, U.S. Patent No. 8,762,734 B2 (filed Feb. 10, 2010) (issued June 24, 2014). The current assignee of this patent is Raytheon. *Id.* at [73].

221. *See* Yuqing Qi et al., Emotion Recognition Based on Piezoelectric Keystroke Dynamics and Machine Learning, *in* IEEE INT'L CONF. ON FLEXIBLE & PRINTABLE SENSORS AND SYS. 1, 1–2 (IEEE, 2021), https://ieeexplore.ieee.org/document/9469843; Clayton Epp et al., Identifying Emotional States Using Keystroke Dynamics, *in* PROC. OF THE SIGCHI CONF. ON HUM. FACTORS IN COMPUTING SYS. 715, 715 (Ass'n for Computing Mach., 2011), https://dl.acm.org/doi/10.1145/1978942.1979046; A. Kołakowska, A Review of Emotion Recognition Methods Based on Keystroke Dynamics and Mouse Movements, *in* 6TH INT'L CONF. ON HUM. SYS. INTERACTIONS 548, 548, 553 (IEEE, 2013), https://doi.org/10.1109/HSI.2013.6577879.

222. *See* Surjya Ghosh et al., *Emotion Detection from Touch Interactions During Text Entry on Smartphones*, 130 INT'L J. HUM.-COMPUT. STUD. 47, 48 (2019).

223. *See, e.g.*, Wide-Field Radar-Based Gesture Recognition, U.S. Patent Application No. 16/153,395 para. [0005] (filed Oct. 5, 2018) (in-air movements); Gesture Recognition for Device Input, U.S. Patent No. 9,921,659 B2 col. 5 ll. 3–8, col. 9 ll. 25–29, 38–48, col. 10 ll. 9–22 (filed Aug. 25, 2014) (issued Mar. 20, 2018) (signature dynamics).

224. *See* Taekyoung Kwon & Hyeonjoon Moon, Knowledge-Based User Authentication Associated with Biometrics, *in* INT'L CONF. ON UNIVERSAL ACCESS IN HUM.-COMPUT. INTERACTION 414, 415–16 (Springer-Verlag Berlin Heidelberg, 2007), https://link.springer.com/chapter/10.1007/978-3-540-73279-2_46. Human knowledge biometrics can be distinguished from knowledge-based identification

more specialized the knowledge, particularly in relation to an individual's education, skill base, past history, or thought processes, the more accurately an individual can be identified.[225] Sentiment analysis sources vary from galvanic skin responses, gestures, and posture to facial expressions, vocal traits (such as pitch, volume, or word choice), speed of walking, and pressure.[226] Brainprinting generates a dynamic picture of neural activity, which can be manipulated and subject to biochemical and electromagnetic modulation.[227] Systems map both spontaneous and event-related neural responses.[228] Collection techniques include ultrasounds, X-rays, magnetic fields, radioisotopes, and electrical activity monitoring.[229] Structural approaches identify activity in different anatomic regions, while procedural analyses provide insight into the physiology and metabolism of the regions examined.[230] Brain scans also can be used to ascertain mental and emotional health.[231] The

systems, which employ things like passwords for verification and are dependent on memorization or notation (making a record of the password for later use). *See id.* at 416.

225. *Cf. id.* at 414. CAPTCHAs, although not sufficiently specialized for identification purposes, are built on this concept. *See generally id.* (arguing that CAPTCHAs can help prevent identity theft due to their use of dynamic knowledge not specific to an individual's characteristics).

226. *See, e.g.*, Yekta Said Can et al., *Stress Detection in Daily Life Scenarios Using Smart Phones and Wearable Sensors: A Survey*, J. BIOMEDICAL INFORMATICS, Feb. 2019, at 1, 5 (discussing galvanic skin response in the context of emotional sentiment analysis); Selma Medjden et al., *Adaptive User Interface Design and Analysis Using Emotion Recognition Through Facial Expressions and Body Posture from an RGB-D Sensor*, 15 PLOS ONE, July 16, 2020, at 1, 1 (presenting the design and analysis of an Adaptive User Interface as a way to recognize the emotional state of a user through facial expressions and body posture); Alex S. Cohen et al., *Vocal Acoustic Analysis as a Biometric Indicator of Information Processing: Implications for Neurological and Psychiatric Disorders*, 226 PSYCHIATRY RSCH. 235, 236 (2015) (noting connection of vocal expression to arousal and trying to disaggregate cognitive and emotional/arousal elements); Nitchan Jianwattanapaisarn et al., *Emotional Characteristic Analysis of Human Gait While Real-Time Movie Viewing*, 5 FRONTIERS IN A.I., Oct. 14, 2022, at 1, 1 (examining gait and posture as an alternative to conventional biometrics such as facial features for emotion recognition); Agata Kołakowska et al., *A Review of Emotion Recognition Methods Based on Data Acquired via Smartphone Sensors*, SENSORS, Nov. 2020, at 1, 5 (discussing pressure sensors, accelerometers, gyroscopes, and various other technologies located in smartphones which can be used for sentiment analysis).

227. *See* NAT'L INSTS. HEALTH, BRAIN 2025: A SCIENTIFIC VISION 6 (2014) [https://perma.cc/XF2N-T8LZ]. In 2013, for instance, the National Institutes of Health established the Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative. *See id.* at 5. It sought to demonstrate causality, linking brain activity to behavior with precise interventional tools to change neural circuit dynamics. *Id.* at 83. The Initiative's first report wanted "[t]o enable the immense potential of circuit manipulation" as well as "biochemical and electromagnetic modulation." *Id.* at 6.

228. *See* Gui Xue et al., *Brain Imaging Techniques and Their Applications in Decision-Making Research*, 42 ACTA PSYCHOLOGICA SINICA 120, 120–21 (2010); Tolgay Ergenoglu et al., *Alpha Rhythm of the EEG Modulates Visual Detection Performance in Humans*, 20 COGNITIVE BRAIN RSCH. 376, 376 (2004).

229. Dean F. Wong & James Robert Brašić, *In Vivo Imaging of Neurotransmitter Systems in Neuropsychiatry*, 1 CLINICAL NEUROSCIENCE RSCH. 35, 35–36 (2001); *see also* A. Lenartowicz & R.A. Poldrack, *Brain Imaging*, *in* ENCYCLOPEDIA OF BEHAVIORAL NEUROSCIENCE 187, 187–90 (George F. Koob et al. eds., 2010) (describing additional methods).

230. *See* Lenartowicz & Poldrack, *supra* note 229, at 187; James Robert Brašić & Mona Mohamed, *Human Brain Imaging of Autism Spectrum Disorders*, *in* IMAGING OF THE HUMAN BRAIN IN HEALTH AND DISEASE 373, 376 (Philip Seeman & Bertha Madras eds., 2014).

231. *See, e.g.*, Ginny Smith, *A Scan of Your Brain Could Predict Future Mental Health Problems. Here's How*, BBC SCI. FOCUS (June 13, 2023, 6:20 AM), https://www.sciencefocus.com/the-human-

information obtained through these devices can be used to ascertain everything from cognitive impairment[232] and autism spectrum disorder[233] to whether people are likely to still be hungry after they eat.[234] By pairing neural activities with metabolic shifts, like increased blood flow and oxygen supply to local vasculature, further insight can be gained.[235] Brain patterns can be remarkably consistent across time. One study, for instance, found a 93% accuracy rate while monitoring a subject's delta, theta, alpha, beta, and gamma waves.[236]

The third category, systemic BBCs, focuses on corporal systems. Patterns in cognitive functioning, such as episodic memory, word fluency, attention, and perceptual, cognitive, and motor speed, can be measured using magnetic resonance imaging (MRI).[237] While electroencephalograms (EEGs) can be used to capture an individual's basal state (e.g., their level of arousal or stress), an event-related stimulus can elicit a unique response from different brain systems.[238] Multiple stimuli can achieve a significant degree of accuracy: in one instance, it obtained a 100% accuracy rate (albeit based on a sample of just fifty people).[239] One of the strengths of this approach is that it allows the individual establishing identity to manipulate the cognitive state of the individual by shaping the event and possibly the broader environment within which the target responds.[240] The more unconventional or unusual such stimuli, the more likely the individual's response will be unique.[241] Metabolic data, such as systolic and diastolic blood pressure and

body/brain-fingerprints [https://perma.cc/N9QK-4LHC]; Method & Apparatus for Virtual-Reality-Based Mindfulness Therapy, U.S. Patent No. 11,224,717 B2 col. 5 ll. 53–67, col. 6 ll. 1–24 (filed May 9, 2019) (issued Jan. 18, 2022).

232. *See, e.g.*, Somaiyeh Azmoun et al., *Cognitive Impact of Exposure to Airborne Particles Captured by Brain Imaging*, *in* ADVANCES IN NEUROTOXICOLOGY: OCCUPATIONAL NEUROTOXICOLOGY 29, 30–31 (Roberto G. Lucchini et al. eds., 2022).

233. Maya M. Evans et al., *Developmental Disruptions of the Dorsal Striatum in Autism Spectrum Disorder*, 95 BIOLOGICAL PSYCHIATRY 102, 103 (2024); Cheryl Brandenburg, Commentary, *The Obstacle Is the Way: Unraveling Mysteries in Neural Circuitry Development*, 95 BIOLOGICAL PSYCHIATRY 96, 96 (2024).

234. DC Bittel & MG Butler, *Prader–Willi Syndrome*, REFERENCE MODULE NEUROSCIENCE & BEHAV. PSYCH., 2017, at 1, 10–11.

235. Xue et al., *supra* note 228, at 120–21.

236. *See* Jim Nash, *Brain Wave Biometrics Yield 93% Authentication Rate in Research*, BIOMETRICUPDATE.COM (Oct. 20, 2021, 2:45 PM), https://www.biometricupdate.com/202110/brain-wave-biometrics-yield-93-authentication-rate-in-research [https://perma.cc/2PC9-WWDX] (detailing a study that recorded an accuracy rate of 92.6% using an EEG to measure brain waves); PRIYANKA A. ABHANG ET AL., INTRODUCTION TO EEG- AND SPEECH-BASED EMOTION RECOGNITION 20–21 (2016) (characterizing the five different brain waves recorded via EEG).

237. Hedvig Söderlund et al., *Cerebral Changes on MRI and Cognitive Function: The CASCADE Study*, 27 NEUROBIOLOGY AGING 16, 17–18 (2006); *see* J.S. Anderson et al., *Decreased Left Posterior Insular Activity During Auditory Language in Autism*, 31 AM. J. NEURORADIOLOGY 131, 131 (2010).

238. *See* Ruiz-Blondet et al., *supra* note 176, at 1618–19 (highlighting the primary visual, facial recognition, and gustatory/appetitive brain systems).

239. *Id.* at 1618.

240. *See id.* at 1626.

241. *Id.* at 1619–20. Research, for example, has consistently shown that individuals respond differently to words with which they are familiar compared with ones they do not know. *Id.* at 1620. People, moreover, differ markedly in their vocabularies. *Id.* Food preference is similarly highly subjective, and structures in the midbrain activate differently in response to foods that people prefer. *Id.*

oxygenation, may alter in consistent patterns in response to certain types (and levels) of activity.[242] Electrochemical responses (release of hormones), heart rate variability, and sleep and circadian rhythms follow course.[243]

The fourth category, task-based BBCs, relates to the first (locomotor skills) but takes it in a slightly different direction, looking at interaction with certain stimuli. Driving styles, for instance, may reflect common patterns in speed, pressure on the pedals, braking distances, and tendency to obey traffic signals (or not). Programming styles similarly correlate: use of conventions, layout of source code, capitalization, and variable names may reflect common cognitive processes indicative of certain persons and personalities. Navigational patterns reflect neural processes. How individuals tend to orient themselves to people, animals, places, and objects yields insight into what attracts (and repels) them, how they approach adversity, what is considered an obstacle versus merely a distraction, and the like. Micro and macro gesture analysis provides yet another method.[244] Hand tracking may incorporate PBCs, using palm detection and landmarks as part of a multimodal analysis.[245] How an individual shoots a basketball, passes a football, or dives stems from muscle memory and learned anticipatory actions. In

Celebrity faces can be extremely polarizing, with structures in the orbitofrontal cortex exhibiting activation profiles—in response to an individual seeing such images—which vary proportionate to how that celebrity is perceived. *Id.*

242. *See, e.g.*, Petros Spachos et al., Feasibility Study of Photoplethysmographic Signals for Biometric Identification, *in* 17th INT'L CONF. ON DIGIT. SIGNAL PROCESSING 1, 1, 4 (IEEE, 2011), https://ieeexplore.ieee.org/document/6004938 (arguing that photoplethysmographic signals, which detect blood volume changes in the microvascular bed of tissue, can be used for identification).

243. *See, e.g.*, Mindy Greco et al., *Metabolite Monitoring Concept for the Biometric Identification of Individuals from the Skin Surface*, 149 ANALYST 350, 354–55 (2024) (finding that metabolites in sweat can differentiate individuals); Budiman et al., *supra* note 168, at 3 (analyzing heart rate variability as a biometric). Sleep spindles, short-oscillation waveforms less than two seconds each, are linked to an individual's ability to convert short-term memories to long-term ones. *See, e.g.*, Patrick A. Stokes et al., *Transient Oscillation Dynamics During Sleep Provide a Robust Basis for Electroencephalographic Phenotyping and Biomarker Identification*, SLEEP RSCH. SOC'Y, 2023, at 1, 2–3; David R. Samson, *Taking the Sleep Lab to the Field: Biometric Techniques for Quantifying Sleep and Circadian Rhythms in Humans*, AM. J. HUM. BIOLOGY, 2021, at 1, 2. Both consistent and unique, they can be used to diagnose disorders like schizophrenia and Alzheimer's, as well as neurodivergence. Stokes et al., *supra*, at 3. As with locomotor skills, myriad patents emphasize the collection of systemic information as a means of identification. *See, e.g.*, Infant Monitoring Sys. with Observation-Based Sys. Control & Feedback Loops, U.S. Patent Application No. 15/859,654 para. [0008] (filed Dec. 31, 2017) (sleeping patterns); Cognitive Function Estimation Device, Cognitive Function Estimation Method, & Storage Medium, U.S. Patent Application No. 18/379,326 para. [0008] (filed Oct. 12, 2023) (cognitive function); Sys. for Providing Insightful Lifestyle Notifications, U.S. Patent Application No. 15/699,853 paras. [0003], [0005] (filed Sept. 8, 2017) (sleeping patterns); Opportunistic Sonar Monitoring of Vital Signs, U.S. Patent Application No. 17/360,999 para. [0003] (filed June 28, 2021) (breathing patterns).

244. *See, e.g.*, Tenglong Fan et al., *Wireless Hand Gesture Recognition Based on Continuous-Wave Doppler Radar Sensors*, 64 IEEE TRANSACTIONS ON MICROWAVE THEORY & TECHS. 4012, 4012 (2016); Jaime Lien et al., *Soli: Ubiquitous Gesture Sensing with Millimeter Wave Radar*, ACM TRANSACTIONS ON GRAPHICS, JULY 2016, at 1, 1; Chuan Zheng et al., Doppler Bio-Signal Detection Based Time-Domain Hand Gesture Recognition, *in* IEEE MTT-S INT'L MICROWAVE WORKSHOP SERIES ON RF & WIRELESS TECHS. FOR BIOMEDICAL & HEALTHCARE APPLICATIONS fig. 1 (IEEE, 2013), https://ieeexplore.ieee.org/document/6756200.

245. *See, e.g.*, Scalable Real-Time Hand Tracking, U.S. Patent No. 11,783,496 B2, at [57] (filed Nov. 16, 2021) (issued Oct. 10, 2023) (integrating machine learning for analysis).

online gaming patterns, names employed and weapons of choice reflect style choices. Communication patterns employed, as well as linguistic patterns and data more broadly, reflect neural patterns and generate insight.[246]

The last two categories, strategy- and preference-based BBCs, relate to habitual thought processes. They reveal decisionmaking and calculations taken into account before deciding to act. To isolate strategic processes, studies tend to focus on neural functions and actions undertaken in response to stimuli, as targets perform "perceptual, motor, and/or cognitive tasks."[247] To the extent that such contexts are goal-oriented, degrees of engagement can be ascertained.[248] In the gaming world, patterns in terrain exploration, or collecting resources prior to engaging with (virtual) enemies, reflect choices in how to approach the goal of winning. While strategic biometrics data demonstrates an individual's cognitive or emotional preferences, it can be distinguished from preference-based behavioral biometrics in that the latter captures an individual's tendencies to select one of two or more options when confronted with a choice between a limited number of options. It includes modes employed, such as credit cards versus cash (and which card), which store, which language, and which tools.[249] Some people are more motivated by music, others by punishments, others through positive reinforcement.[250] These technologies can be used for a range of purposes, such as education, exercise, and entertainment—or to get individuals to adopt certain courses of action in the social, political, or economic sphere.[251] Preference biometrics may also center around choice of tool, or which options are employed to accomplish a goal. This choice tends to reflect personality and experience and, like other BBCs, be remarkably consistent over time.

B. QUALITY OF INFORMATION

From the outside, many PBCs and BBCs might just appear to be physical characteristics of the human body or its associated biological systems. Upon closer inspection, however, they reveal significantly more in terms of the scope of information that can be obtained and the sensitivity of that information to exploitation. They are increasingly paired, moreover, with other biometric markers as well as

246. Facebook, for instance, holds patents in using linguistic data to ascertain a user's personality. '752 B2 Patent. This information can be paired with data stored by the company in the user profile, such as gender, number of additional users connected to the target, percentage of connections initiated by the target, profile picture, and number of times the user accesses the site, to identify personality characteristics. *Id.* col. 2 ll. 13–42. By adding additional data, such as the individual's "geographic location, employer, job type, age, music preferences, interests," and other attributes, the company can "select news stories, advertisements, [and] recommendations," thus "increase[ing] the likelihood that the user will favorably interact with the selected content." *Id.* col. 1 ll. 31–33, col. 2 ll. 38–42.

247. Xue et al., *supra* note 228, at 120.

248. *Id.* at 130.

249. Some patents, for instance, emphasize ways in which biometric feedback can help to determine which stimuli most effectively motivate the target. *See, e.g.*, Memory-Based Motivational Mode, U.S. Patent No. 11,883,744, at [57] (filed Oct. 26, 2021) (issued Jan. 30, 2024).

250. *Id.* col. 1 ll. 54–59.

251. *Id.* col. 1 ll. 39–44.

non-biometric information and contextual data, enabling the growth of biomanipulation.

1. Scope

There is a tendency to think about traditional PBCs as relatively innocuous. Dermatoglyphics, the study of finger, hand, and foot shapes and patterns, after all, has been around for centuries.[252] But information that can be obtained from even traditional PBCs has altered. Palm and finger print ridges are now correlated to a range of medical conditions, from Down Syndrome and diabetes to asthma, cancer, and schizophrenia.[253] Body odor does more than just identify a person: menstrual periods, emotions, and the presence of certain diseases can impact it, making their detection possible.[254] The shift from static to systemic data yields deeper insights. Electrocardiographs, phonocardiographs, photoplethysmography, and encephalography do more than just identify individuals: they provide access to medical conditions and physiological strengths and weaknesses.[255] DNA sequencing can show familial connections and genetic dispositions.

The depth of information that can be obtained from BBCs, in turn, is nothing short of remarkable. Eye tracking, for instance, can provide insight into identity,

252. The Chinese Qin Dynasty (221–206 B.C.) is believed to be the first to use fingerprints for identification. Barnes, *supra* note 147, at 8. Much later, in 1858, William James Herschel, a British Administrator for the East India Company, began using handprints to administer criminal law, register deeds, and prevent fraud. *Id*. at 11; JOE NICKELL & JOHN F. FISCHER, CRIME SCIENCE: METHODS OF FORENSIC DETECTION 113 (1999). Soon afterwards, Henry Faulds, a Scottish physician based in Tokyo, used latent prints to exonerate a man, publishing his research in *Nature* magazine. *See* Henry Faulds, *On the Skin-Furrows of the Hand*, 22 NATURE 605 (1880). Francis Galton went on to distinguish finger, palm, and foot prints, declaring papillary ridges "the most important of all anthropological data." GALTON, *supra* note 147, at 1–2. He explained: "They have the unique merit of retaining all their peculiarities unchanged throughout life, and afford in consequence an incomparably surer criterion of identity than any other bodily feature." *Id*. at 2. Print analyses proved just one of myriad correlative traits. In 1893, Alphonse Bertillon from the *Préfecture de police* in Paris proposed a system of facial recognition, categorizing the size and shape of each part of the ear; the contours of the nose and its distance from other facial features; iris color and size; and upper and lower eyelids to aid in criminal suspect identification. BERTILLON, *supra* note 6, at 28, 67–79 (classifying the morphological qualities of each part of the ear); *id*. at 45 (noting upper and lower eyelid, pupil size, and iris contours and color); *id*. at 63–65 (noting nose characteristics); *id*. at 82 (noting distance from the base of the nose to the lips, prominence of the lips, etc.); *id*. at 129–33 (noting front and side photographs of the head). Bertillon paired eleven body measurements with profile analysis, hair color, and skin pigmentation for identification. *See id*. at xvi–xxi (including among the eleven measurements length of left arm; length, breadth, and diameter of skull; distance between left and right fingertips arms outstretched; height sitting and standing; length of left middle and little fingers; and length of left foot and right ear); *id*. at xxxi, lxviii (noting use of the system in the Préfecture); *id*. at 43 (noting eye color); *id*. at 55–57 (noting beard and hair color); *id*. at 57–58 (noting complexion/skin pigmentation); *id*. at 59 (noting profile); *id*. at 80, 84–86 (noting head profile).

253. *See, e.g.*, *supra* note 64 and accompanying text.

254. *See* Denise Chen & Jeannette Haviland-Jones, *Human Olfactory Communication of Emotion*, 91 PERCEPTUAL & MOTOR SKILLS 771, 779–80 (2000); Jan Havlicek & Pavlina Lenochova, *Environmental Effects on Human Body Odour*, *in* CHEMICAL SIGNALS IN VERTEBRATES 11, at 199, 200 (Jane L. Hurst et al. eds., 2008).

255. Jean-Philippe Couderc et al., *Detection of Atrial Fibrillation Using Contactless Facial Video Monitoring*, 12 HEART RHYTHM 195, 200 (2015).

gender, body weight, age, cultural background, native language, and ethnicity, as well as drug use.[256] It can reveal personality traits, emotional states, and levels of attentiveness.[257] Paired with emotion recognition software, it can generate insight into what feelings a target experiences.[258] It can reveal gambling tendencies or consumption and purchasing behavior.[259] So, too, can it shed light on athletic, social, and cognitive skills and abilities, as well as fears.[260] It can convey sexuality.[261] It can be used to diagnose a range of mental and physical health conditions, from schizophrenia and bipolar disorder to Tourette's syndrome and Parkinson's disease.[262]

Studies have used eye tracking to reveal emotional intelligence (itself a predictor of mental health), indecision, anxiety, sexual compulsiveness, impulsivity,

256. *See* Kröger et al., *supra* note 66, at 226, 228, 230, 233–34 (surveying the literature on eye tracking and summarizing what information can be gleaned); Joshua O. Goh et al., *Culture Modulates Eye-Movements to Visual Novelty*, PLOS ONE, Dec. 2009, at 1, 1; Stephen D. Goldinger et al., *Deficits in Cross-Race Face Learning: Insights from Eye Movements and Pupillometry*, 35 J. EXPERIMENTAL PSYCH. 1105, 1105–06 (2009); Aine Ito et al., *Investigating the Time-Course of Phonological Prediction in Native and Non-Native Speakers of English: A Visual World Eye-Tracking Study*, J. MEMORY & LANGUAGE, FEB. 2018, at 1, 20. Inferences can be drawn about which drugs have been used or consumed (e.g., alcohol, tobacco, cocaine, cannabis, etc.). *See* Kröger et al., *supra* note 66, at 228.

257. *See* Sys. & Method for Determining Hum. Emotion by Analyzing Eye Props., U.S. Patent Application No. 11/522,476 paras. [0003], [0083] (filed Sept. 18, 2006); Sabrina Hoppe et al., *Eye Movements During Everyday Behavior Predict Personality Traits*, FRONTIERS HUM. NEUROSCIENCE, Apr. 13, 2018, at 1, 1.

258. *See* Vidas Raudonis et al., *Evaluation of Human Emotion from Eye Motions*, 4 INT'L J. ADVANCED COMPUT. SCI. & APPLICATIONS 79, 84 (2013).

259. *See* Daniel S. McGrath et al., *The Specificity of Attentional Biases by Type of Gambling: An Eye-Tracking Study*, PLOS ONE, Jan. 31, 2018, at 1, 13 (gambling); H. Zamani et al., *Eye Tracking Application on Emotion Analysis for Marketing Strategy*, 8 J. TELECOMM., ELEC. & COMPUT. ENG'G 87, 89 (2016) (purchasing patterns).

260. *See Eye Tracking Gives Athletes an Unprecedented Edge*, FREETHINK (Feb. 6, 2020), https://www.freethink.com/series/the-edge/eye-tracking [https://perma.cc/P86M-NL3R] (athletic skills); Rachel K. Greene et al., *Dynamic Eye Tracking as a Predictor and Outcome Measure of Social Skills Intervention in Adolescents and Adults with Autism Spectrum Disorder*, 51 J. AUTISM & DEVELOPMENTAL DISORDERS 1173, 1174 (2021) (social skills); Kröger et al., *supra* note 66, at 229 (cognitive processing); Jorg Huijding et al., *To Look or Not to Look: An Eye Movement Study of Hypervigilance During Change Detection in High and Low Spider Fearful Students*, 11 EMOTION 666, 667 (2011) (fear).

261. *See* Wenzlaff et al., *supra* note 66, at 1013. Pupillary responses, blink properties, and length of gaze can be used to build a model of mating preferences towards particular body shapes, facial characteristics, body parts, or individuals with different levels of social status or dominance. *See id.* at 1008, 1011; *see also* Method & Sys. of Using Eye Tracking to Evaluate Subjects, U.S. Patent Application No. 14/681,083, at [57] (filed Apr. 7, 2015) (using eye position, movement, and gaze pattern and pupil response to ascertain attractors and aversions).

262. *See* Katarzyna Harezlak & Pawel Kasprowski, *Application of Eye Tracking in Medicine: A Survey, Research Issues and Challenges*, 65 COMPUTERIZED MED. IMAGING & GRAPHICS 176, 181 (2018) (schizophrenia, bipolar disorder, Parkinson's disease); Eckstein et al., *supra* note 208, at 81 (Tourette's syndrome); Philip J. Benson et al., *Simple Viewing Tests Can Detect Eye Movement Abnormalities that Distinguish Schizophrenia Cases from Controls with Exceptional Accuracy*, 72 BIOLOGICAL PSYCHIATRY 716, 722–23 (2012) (schizophrenia). *See also* Kröger et al., *supra* note 66, at 227 (discussing physical and mental health conditions).

and aggressive tendencies.[263] It can be used to gauge reading and listening comprehension skills and level of expertise in a variety of contexts—from chess to surgery.[264] Researchers examining reaction times and ocular movements have gleaned insight into how responsive individuals are to peer pressure and social norms.[265] It is far from the only BBC employed.

2. Nature of Data and Target Vulnerability

Not only can a tremendous amount of information be obtained via collection of BBCs and PBCs, but much of the information garnered can be used to gain insight, directly and through inference, into the most sensitive personal information possible. To the extent that biomanipulation takes advantage of a target's vulnerabilities, it matters.

Consider again, for instance, the ability to measure gaze direction and pupil reactivity. In addition to the myriad types of information already discussed, pupil size, blink properties, and saccadic eye movements can be used to evaluate an individual's emotional state.[266] Happiness, disgust, fear, surprise, and other responses can be tracked over time points.[267] Biometric data can be used to evaluate the subject's "mental workload" or whether an individual is tired.[268] It can reveal the onset

263. *See, e.g.*, Kröger et al., *supra* note 66, at 230 (finding gaze metrics to be associated with all listed characteristics); Rosanna G. Lea et al., *Trait Emotional Intelligence and Attentional Bias for Positive Emotion: An Eye Tracking Study*, 128 PERSONALITY & INDIVIDUAL DIFFERENCES 88, 91 (2018); Alexandra Martins et al., *A Comprehensive Meta-Analysis of the Relationship Between Emotional Intelligence and Health*, 49 PERSONALITY & INDIVIDUAL DIFFERENCES 554, 561–62 (2010); Yannick Lufimpu-Luviya et al., *Degree of Subject's Indecisiveness Characterized by Eye Movement Patterns in Increasingly Difficult Tasks*, *in* CURRENT TRENDS IN EYE TRACKING RESEARCH 107, 120 (Mike Horsley et al. eds., 2014); Wenzlaff et al., *supra* note 66, at 1010; Jasmine Pettiford et al., *Increases in Impulsivity Following Smoking Abstinence Are Related to Baseline Nicotine Intake and Boredom Susceptibility*, 32 ADDICTIVE BEHAVS. 2351, 2355 (2007); Katja Bertsch et al., *Interpersonal Threat Sensitivity in Borderline Personality Disorder: An Eye-Tracking Study*, 31 J. PERSONALITY DISORDERS 647, 667 (2017).

264. *See, e.g.*, Zehui Zhan et al., *Online Learners' Reading Ability Detection Based on Eye-Tracking Sensors*, 16 SENSORS 1457, 1457–58, 1468 (2016) (recognizing information about the eye as indicative of reading ability); Eyal M. Reingold & Neil Charness, *Perception in Chess: Evidence from Eye Movements*, *in* COGNITIVE PROCESSES IN EYE GUIDANCE 325, 330 (Geoffrey Underwood ed., 2005) (examining eye movement patterns during chess games); Harezlak & Kasprowski, *supra* note 262, at 186 (examining eye-gaze patterns in surgeons).

265. *See* Andrea Guazzini et al., *Cognitive Dissonance and Social Influence Effects on Preference Judgments: An Eye Tracking Based System for Their Automatic Assessment*, 73 INT'L J. HUM.-COMPUT. STUD. 12, 12–13 (2015).

266. *See, e.g.*, Attila Gere et al., *Influence of Mood on Gazing Behavior: Preliminary Evidences from an Eye-Tracking Study*, 61 FOOD QUALITY & PREFERENCE 1, 1–2 (2017) (distinguishing between positive and negative moods); Richard J. Macatee et al., *Attention Bias Towards Negative Emotional Information and Its Relationship with Daily Worry in the Context of Acute Stress: An Eye-Tracking Study*, 90 BEHAV. RSCH. & THERAPY 96, 100, 104 (2017); '476 Patent Application, *supra* note 257, at [57].

267. *See, e.g.*, Utilizing Eye-Tracking to Estimate Affective Response to a Token Instance of Interest, U.S. Patent No. 9,569,734 B2 col. 35 ll. 20–23, 34–36 (filed Mar. 15, 2015) (issued Feb. 14, 2017).

268. *See id.* col. 39 ll. 43–48; Kilseop Ryu & Rohae Myung, *Evaluation of Mental Workload with a Combined Measure Based on Physiological Indices During a Dual Task of Tracking and Mental Arithmetic*, 35 INT'L J. INDUS. ERGONOMICS 991, 993 (2005).

and evolution of cognitive, developmental, and mental disorders.[269] It yields insight into what individuals remember, as well as decisionmaking strategies and ways in which individuals acquire, process, and interpret data.[270]

Despite the sensitivities involved, numerous companies are looking to capitalize on the insights that can be gained from eye tracking and then using the information for biomanipulation.[271] Such information could be collected not just for one user, but for entire groups. By calculating whether the shift is linear, exponential, logarithmic, or some other rate, the system can then anticipate what images, colors, and sequences to use in the future to be able to manipulate individuals to the desired emotional state—from joy and sexual arousal to sorrow or fear.[272]

3. Multimodal Collection and Combined Data

One of the enabling features of biomanipulation is the use of multimodal collection, as well as the combination of biometric data with other kinds of information. Over the past fifteen years, there has been an explosion in the integration of each into product and system design.[273] Even within PBCs, multimodal collection proliferates. Part of the reason is that it tends to offer higher degrees of certainty than unimodal systems, with the result being pressure on anyone designing such systems to collect multiple PBCs to reach a higher level of assuredness. Doing so helps to ensure the integrity of future results, in terms of verifying identity as well as eliminating potentially erroneous matches. Even systems which focus on just one body part, such as the hand, may rely on multiple modalities, such as hand

269. *See, e.g.*, Laurent Itti, *New Eye-Tracking Techniques May Revolutionize Mental Health Screening*, 88 NEURON 442, 442, 444 (2015); Vidal et al., *supra* note 207, at 1306, 1310; Dmitry Lagun et al., *Detecting Cognitive Impairment by Eye Movement Analysis Using Automatic Classification Algorithms*, 201 J. NEUROSCIENCE METHODS 196, 202 (2011).

270. Eckstein et al., *supra* note 208, at 86; George E. Raptis et al., Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies, *in* UMAP '17: PROC. OF THE 25TH CONF. ON USER MODELING, ADAPTATION & PERSONALIZATION 164, 166, 171 (Ass'n for Computing Mach., 2017), https://dl.acm.org/doi/10.1145/3079628.3079690.

271. *See, e.g.*, Interactive Media Facial Emotion-Based Content Selection Sys., U.S. Patent No. 11,373,446 B1 figs. 3A–B (filed Apr. 26, 2019) (issued June 28, 2022).

272. *See* '734 B2 Patent, *supra* note 267, col. 46 ll. 27–31. To the extent that companies *use* such vulnerabilities, particularly outside consent, targets can be exploited. Take, for instance, a common insecurity: weight. Apple's relatively recent application for body composition analysis notes that by collecting biometric data from just a few regions, such as the cheeks and neck, biometric systems can provide detailed analysis of body composition. It is not a particularly significant leap to assume that if a digital device is monitoring "certain fat pockets," it may alert the user and propose ways to address it. The patent application explains, "health and fitness data may be used to provide insights into a user's general wellness." '194 Patent Application, *supra* note 132, paras. [0066], [0092]. The company can then market various solutions to the user.

273. *See, e.g.*, Multi-Modal Biometric Database Searching Methods, U.S. Patent No. 9,286,528 B2 fig. 6 (filed Apr. 16, 2014) (issued Mar. 15, 2016); Multimodal Biometric Platform, U.S. Patent No. 7,596,246 B2 fig. 1 (filed Oct. 29, 2007) (issued Sept. 29, 2009); Multimodal Biometric Platform, U.S. Patent No. 7,606,396 B2 fig. 1 (filed Oct. 29, 2007) (issued Oct. 20, 2009); Voice-Based Multimodal Speaker Authentication Using Adaptive Training & Applications Thereof, U.S. Patent No. 7,529,669 B2 fig. 1 (filed June 13, 2007) (issued May 5, 2009); Sys. & Method for Using, Processing, & Displaying Biometric Data, U.S. Patent Application No. 16/704,844 fig. 2B (filed Dec. 5, 2019).

geometry, palm prints, and dorsal vascular patterns.[274] Similarly, in systems focused on facial features, molecular biometric signatures can be paired with FRT or periocular data.[275]

Numerous systems cross PBCs and BBCs to gain deeper insight.[276] Others combine multiple BBCs, like gaze and touch.[277] In 2015, for instance, Yahoo introduced Bodyprint, a biometric authentication system for mobile phones that combined ear, fist, phalanges, palm grip, and finger grip biometrics to bypass FRT and ensure higher accuracy.[278] While that approach was limited to a handful of PBCs, others collect multitudinous markers. In the realm of mental health, for example, one patent contemplates use of heart rate, electrodermal activity, galvanic skin response, electroencephalogram, and eye-tracking sensors, as well as microphones and thermometers.[279] Together, they generate insight into anxiety, mood, psychotic, eating, impulse control, addiction, personality, obsessive-compulsive, and post-traumatic stress disorders.[280]

The pairing of biometric data with other information further enables biomanipulation. The resulting volume and complexity require ML models to be able to analyze and generate information that can most effectively lead an individual to act in certain ways. Myriad examples present. One of the largest growing areas, for instance, relates to customized media content. Patents employ deep learning, neural networks, and AI in conjunction with facial recognition, geolocational data, and secondary content to identify a user's preferences and generate a custom media stream.[281] In one case, "age, gender, education, interests, [and] interaction history" also are fed into the model.[282] The system not only identifies who is using the device, and their preferences, but where they are located—whether it be a museum, a park, a doctor's office, a bar, a public space, a retail establishment, a restaurant, or

274. *See, e.g.*, GiTae Park & Soowon Kim, *Hand Biometric Recognition Based on Fused Hand Geometry and Vascular Patterns*, 13 SENSORS 2895, 2896 (2013).

275. *See* Sengupta et al., *supra* note 184, at 831.

276. *See, e.g.*, Kumar M. & Swamy, *supra* note 117, at 201 (correlating speaker identity with the physiological and behavioral characteristics of the speaker and suggesting that the most effective fusion relies on operational requirements like accuracy needed, training sets, and the validity of simplifying assumptions).

277. *See, e.g.*, Mohamed Khamis et al., GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices, *in* CHI EA '16: PROC. OF THE CHI CONF. EXTENDED ABSTRACTS ON HUM. FACTORS IN COMPUTING SYS. 2156, 2157 (Ass'n for Computing Mach., 2016), https://dl.acm.org/doi/abs/10.1145/2851581.2892314.

278. Holz et al., *supra* note 150, at 3011–12.

279. Mgmt. of Psychiatric or Mental Conditions Using Digit. or Augmented Reality with Personalized Exposure Progression, U.S. Patent Application No. 18/073,407 fig. 4A (filed Dec. 1, 2022) (issued June 1, 2023).

280. *See id.*

281. *See, e.g.*, Sys. & Method of Providing Customized Media Content, U.S. Patent No. 11,838,587 B1 figs. 2, 5, col. 3 ll. 5–10 (filed July 14, 2023) (issued Dec. 5, 2023).

282. *Id.* col. 11 ll. 37–44.

a sporting event.[283] It "may then use the information . . . to learn complex patterns and inform the neural network's decisionmaking process."[284] The technology has become increasingly sophisticated and worked its way into the online world, with virtual reality and gaming systems enabling further collection.[285] AI/ML helps to generate further insight into how people think and what they believe, and how to shape their beliefs, desires, emotions, and behavior in the future.

C. REMOTE ACCESS AND ENVIRONMENTAL MONITORING

Another characteristic enabling biomanipulation stems from the ability to obtain biometric data from a distance. The result has been a growth in what I term "environmental monitoring," which I define as the collection of biometric data from one or more individuals within a specified area over time. The place itself may be three-dimensional, such as a room in a home, or a street corner, or an online or device-specific digital space, such as YouTube channels or photo or video streams. In either case, new and emerging technologies are making biometric collection from afar possible. Full body scanning, for instance, can use millimeter or THz waves, quantum sensors, camera-based scanning systems, radar, or holographic systems to capture biometric data from afar.[286] Height can be ascertained from direct measurements, or by calculating the relationship between the individual and their distance from the camera as well as a stationary marker, such as a door frame. Thermal infrared, near-infrared, video-based, image-based, and 3D recognition can be applied to facial, dermal, and vascular characteristics.[287]

Numerous implications follow. For one, targets may be unaware that they are giving up any data—much less what information they have revealed. Unless the law requires consent prior to collection, analysis, and distribution of the information—or companies voluntarily limit each—there may be no indication that a company has collected biometric information, much less how it has been used, with whom it has been shared, or to whom it has been leased or sold. Remote access also means that formal enrollment is no longer necessary. Instead, systems can collect data as individuals pass through a space, correlating it with prior visitors to identify repeat performers. Names no longer matter. The biometric itself becomes the anchor, making it possible to correlate data with *that* individual in the future. Such information, moreover, is not just obtained from one person, but

283. *Id.* col. 2 ll. 62–67.

284. *Id.* col. 10 ll. 28–31.

285. Haptic gaming gear and associated sensors introduce a new level of insight. The Teslasuit, for instance, is billed as "a complete solution for understanding human behavior." *See A Breakthrough in Human Performance Training*, TESLASUIT, https://teslasuit.io/(last visited Jan. 2, 2025). It "provides haptic feedback and captures motion and biometrics." *Id.*

286. *See* FRONTEX, *supra* note 130, at 29.

287. *Id.* at 28; *see also* Sys. & Method for Biometric Identification Using Ultraviolet (UV) Image Data, U.S. Patent Application No. 13/076,725 paras. [0002], [0006] (filed Mar. 31, 2011) (issued Oct. 4, 2012) (critiquing prior systems for being "inadequate for detecting and accurately identifying target individuals from a distance" and offering a system instead based on ultraviolet imaging of at least one skin area).

can be collected from multiple people at the same time, with implications for generating further insight into individuals' associations.[288]

D. PREDICTIVE ANALYTICS AND THE FEEDBACK LOOP

Part of the power of behavioral biometrics is that they can be used to predict future behavior: how individuals are likely to feel, act, or react in different circumstances.[289] Collecting data on patterns enhances the potential for future manipulation. Once predictions are established and interference in the decision-making process enabled, the hypotheses on which they rest can be tested. Targets' responses to stimuli or situations can be evaluated. As information is recorded and analyzed, it provides for a feedback loop, allowing third parties to refine their models to become more effective at shaping individuals.[290] To the extent that such behavior both draws on and plays into biological processes and predilections, the target may increasingly lose agency or authorship. Their beliefs, desires, emotions, and ultimately (non)actions are being captured by others. While it may be an obvious point, it is worth noting that the more power a system has over input or stimuli on the one hand and environmental factors on the other, the more effective the system can be in developing ever more accurate methods of manipulating the target. Particular attention should therefore be paid to VR and gaming contexts. Using sophisticated AI and ML, numerous patents call out ways in which entire worlds can be created, and personalized, to ensure that a target acts in a manner commensurate with the system's goals.[291] In some manifestations, this may mean that healthcare can be more effectively delivered.[292] The flip side is that it also may mean that individuals have an ever-decreasing amount of agency.

III. STATUTORY AND REGULATORY PROVISIONS

Although Congress has recently begun to inquire into biometrics, no federal legislation addresses the collection, analysis, use, retention, and trade of biometric data writ large, much less biomanipulation.[293] Nor is there a comprehensive consumer privacy statute at a federal level which might otherwise incorporate

288. *See, e.g.*, Qifan Pu et al., Whole-Home Gesture Recognition Using Wireless Signals, *in* MOBICOM '13: PROC. OF THE 19TH ANN. INT'L CONF. ON MOBILE COMPUTING & NETWORKING 27, 28, 36–37 (Ass'n for Computing Mach., 2013), https://dl.acm.org/doi/10.1145/2500423.2500436 (identifying and classifying nine gestures with an average accuracy of 94%).

289. *See, e.g.*, Guazzini et al., *supra* note 265, at 13–14 (arguing that eye-tracking data will enable collectors to predict human decisions and behavior).

290. *See, e.g.*, '587 Patent, *supra* note 281, col. 11 ll. 41–46 ("The outputs from the deep learning module can be employed by the other modules within the machine learning model to make predictions about what content to deliver to a particular user. Over the course of predictions and feedback, the deep learning module can become more accurate in determining user preferences.").

291. *See, e.g.*, Adapting a Virtual Reality Experience for a User Based on a Mood Improvement Score, U.S. Patent Application No. 18/064,258 fig. 4 (filed Dec. 10, 2022).

292. *See, e.g.*, Biofeedback for Therapy in Virtual & Augmented Reality, U.S. Patent No. 11,523,773 B2, at [57], col. 1 ll. 15–18 (filed Feb. 18, 2020) (issued Dec. 13, 2022).

293. *See, e.g.*, *Privacy in the Age of Biometrics: Hearing Before the Subcomm. on Investigations & Oversight of the H. Comm. on Science, Space, & Tech.*, 117th Cong. 63 (2022); *Facial Recognition*

biometrics as a subcategory. In the regulatory realm, only one entity, the Federal Trade Commission (FTC), appears to have paid any attention to the matter.[294] This Section, accordingly, begins with an overview of FTC enforcement actions. At a state level, only four (Texas, Illinois, Washington, and Colorado) have biometric-specific laws.[295] Three limit their focus to just a handful of PBCs and one BBC.[296] (Colorado, whose law will go into effect in 2025, is the only state which includes a clause that captures other forms of biometrics.)[297] Fourteen states (including Colorado) have enacted broader, comprehensive consumer protection

Technology (Part III): Ensuring Commercial Transparency and Accuracy: Hearing Before the H. Comm. on Oversight & Reform, 116th Cong. 2, 3, 49, 53 (2020). A few federal measures address narrow aspects of biometrics. The Genetic Information Nondiscrimination Act, for instance, requires that employers, employment agencies, labor organizations, and joint labor–management committees maintain genetic information about employees on separate forms and medical files and treat them as confidential medical records, but it does not regulate DNA-related biometric data writ large. *See* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 206, 122 Stat. 881, 913. But there are no broader statutes regulating the capture and use of biometric data.

294. Unlike the FTC, neither the FCC nor the SEC has taken recent enforcement actions related to the protection of biometric data. Instead, the SEC appears to only act against biometrics companies when they lie to investors, instead of in relation to the underlying privacy concerns raised by the collection and use of sensitive information. *See, e.g.*, Complaint at 1–4, SEC v. NAC Found., LLC, No. 20-cv-04188 (N.D. Cal., June 25, 2020). In June 2023, the FCC announced the creation of a Privacy and Data Protection Task Force, which might indicate future interest, but as of the time of writing, no public actions appear to have been taken. *See* Press Release, FCC, Chairwoman Rosenworcel Launches New 'Privacy and Data Protection Task Force' (June 14, 2023) [https://perma.cc/YWB8-BJUG].

295. Capture or Use of Biometric Identifier Act, TEX. BUS. & COM. CODE ANN. § 503.001; Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5; Washington My Health My Data Act, WASH. REV. CODE § 19.373.020 (supplementing WASH. REV. CODE § 19.375 concerning biometric identifiers); H.R. 24-1130, 75th Gen. Assemb., Reg. Sess. (Colo. 2024). Fifteen more states in 2023 considered bills related to biometric collection. *See* S. 1238, 56th Leg., 1st Reg. Sess. (Ariz. 2023); S. 730, 2023 Gen. Assemb., Jan. Sess. (Conn. 2023); S. 1085, 2023 Leg., 32nd Sess. (Haw. 2023); S. 239, 2023 Gen. Assemb., Reg. Sess. (Ky. 2023); H.R. 1705, 131st Leg., 1st Spec. Sess. (Me. 2023); S. 169, 2023 Gen. Assemb., Reg. Sess. (Md. 2023); S. 195, 193rd Gen. Ct., Reg. Sess. (Mass. 2023); S. 954, 2023 Leg., 93rd Sess. (Minn. 2023); H. 1047, 102nd Gen. Assemb., 1st Reg. Sess. (Mo. 2023); S. 351, 68th Leg. (Mont. 2023); S. 370, 2023 Leg., 82nd Sess. (Nev. 2023); S. 3499, 220th Leg. (N.J. 2023); G.A. 1362, 2023 Leg., 2023–2024 Reg. Sess. (N.Y. 2023); H.R. 926, 2023 Gen. Assemb., Reg. Sess. (Pa. 2023); S. 339, 113th Gen. Assemb. (Tenn. 2023). None passed. *See 2024 State Biometric Privacy Law Tracker*, HUSCH BLACKWELL (Jan. 16, 2025), https://www.huschblackwell.com/2024-state-biometric-privacy-law-tracker. A few states and municipalities have extremely narrow provisions dealing with certain aspects of FRT or fingerprinting. *See, e.g.*, MD. CODE ANN., LAB. & EMPL. § 3-717 (prohibiting employers from "creating a facial template" of a job applicant during an interview without their consent); N.Y. LAB. LAW § 201-a (prohibiting employers from requiring a fingerprint from employees as a condition of employment); PORTLAND, OR., CITY CODE ch. 34.10 (prohibiting FRT in specific locations); NEW YORK, N.Y., ADMIN. CODE §§ 22-1201 (requiring commercial establishments which collect biometric identifiers to post signs at their entrance notifying customers).

296. TEX. BUS. & COM. CODE ANN. § 503.001(a) (defining a biometric identifier as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry"); 740 ILL. COMP. STAT. 14/10 (defining a biometric identifier as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"); WASH. REV. CODE § 19.373.010(4)(b) (including keystroke patterns and gait in the "biometric data" protected by the Act).

297. *See* Colo. H.R. 24-1130 § 3(2.4).

laws, which might conceivably cover this type of data, but only a limited number address biometrics, and even then the statutory reach is restricted.[298]

A. FEDERAL LANDSCAPE

No federal statutes govern biometrics, and neither the FCC nor the SEC have taken enforcement actions related to the protection of biometric data. The FTC, for its part, approaches biometric collection through the lens of deceptive and unfair trade practices, over which the agency has jurisdiction through the 1914 Federal Trade Commission Act (FTA) and the 1998 Children's Online Privacy Protection Act (COPPA).[299] It does not regulate the collection, analysis, use, or transmission of biometric data writ large.[300] Even in its limited realm, it has brought only a handful of actions.

In 2012, for instance, according to the FTC, Facebook agreed to give "consumers clear and prominent notice and obtain[] their express consent before sharing their information beyond their privacy settings, [to] maintain[] a comprehensive privacy program to protect consumers' information, and [to] obtain[] biennial privacy audits from an independent third party."[301] The company did not act consistent with its representation. So, in 2019, the FTC fined Facebook $5 billion for, *inter alia*, violating the 2012 agreement and deceiving consumers about its FRT.[302] Two years later, the FTC brought a second action, accusing Everalbum—

298. *See, e.g.*, Texas Data Privacy and Security Act, TEX. BUS. & COM. CODE ANN. § 541 (took effect July 1, 2024); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 to -576, -578, -580 (took effect Jan. 1, 2023); Indiana Consumer Data Protection Act, IND. CODE § 24-15-6-1(b)(3)(C) (to take effect Jan. 1, 2026); Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-101 to -102 (took effect May 1, 2024); Iowa Data Privacy Act, S. 262, 89th Gen. Assemb., Reg. Sess. (to take effect Jan. 1, 2025).

299. Federal Trade Commission Act, 15 U.S.C. § 45(a)(2); Children's Online Privacy Protection Act, 15 U.S.C. §§ 6502, 6506; *see also* FED. TRADE COMM'N, NO. P221202, POLICY STATEMENT REGARDING THE SCOPE OF UNFAIR METHODS OF COMPETITION UNDER SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT (2022) ("Section 5 . . . encompass[es] various types of unfair conduct. . . ."); 16 C.F.R. § 312.3 (making it unlawful to engage in tracking personal information of a child online).

300. The agency first dipped its toe in the water with a 2007 workshop on identity authentication. *See* Press Release, Fed. Trade Comm'n, FTC to Host Identity Authentication Workshop (Feb. 21, 2007), https://www.ftc.gov/news-events/news/press-releases/2007/02/ftc-host-identity-authentication-workshop [https://perma.cc/BK7Y-CPUX]. Four years later, it hosted a second workshop on FRT, bringing participants from government, academia, and industry together to discuss the state of the technologies, potential commercial benefits, and associated privacy and security concerns. *See* Press Release, Fed. Trade Comm'n, Face Facts: A Forum on Facial Recognition Technology (Dec. 8, 2011), https://www.ftc.gov/news-events/events/2011/12/face-facts-forum-facial-recognition-technology [https://perma.cc/Q6TE-C29L]; *see also* FED. TRADE COMM'N, POLICY STATEMENT OF THE FEDERAL TRADE COMMISSION ON BIOMETRIC INFORMATION AND SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT 1–2 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf [https://perma.cc/C3ZJ-JGSN] [hereinafter FTC POLICY STATEMENT] (discussing the 2011 forum). The findings formed the bases for a 2012 report. *See* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES, at ii (2012), https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies [https://perma.cc/8NW7-LQXD].

301. Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/ftc-approves-final-settlement-facebook [https://perma.cc/RSF9-2B2Q].

302. Although the company's policy explained the company would use FRT "[i]f it is turned on" (giving customers the opportunity to opt in), "tens of millions of users who still had an older version of Facebook[] . . . had to opt out to disable facial recognition." Complaint at 6, United States v. Facebook,

whose product (Ever) provided photo storage and organization—of misleading consumers by stating that it would not use FRT on consumer content without customers' express consent, while simultaneously doing just that.[303] In 2023, the FTC took three further biometric-related actions under COPPA.[304]

In May 2023, the FTC issued a policy statement noting the sudden growth in biometric technologies and outlining how it planned to apply Section 5 of the FTC Act going forward.[305] It defined biometric data as information "that depict[s] or describe[s] physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body."[306] This includes "depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern)."[307] It also incorporates information "derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had

Inc., No. 19-cv-2184 (D.D.C. July 24, 2019); *see also* FTC POLICY STATEMENT, *supra* note 300, at 7 & n. 35 (referencing FTC actions taken against businesses "engaging in deceptive practices related to the collection and use of biometric information").

303. *See* Complaint at 3, Everalbum, Inc., FTC File No. 1923172, No. C-4743 (F.T.C. May 6, 2021). The settlement requires Everalbum to disclose to users all purposes for using and/or sharing biometric data, delete consumer content after deactivation, and obtain "affirmative express consent" before using consumer biometric information. *See* Everalbum, Inc., No. C-4743 (F.T.C. May 6, 2021), 2021 WL 1922417, at *4.

304. In the first, the FTC required Microsoft to pay $20 million for statutory violations resulting from collecting and retaining information from children who used Xbox without notifying or obtaining consent from parents. Press Release, Fed. Trade Comm'n, FTC Will Require Microsoft to Pay $20 Million over Charges It Illegally Collected Personal Information from Children Without Their Parents' Consent (June 5, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-will-require-microsoft-pay-20-million-over-charges-it-illegally-collected-personal-information [https://perma.cc/CB8X-VFRM]. The FTC made "clear that avatars generated from a child's image, and biometric and health information, are covered by the COPPA Rule when collected with other personal data." *Id.* Amazon's Alexa also came under fire for recording and indefinitely storing voice recordings (including from children) and using them for machine learning, contradicting representations made to customers by Amazon that they could delete any stored recordings of their communications with the device. Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever [https://perma.cc/F4V6-Z56U]. The proposed order requires that the company delete significant amounts of information and pay a $25 million penalty. *Id.* The final complaint against Edmodo, a K–12 edtech company, alleged the collection of children's data (described as "persistent identifiers") without consent and use of the data for advertising in violation of COPPA. Press Release, Fed. Trade Comm'n, FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts (May 22, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising [https://perma.cc/N6EH-9G9B]. The order requires the company to "delete models or algorithms developed using personal information collected from children without verifiable parental consent or school authorization" and to pay a $6 million penalty. *Id.*

305. FTC POLICY STATEMENT, *supra* note 299, at 1–2, 5.

306. *Id.* at 1.

307. *Id.*

been derived."[308] That covers both the original photograph of a person's face and the template, embedding, faceprint, or other production of data associated with the original image.[309]

Despite the breadth of the definition, as a statutory matter the FTC's actions are largely limited to restricting fraudulent or unfair practices—not to regulating biometric collection, much less biomanipulation writ large. The agency, accordingly, lists potential practices that may fall within its purview: "false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information" and "[d]eceptive statements about the collection and use of biometric information."[310] While unfair practices include failing to assess foreseeable harms prior to collection, to address known or foreseeable risks, to evaluate third-party capabilities, to provide appropriate training, and to conduct ongoing monitoring of technologies,[311] *none* of the requirements set an objective standard for what the companies must do to comply. Merely evaluating third parties says nothing about precisely what they need to evaluate or what they need to do with the information once they do so. Nor does it detail "appropriate training" or the end to which ongoing monitoring of the company's technologies will be put. The most promising of the unfair practices relates to the potential for FTC enforcement action in response to "surreptitious and unexpected collection or use of biometric information."[312]

B. STATE LAWS

State protections against the collection, analysis, and use of PBCs and BBCs and corporate (or government) engagement in biomanipulation are paltry at best and, in any event, only apply to corporate actors. Only four states have biometric-specific laws, just one of which incorporates a private right of action.[313] Five states mention biometric identifiers in their broader privacy statutes, but here, too, their reach is severely cabined.[314]

In 2001, Texas became the first state to limit the capture of biometric identifiers.[315] Further amended in 2009 and 2017, the Capture or Use of Biometric Identifier (CUBI) Act incorporates only five PBCs and one BBC, defining "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[316] It says nothing about myriad other PBCs or BBCs

308. *Id.*
309. *Id.*
310. *Id.* at 6–7.
311. *Id.* at 9–12.
312. *Id.* at 10.
313. *See* note 297 and accompanying text.
314. California's is the only such statute that has created a private right of action; even then, the right of action only applies to violations resulting from data breaches. CAITRIONA FITZGERALD, KARA WILLIAMS & R.J. CROSS, ELEC. PRIV. INFO. CTR., THE STATE OF PRIVACY: HOW STATE "PRIVACY" LAWS FAIL TO PROTECT PRIVACY AND WHAT THEY CAN DO BETTER 18, 25 (2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf [https://perma.cc/J7QU-E259].
315. *See* TEX. BUS. & COM. CODE ANN. § 503.001.
316. *Id.* § 503.001(a). The CUBI Act was first amended by § 1 of H. 3186, 81st Leg., Reg. Sess. (Tex. 2009), and then by § 1 of S. 1343, 85th Leg., Reg. Sess. (Tex. 2017). *See* H. 81R-32595, at 1 (Tex.

discussed in Section II.A. It makes it illegal for commercial entities to sell, lease, or otherwise disclose biometric identifiers to any other person outside of narrow circumstances.[317] The law obliges the data holder to store, transmit, and protect the information using the same amount of care that the subject does in storing, transmitting, and protecting "any other confidential information."[318] Data must be destroyed within a year of the date on which it is no longer required for the original purpose for which it was collected, outside of certain exceptions.[319] The law carries a hefty fine: up to $25,000 per violation.[320]

In 2008, Illinois passed the Biometric Information Privacy Act (BIPA).[321] The legislature acknowledged the growing emphasis being placed by industry on biometrics, calling out their use in financial transactions and the use of finger scanning at grocery stores, gas stations, and school cafeterias.[322] Because of the uniqueness of biometric markers, compromised targets had no recourse other than to no longer use biometric-facilitated transactions. As the "full ramifications of biometric technology" were not yet apparent, the legislature determined that "[t]he public welfare, security, and safety" would best "be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[323]

Like Texas, Illinois explicitly limited the statute's applicability to a handful of PBCs, defining "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[324] It excluded certain PBCs and BBCs.[325] BIPA defined "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[326] The statute prohibits any

2009), https://capitol.texas.gov/tlodocs/81R/analysis/pdf/HB03186H.pdf#navpanes=0 [https://perma.cc/UFY4-7HTX]. Note that the 2017 provision excepts voiceprint data retained by financial institutions under 15 U.S.C. § 6809. In March 2023, a separate initiative, the Biometric Data Privacy Act of 2023, was introduced specifically to focus on biometric identifiers and voiceprints. *See* Tex. H. 4705, 88th Leg., Reg. Sess. (Tex. 2023). However, the bill did not survive committee review.

317. Namely, unless the individual consents to disclosure for identification in the case of death, the disclosure completes a financial transaction requested or authorized by the individual, such provision is authorized by either state or federal statute, or the information is disclosed to law enforcement pursuant to a warrant. *See* TEX. BUS. & COM. CODE ANN. § 503.001(c)(1)(A)–(D).

318. *Id.* § 503.001(c)(2).

319. *See id.* § 503.001(c)(3).

320. *Id.* § 503.001(d).

321. 740 ILL. COMP. STAT. 14/1.

322. *See id.* § 14/5(a)–(b).

323. *Id.* § 14/5(f)–(g).

324. *Id.* § 14/10.

325. *See id.* (excluding "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color," as well as organ, tissue, and blood donations, information already captured under the Genetic Information Privacy Act, information obtained in a healthcare system, and any "X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition").

326. *Id.*

private entity from collecting, capturing, purchasing, trading for, or otherwise obtaining a person's biometric identifiers or information unless it (1) informs the subject's legally authorized representative, in writing, that the information is being collected; (2) details the length of time for which it is being collected, stored, and used; and (3) receives a written release authorizing such collection.[327] The law prohibits data holders from selling, leasing, trading, or otherwise profiting from a customer's biometric data; nor are they allowed to disclose the information to others unless the subject consents or disclosure is required by law.[328] Having created a right of action in state circuit court or as a supplemental claim in federal district court, the statute sets a minimum in liquidated damages ($1,000 for negligence and $5,000 for intentional or reckless violation or actual damages, whichever is greater), plus attorney's fees.[329] The law further requires any private entities in possession of biometric identifiers or information to develop a publicly available written policy establishing the retention period, with a maximum period of three years from the individual's last interaction with the privacy entity.[330]

In 2017, the state of Washington introduced biometric legislation. Unlike Texas and Illinois, it defines biometric identifier in a manner that *could* be interpreted to include PBCs and BBCs—although it added a qualifier that the statute only applies when used by way of identification.[331] It thus does not govern the collection of biometric data writ large, much less biomanipulation. The law excludes any "physical or digital photograph, video or audio recording or data generated therefrom," as well as information collected, used, or stored for healthcare, gutting its impact.[332] Washington also focuses on the enrollment process, for which notice alone (and not informed consent) is sufficient.[333] The data can be disclosed to a third party as long as they "contractually promise[]" to use the information in a manner consistent with the notice previously provided.[334] No restrictions apply to biometrics collected for a "security purpose."[335] To the

327. *Id.* § 14/15(b)(1)–(3).

328. *Id.* § 14/15(c)–(d).

329. *Id.* § 14/20(a)(1)–(4).

330. *Id.* § 14/15(a).

331. WASH. REV. CODE § 19.375.010(1) (defining biometric identifiers as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual").

332. *Id.*

333. *Id.* § 19.375.020(1) (prohibiting enrolling "a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose"); *id.* § 19.375.020(3)(b), (c), (d), (f) (stating that whoever enrolls an individual's biometric identifier cannot sell, lease, or otherwise disclose it unless it is necessary for a product or service subscribed to or authorized by the individual, is necessary for a financial transactions, or is required by law or as part of a judicial process).

334. *Id.* § 19.375.020(3)(e).

335. *Id.* §§ 19.375.020(7), .010(8) (defining "[s]ecurity purpose" as "preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person").

extent that industry therefore employs PBCs and BBCs to access their services, the statute explicitly exempts any requirement for them to collect, capture, enroll, analyze, or use individuals' biometric data as outlined in the statute.

Colorado is the most recent state to adopt a biometric statute, which goes into effect July 1, 2025.[336] It defines "biometric identifiers" more broadly than other jurisdictions:

> "Biometric identifier" means data generated by the technological processing, measurement, or analysis of a consumer's biological, physical, or behavioral characteristics, which data can be processed for the purpose of uniquely identifying an individual. "Biometric identifier" includes:
>
> (a) A fingerprint;
>
> (b) A voiceprint;
>
> (c) A scan or record of an eye retina or iris;
>
> (d) A facial map, facial geometry, or facial template; or
>
> (e) *Other unique biological, physical, or behavioral patterns or characteristics.*[337]

The last element ensures that other PBCs and BBCs are captured by the statute, which prohibits the collection or processing of biometric identifiers absent clear, reasonably accessible, and understandable notification to the consumer regarding what information will be obtained, the purpose for which it is being collected, and the length of time it will be retained, as well as whether it will be disseminated consistent with the purpose for which it is being collected.[338] It also requires that the consumer actively consent to any disclosure of the information.[339] Biometric data controllers are required to develop a written policy to establish a retention schedule, provide a protocol for breaches, and ensure the deletion of the underlying information within certain timeframes.[340] Consumers have the right to access their data free of charge and to be provided with certain information, such as the source from which the biometric was collected, the purpose for which it was obtained, and the identity of any third parties with whom it was shared.[341]

---

336. *See HB24-1130, Privacy of Biometric Identifiers & Data*, COLO. GEN. ASSEMBLY, https://leg.colorado.gov/bills/hb24-1130 (last visited Jan. 27, 2025); H.R. 24-1130, 75th Gen. Assemb., Reg. Sess. (Colo. 2024). The General Assembly called attention to the increasing use of biometric identifiers by businesses in their effort to verify their customers' identities, make transactions more efficient, control access to secure areas, and maximize their revenues. *See* Colo. H.R. 24-1130 § 1(1)(a). The legislators also noted increasing public concern about the security of the information, particularly in light of data breaches, as well as misidentification and misclassification accompanying the use of FRT in particular. *See id.* § 1(1)(c), (2)(a).

337. Colo. H.R. 24-1130 § 3(2.4) (emphasis added).

338. *Id.* § 2(4)(a)(II)–(IV).

339. *Id.* § 2(4)(b)(II)(A)–(C).

340. *Id.* § 2(2).

341. *Id.* § 2(5)(a)(I)–(III).

The statute limits the purposes for which an employer can require employees' biometrics.[342] Colorado's biometric statute amends its broader privacy law, the Colorado Privacy Act. Both statutes, however, lack a private right of action. Instead, they are concurrently enforced by the Colorado attorney general and district attorneys who bring suit on behalf of the state or Coloradans.

In the absence of comprehensive federal privacy legislation, some states have picked up the reins, but only five (including Colorado) incorporate biometric identifiers. Each falls short in important ways.

On the one hand, the definitions of "biometric data" in many of these statutes potentially apply to many of the PBCs and BBCs highlighted in Section II.A. Outside of Colorado's amendments (discussed above), the most comprehensive language appears in the California Consumer Privacy Act (CCPA), which defines biometric information as

> an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[343]

Oregon, Texas, and Utah adopted a less comprehensive approach, along with a number of exceptions.[344] Oregon, for instance, excludes photographs, audio and voice recordings, data obtained from such recordings, and facial mapping or geometry, unless obtained "for the purpose of identifying a specific consumer."[345] It therefore does not apply to environmental monitoring or remote capture of biometric data. Texas and Utah similarly exclude photographs and video or audio

342. *Id.* § 2(6).

343. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.140(c).

344. S. 619, 82nd Leg., Reg. Sess. § 1(3)(a) (Or. 2023) (defining "[b]iometric data" as "data generated by automatic measurements of a consumer's biological characteristics, such as the consumer's fingerprint, voiceprint, retinal pattern, iris pattern, or other unique biological characteristics"); TEX. BUS. & COM. CODE ANN. § 541.001(3) (defining "biometric data" as "data generated by automatic measurements of an individual's biological characteristics. The term includes a fingerprint, voiceprint, eye retina or iris, or other unique biological pattern or characteristic that is used to identify a specific individual"); UTAH CODE ANN. § 13-61-101(6)(a) (defining "[b]iometric data" as "data generated by automatic measurements of an individual's unique biological characteristics"); *id.* § 13-61-101(6)(b) (delimiting "[b]iometric data" to information "generated by automatic measurements of an individual's fingerprint, voiceprint, eye retinas, irises, or any other unique biological pattern or characteristic that is used to identify a specific individual").

345. OR. REV. STAT. § 646A.570(3)(b)(C)–(D). The statute defines "[s]ensitive data" as personal data that "[r]eveals a consumer's racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, status as transgender or nonbinary, status as a victim of crime or citizenship or immigration status." *Id.* § 646A.570(18)(a).

recordings, any data generated therefrom, and any information used for certain healthcare treatment, limiting the statutory reach.[346]

These statutes also limit the collection, use, and disclosure of sensitive data.[347] For Colorado, in its broader privacy provisions, this includes not just "[g]enetic or biometric data that may be processed for the purpose of uniquely identifying an individual," but also personal information that reveals "racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or . . . citizenship status."[348] Utah and Oregon have similar provisions, with the notable addition in the latter of an individual's status as transgender or non-binary.[349] Texas also includes certain inferences (i.e., racial or ethnic origin, religious beliefs, mental or physical health diagnosis, and sexuality) as sensitive information.[350] The notice limitations, however, only apply to genetic or biometric information when used for identification.[351] California, in contrast, includes certain kinds of biometric data as personal information but does not include biometric markers writ large in its sensitive information category.[352]

The privacy acts require notice and consent prior to collection of sensitive data.[353] Some states, like Colorado, include a right to opt out of targeted advertising, the sale of personal data, and certain types of profiling.[354] They create a right to access, correct, and delete personal data—an approach potentially relevant to

346. UTAH CODE ANN. § 13-61-101(6)(c)(i)–(v) (excluding from the definition of "[b]iometric data" "physical or digital photograph[s]," "video or audio recording[s]," data generated from either of them, "information captured from a patient in a health care setting," or "information collected, used, or stored for treatment, payment, or health care operations"); TEX. BUS. & COM. CODE ANN. § 541.001(3) (excluding from the definition "a physical or digital photograph or data generated from a physical or digital photograph, a video or audio recording or data generated from a video or audio recording, or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996").

347. *See, e.g.*, CAL. CIV. CODE § 1798.100(a)(1), (e).

348. COLO. REV. STAT. § 6-1-1303(24)(a)–(b).

349. UTAH CODE ANN. § 13-61-101(32)(a)(i)–(ii) (defining "[s]ensitive data" as personal data that reveals race or ethnic origin, religious beliefs, and sexual orientation as well as "the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual"); S. 619, 82nd Leg., Reg. Sess. § 1(17)(a) (Or. 2023) (including gender identity in the definition of sensitive data).

350. TEX. BUS. & COM. CODE ANN. § 541.001(29)(A).

351. *Id.* § 541.001(29)(B).

352. CAL. CIV. CODE § 1798.140(v)(1)(A), (ae)(1)(D)–(F) (including "racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership" along with "genetic data," but considering biometric data to be part of personal (not sensitive personal) information).

353. CAL. CIV. CODE § 1798.130 (notice, disclosure, correction, and deletion requirements); COLO. REV. STAT. § 6-1-1308 (notice and consent); *id.* § 6-1-716(1)(a) (defining "[b]iometric data" as "unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account"); *id.* § 6-1-1303(24)(b) (defining "[s]ensitive data" in part as "[g]enetic or biometric data that may be processed for the purpose of uniquely identifying an individual"); UTAH CODE ANN. § 13-61-302(1) (notice requirements); *id.* § 13-61-101(9) (defining "[c]onsent" as "an affirmative act by a consumer that unambiguously indicates the consumer's voluntary and informed agreement to allow a person to process personal data related to the consumer").

354. COLO. REV. STAT. § 6-1-1306(1)(a)(I)(A)–(C).

ensuring that companies delete biometric data once collected.[355] Others, like Texas, do not restrict companies from collecting, analyzing, or selling anything; the law merely requires notice to the customer.[356]

It is too early to know the impact the broader privacy laws will have on biometric collection, not only because of the exceptions noted above and their recent entry into force, but because all but California's lack a private right of action for the unlawful collection of biometric data. The remaining statutes rely on state officials for enforcement.[357] In the meantime, to the extent that the PBC and BBC subcategories are covered, it tends to be just in relation to identification—which, as noted in Section I.B, is far from the only function performed by biometric collection. The laws, moreover, only apply to commercial entities—not to individuals, groups, foreign governments, or others who may engage in biomanipulation.

IV. RISKS TO DEMOCRATIC STRUCTURES

The rapid expansion of systems enabling the collection of PBCs and BBCs, the advent of biomanipulation, and the dearth of federal or state statutory restrictions mark a new era which carries significant risks. While it is not the intent of this Article to analyze each, this Section addresses one of the most serious: the shift in power heralded by these technologies and its consequent impact on democratic governance. Biomanipulation can be used to undermine political authority. It can be employed by private entities, government officials, and foreign actors to exploit individuals and communities. It can be used to deny targets certain privileges and rights. And although we often think in terms of coercing individuals to act in certain ways, it can also be used to prevent individuals from being able to act by isolating, ostracizing, or excluding them. The cost is borne in individual autonomy.

A. POLITICAL AUTHORITY

The political economist Max Weber considered the continuous operation of a compulsory political association "a 'state' insofar as its administrative staff successfully upholds the claim to the *monopoly* of the *legitimate* use of physical force in the enforcement of its order."[358] It is not that a government has the freedom to employ violence or coercion and can do so without restriction or consequence, but that citizens' belief in the government's ability to do so and their duty

355. *Id.* § 6-1-1302(c)(II)(A) (noting that the legislation "[p]rovides consumers the right to access, correct, and delete personal data and the right to opt out not only of the sale of personal data but also of the collection and use of personal data"); *id.* § 6-1-1306(1)(a)–(e) (incorporating the right to opt out, access, correct, delete, and transfer data); CAL. CIV. CODE § 1798.105(a) (right to delete personal information); *id.* § 1798.106(a) (right to correct inaccurate personal information); *id.* § 1798.120(a) (right to opt out of sale or sharing of personal information); *id.* § 1798.121(a) (right to limit use and disclosure of sensitive personal information).

356. TEX. BUS. & COM. CODE ANN. § 541.102(a).

357. *See, e.g.*, UTAH CODE ANN. § 13-61-402 (granting the attorney general exclusive enforcement authority).

358. MAX WEBER, ECONOMY AND SOCIETY: AN OUTLINE OF INTERPRETIVE SOCIOLOGY 54 (Guenther Roth et al. eds. & trans., Univ. of Cal. Press 1978) (1921) (emphasis in original).

to obey amounts to an essential characteristic of what it means to be a state.[359] While a careful exegesis of the relationship between Weberian thought and the phenomena that mark biomanipulation would take considerably more ink, the insight that Weber's construction brings is the extent to which biomanipulation potentially undermines statehood. The ability of private and public actors to use citizens' biological processes to alter their beliefs, desires, emotions, and actions (or non-actions) poses a challenge to the political structure.

Imagine, for instance, a circumstance in which a private entity decided that it would prevent individuals from leaving their home. The basic premise could be merely that by spending more time in a VR world, companies could obtain ever-deeper levels of information about the users. To keep them online, corporations could play to targets' cerebral pleasure centers, delivering them content which makes them happy, as ascertained from BBCs. Alternatively, they could exploit their fears, building increased anxiety about the world outside their doors. The delivery device could be a gaming platform, shopping, music concerts, sporting events, or any number of contexts. To the extent that a system exploits innate biological characteristics and processes, a target may be both unaware and face a high barrier to being able to resist. Third parties essentially confining targets to their home would thus be exercising power at least bordering on coercion, using the target's biological processes to restrict their liberty.

Granted, there is a distinction to be drawn between biomanipulation and coercion, in that the latter has typically been thought of as the constriction of acceptable options to just one. Take, for instance, a futuristic chip which could be inserted into the brain that controls an individual's arms and legs in a way that the conscious self does not want. In this case, the controller bypasses the target's will, instead of using or working through it. Biomanipulation presents a mixed case in that it evinces characteristics of manipulation and coercion, as well as direct control, wherein choice is circumscribed or significantly narrowed, challenging traditional concepts of state-monopolized coercion—indeed, going well beyond it by capturing the essence of individual autonomy.

It is not just the corporations, however, which could wield such power. Without legal restrictions, biometric information could be collected by, obtained, given to, leased, or sold to other countries or nonstate actors—including adversaries, which could then use the data to undermine U.S. government power. This scenario is not far-fetched. If anything, it is the next logical step for ways in which adversaries already have proceeded.

Throughout the Cold War, for example, Soviet active measures sought to exacerbate racial, religious, and ethnic tensions within the United States.[360] The KGB

359. The political community simultaneously evinces a belief ("legitimitätsglaube") not only that the government has a monopoly on coercion, but that such exercise must be obeyed. *See* MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 382 (A. M. Henderson & Talcott Parsons trans., 1947); Fabienne Peter, *Political Legitimacy*, STAN. ENCYC. OF PHIL. (Dec. 11, 2023), https://plato.stanford.edu/entries/legitimacy/ [https://perma.cc/N4RV-W72P].

360. *See* THOMAS RID, ACTIVE MEASURES: THE SECRET HISTORY OF DISINFORMATION AND POLITICAL WARFARE 134 (2020). As Dennis Kux notes, "the terms 'active measures' and

posed as civil rights organizations, ordinary citizens, white supremacists, and the Ku Klux Klan to undermine U.S. authority at home and abroad.[361] In the early twenty-first century, Russia again picked up active measures, this time online, employing false scientific reports, fraudulent news, and fictitious personalities to sway Americans' thoughts and actions.[362] Russia's goals included "[u]ndermin[ing] citizen confidence in democratic governance; foment[ing] and exacerbat[ing] divisive political fractures; [e]rod[ing] trust between citizens and elected officials . . .; [and] [c]reat[ing] general distrust or confusion over information sources."[363] The country deployed online sockpuppets, trolls, botnets, and advertisements to exploit societal and political tensions and reshape how Americans viewed political issues, candidates, and government activity.[364]

Congress and the Executive Branch have sounded alarm bells about Russia's active measures campaign.[365] In 2019, the U.S. Senate Select Committee on

'disinformation' are both imported directly from the Soviet intelligence lexicon," the former being an English translation of "aktivnyye meropriyatiya," the name of the KGB unit charged with implementing "dezinformatsiya." Dennis Kux, *Soviet Active Measures and Disinformation: Overview and Assessment*, 15 U.S. ARMY WAR COLL. Q. 19, 19 (1985). In the Soviet context, the concept spanned a variety of practices, from disinformation operations and political influence to managing front groups and foreign communist parties. *Id.* at 19, 21, 23, 26. In this Article, I use the term "active measures" to describe the effort to undermine U.S. political legitimacy both domestically and abroad and to manipulate Americans' beliefs, desires, emotions, and knowledge through online behavior.

361. *See, e.g.*, Fred Barbash, *U.S. Ties 'Klan' Olympic Hate Mail to KGB*, WASH. POST (Aug. 6, 1984, 8:00 PM), https://www.washingtonpost.com/archive/politics/1984/08/07/us-ties-klan-olympic-hate-mail-to-kgb/80918fe8-fcf0-46cf-bb58-726ee46d8ce9/; OLEG KALUGIN, THE FIRST DIRECTORATE: MY 32 YEARS IN INTELLIGENCE AND ESPIONAGE AGAINST THE WEST 54 (1994); Kux, *supra* note 360, at 26; Philip Ewing, *Russians Targeted U.S. Racial Divisions Long Before 2016 and Black Lives Matter*, NPR (Oct. 30, 2017, 5:00 AM), https://www.npr.org/2017/10/30/560042987/russians-targeted-u-s-racial-divisions-long-before-2016-and-black-lives-matter [https://perma.cc/RV3X-UGCZ].

362. *See Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Hearings Before the S. Select Comm. on Intel.*, 115th Cong. 2–3 (2017) (statement of Thomas Rid, Professor of Security Studies, King's College London); *see also* PETE EARLEY, COMRADE J: THE UNTOLD SECRETS OF RUSSIA'S MASTER SPY IN AMERICA AFTER THE END OF THE COLD WAR 193–94 (2007) (detailing SVR officers' online activities).

363. Andrew Weisburd, Clint Watts & Jim Berger, *Trolling for Trump: How Russia Is Trying to Destroy Our Democracy*, WAR ON THE ROCKS (Nov. 6, 2016), https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/ [https://perma.cc/P3RH-A94C].

364. *See* S. SELECT COMM. ON INTEL., 116TH CONG., REPORT ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS 6, 18–20, 22–23 (Comm. Print 2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf [https://perma.cc/B7V9-RTF6]; Karen Hao, *Troll Farms Reached 140 Million Americans a Month on Facebook Before 2020 Election, Internal Report Shows*, MIT TECH. REV. (Sept. 16, 2021) https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/ [https://perma.cc/MB5Y-LWEF]; *Social Media Influence in the 2016 U.S. Election, Hearing Before the Select Comm. on Intel.*, 115th Cong. 5, 50 (2017) [hereinafter *Social Media Hearing*]; Kux, *supra* note 360, at 19, 23; MAX BERGMANN & CAROLYN KENNEY, CTR. FOR AM. PROGRESS, WAR BY OTHER MEANS: RUSSIAN ACTIVE MEASURES AND THE WEAPONIZATION OF INFORMATION 14–16 (2017).

365. *But see* Christopher A. Bail et al., *Assessing the Russian Internet Research Agency's Impact on the Political Attitudes and Behaviors of American Twitter Users in Late 2017*, 117 PROC. NAT'L ACAD. SCIS. 243, 243, 245–46 (2020) (merging longitudinal data on 1,239 Republicans and Democrats from late 2017 with data on Twitter accounts run by the IRA and concluding that interactions with Kremlin-backed trolls were most common among individuals who were frequent Twitter users, and had strong

Intelligence (SSCI) determined that, at the Kremlin's direction, during the 2016 presidential election the Internet Research Agency (IRA) engaged in a disinformation campaign "to attract and exploit a wide range of real people."[366] As Pavel Zolotarev, a retired major general in the Russian Army, conveyed, Russia "had come to the conclusion . . . that manipulation in the information sphere [was] a very effective tool."[367] According to U.S. experts, Russian influence operators targeted three groups: "useful idiots," referring to "unwitting American[s]" who could be exploited to "further amplify" Russian propaganda, unbeknownst to them; "fellow travelers," who were "ideologically sympathetic to Russia's anti-EU, anti-NATO and anti-immigration ideology"; and "agent provocateurs," who were "manipulated . . . to commit illegal, surreptitious acts" on behalf of the Russian government.[368]

Russia built its strategy on corporate power. With billions of monthly users, Facebook offered an ideal delivery mechanism: as of 2016, 191.3 million people in the United States had accounts.[369] Some 1.18 billion active users globally visited the site on a daily basis.[370] Russia bought access to users via targeted advertisements and false news reports, manipulated algorithms, and hacked and leaked protected information with the aim of polarizing the U.S. electorate.[371]

While the IRA initially imitated individuals, by early 2015 it had created organizations on all sides of the social and political spectrum. It launched conservative groups with names like "Being Patriotic," "Stop All Immigrants," "Secured Borders," and "Tea Party News"; Black social justice groups such as "Black Matters," "Blactivist," and "Don't Shoot Us"; LGBTQ entities like "LGBT United"; as well as religious organizations such as "United Muslims of America."[372] By shaping messages to target communities' predispositions, the campaign managed to distribute its message: on Facebook alone, Russia reached

social media echo chambers and a high interest in politics, and that therefore the Russian interference did not necessarily change their political views).

366. S. SELECT COMM. ON INTEL., *supra* note 364, at 20, 22–23; ROBERT S. MUELLER, III, U.S. DOJ, 1 REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14, 19, 22 (2019) [hereinafter MUELLER REPORT], https://www.justice.gov/archives/sco/file/1373816/dl [https://perma.cc/2KDA-T579].

367. S. SELECT COMM. ON INTEL., *supra* note 364, at 13.

368. *Cyber-Enabled Information Operations, Hearing Before the U.S. S. Armed Servs. Comm.*, 115th Cong. 3–4 (2017) (statement of Clint Watts, Robert A. Fox Fellow, Foreign Policy Research Institute & Senior Fellow, Center for Cyber and Homeland Security, the George Washington University), *quoted and cited in* S. SELECT COMM. ON INTEL., *supra* note 364, at 20; *see also* CLINT WATTS, MESSING WITH THE ENEMY: SURVIVING IN A SOCIAL MEDIA WORLD OF HACKERS, TERRORISTS, RUSSIANS, AND FAKE NEWS 91 (2019).

369. *Leading Countries Based on Number of Facebook Users as of May 2016*, STATISTA, https://web.archive.org/web/20161220185723/https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/ [https://perma.cc/59EF-2ED2] (last visited Jan. 3, 2025).

370. *Number of Daily Active Facebook Users Worldwide as of 3rd Quarter 2016 (in Millions)*, STATISTA, https://web.archive.org/web/20170128220621/https://www.statista.com/statistics/346167/facebook-global-dau/(last visited Jan. 3, 2025).

371. *See* S. SELECT COMM. ON INTEL., *supra* note 364, at 3, 57, 63 77.

372. MUELLER REPORT, *supra* note 366, at 24–25.

126 million people.[373] On Instagram, it reached another 16 million, and it potentially reached an additional 1.4 million via Twitter.[374] Pages like "Don't Shoot Us" attracted over 250,000 followers, while "Being Patriotic" attracted another 200,000, giving Russia the means to shape Americans' thinking.[375]

The sites went beyond online behavior, seeking to promote and encourage citizens to organize and attend rallies in the physical world—actions flamed by further delivery of false advertisements, news, and posts.[376] During the 2016 election, Russia manipulated site followers to engage in marches and protests.[377] Robert Mueller, the former Director of the Federal Bureau of Investigation appointed as special counsel for the investigation into Russian interference in the 2016 presidential election, described the process:

> First, the IRA used one of its preexisting social media personas (Facebook groups and Twitter accounts, for example) to announce and promote the event. The IRA then sent a large number of direct messages to followers of its social media account asking them to attend the event. From those who responded with interest in attending, the IRA then sought a U.S. person to serve as the event's coordinator. In most cases, the IRA account operator would tell the U.S. person that they personally could not attend the event due to some preexisting conflict or because they were somewhere else in the United States. The IRA then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator. After the event, the IRA posted videos and photographs of the event to the IRA's social media accounts.[378]

Dozens of rallies, some drawing hundreds of participants, unfolded in this way.[379] Agents targeted U.S. persons who could most effectively help them reach their goals and then looked for ways to manipulate them directly. On Twitter, for instance, the IRA leveraged users' information to message them privately and convince them to take certain positions and actions.[380] The range of topics pursued included: Black Lives Matter, Blue Lives Matter, pro-Second Amendment, pro- and anti-political candidates, Confederate history, Christian culture, LGBTQ+ culture, feminism, immigration, and states' culture and history as set against the federal government.[381]

---

373. *See Social Media Hearing*, *supra* note 364, at 13.

374. *Id*. at 58 (statement of Colin Stretch, General Counsel of Facebook, Inc. (now Meta)); *Update on Twitter's Review of the 2016 US Election*, X: BLOG (Jan. 31, 2018), https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html [https://perma.cc/UJ5M-VML2].

375. MUELLER REPORT, *supra* note 366, at 26.

376. *Id*. at 29.

377. *Id*.

378. *Id*. (footnotes omitted).

379. *Id*.

380. *See id*. at 27–29, 31–32.

381. RENEE DIRESTA, KRIS SHAFFER, BECKY RUPPEL, DAVID SULLIVAN, ROBERT MATNEY, RYAN FOX, JONATHAN ALBRIGHT & BEN JOHNSON, THE TACTICS & TROPES OF THE INTERNET RESEARCH AGENCY, S. DOC. NO. 10-2019, at 11 (2019).

A campaign based on biomanipulation could be detrimental. Tied to individuals' *biological* processes and not just demographic or profile data (such as whether individuals held a military or law enforcement rank, or appeared sympathetic with liberal concerns—grounds on which the IRA organized pro- and anti-Beyoncé rallies, for instance), biomanipulation would allow for an even more individualized approach.[382] Because of this particularization, it (ostensibly) would be more effective, more binding, swifter, and harder to counter, particularly to the extent that targets themselves are unaware of the manipulation. It is not that humans are merely automatons, lacking any agency or authorship of their actions. In this more individualized and sophisticated format, it could be exponentially more difficult to detect third-party efforts to target and exploit individuals' vulnerabilities.

It is thus not just *corporate* exercise of coercive power which undermines the government's monopoly on physical force, but other states', as well as non-state actors', exercise of *the same power* which erodes the state itself. To the extent that it could be exercised by adversaries, regardless of whether it is Russia, ISIS, or a narco-terrorist drug cartel, serious implications for U.S. national security present—to say nothing of the societal impact of the way in which such power could be leveraged.

B. AUTONOMY

In conjunction with the power imbalance, the potential for exploitation and the absence of a backstop presents a profound challenge to individual autonomy. Whether exercised by corporate entities, private actors, foreign entities, or the U.S. government, biomanipulation cabins a target's ability to live their life according to motives and reasoning taken as their own and not the product of external forces.[383]

The concept of autonomy, although relatively recent, grows out of the western philosophical tradition which grounds the political legitimacy of the state itself in the free exercise of the will of the sovereign.[384] In a democratic state, self-governance requires that individuals be free to develop their own ideas and to act consistent with their authentic selves without undue manipulation or interference from others or imposition upon the same. Autonomy similarly lies at the heart of Kant's conception of practical reason, which plays a critical role in the pursuit of knowledge.[385] What we "know" is comprised of empirical elements and judgment.

---

382. *See* Olivia Solon & Julia Carrie Wong, *#BlueLivesMatter and Beyoncé: Russian Facebook Ads Hit Hot-Button US Issues*, GUARDIAN (May 10, 2018, 4:57 PM), https://www.theguardian.com/us-news/2018/may/10/russia-facebook-ads-us-elections-congress [https://perma.cc/7QWG-5RXV]; *see also* '258 Patent Application, *supra* note 291, at para. [0039] (creating an individualized VR experience utilizing target's biometric data).

383. *See* John Christman, *Autonomy in Moral and Political Philosophy*, STAN. ENCYC. OF PHIL. (June 29, 2020), https://plato.stanford.edu/archives/fall2020/entries/autonomy-moral/ [https://perma.cc/4QMV-MNQ7].

384. *See* J.B. SCHNEEWIND, THE INVENTION OF AUTONOMY: A HISTORY OF MODERN MORAL PHILOSOPHY 483 (1998) (discussing the evolution of the concept in the context of Kantian theory).

385. IMMANUEL KANT, CRITIQUE OF PURE REASON 650–51 (Paul Guyer & Allen W. Wood eds. & trans., Cambridge Univ. Press 1998) (1781).

In this formulation, the senses (because they lack judgment) do not err, whilst cognitive processes may.[386] Thus, we see a straw in a glass and it appears to bend at the water line, but our conclusion that it does so depends upon an error in judgment—not that the contours of the straw do not visibly, suddenly shift. Kant claims that "error is effected only through the unnoticed influence of sensibility on understanding, through which it happens that the subjective grounds of the judgment join with the objective ones."[387] External reasoning, what Kant calls "heteronomy," cannot substitute itself for the judgment of the individual; instead, it must be autonomous.[388] Scholars have looked to this construct as a positive sense of freedom: "constrain[t] by norms rather than merely by causes."[389]

Modernist humanism picks up on the role of autonomy as more than just self-governance: it serves as a basic moral and political value.[390] As John Christman puts it, "to be autonomous is to govern oneself, to be directed by considerations, desires, conditions, and characteristics that are not simply imposed externally upon one, but are part of what can somehow be considered one's authentic self."[391] Autonomy can be distinguished from freedom in that the latter relates to an ability not just to act without internal or external constraints, but also to give effect to one's desires.[392] Therefore, the shaping of an individual's desires—such as through biomanipulation—interferes with individual autonomy. Actions by a third party which either use or act on those desires constitute an external force on the individual.

If an individual, for instance, were to try to manipulate a partner by playing to their known desires to get the partner to concede to a particular course of action, we would consider that manipulative. To the extent that the target's internal desires are accessed via biometrics, then we would be in the realm of biomanipulation. What makes this different from the former case is that the third party need have no personal relationship whatsoever with the target. Remote access, environmental monitoring, and other technologies make it possible to collect insight from afar. In the former case, the partner would have, assumedly, confided in the other person about their desires. In the latter, there has been no such disclosure. It thus undermines autonomy to a greater degree, in terms of the process of revelation and the extent to which such desires can then be shaped and used to accomplish different ends. A similar argument would mark belief and emotion.

386. *Id*. at 384–85.

387. *Id*. at 385.

388. *See* Garrath Williams, *Kant's Account of Reason*, STAN. ENCYC. OF PHIL. (Jan. 4, 2023), https://plato.stanford.edu/entries/kant-reason/ [https://perma.cc/5PXQ-NY55].

389. Robert Brandom, *Freedom and Constraint by Norms*, 16 AM. PHIL. Q. 187, 187 (1979).

390. *See* Christman, *supra* note 383.

391. *Id.*

392. *Id.* (first citing ISAIAH BERLIN, FOUR ESSAYS ON LIBERTY 134 (1969); then citing LAWRENCE CROCKER, POSITIVE LIBERTY: AN ESSAY IN NORMATIVE POLITICAL PHILOSOPHY 82–101 (1980); and then citing Gerald C. McCallum, Jr., *Negative and Positive Freedom*, 76 PHIL. REV. 312, 314 (1967)).

Such autonomy is in conflict with the paternalism advocated by Thaler and Sunstein.[393] Attempting to justify biomanipulation on the grounds that it is helpful for the consumer, voter, student, professional, or member of the public does nothing to address its impact on individual autonomy. And here the question about knowledge of the collection of biometric information, which Susser et al. fail to address, matters.[394] For instance, to what extent has the target specifically requested that the third party collect biometric data? Is it the third party wielding the information? Is the information being used as requested? How aware is the target of the stimulus?[395] To paraphrase Joseph Raz, to be an author of one's own life, an individual's choices must be free and independent.[396] Biomanipulation deprives the target of that freedom.

To some extent the European Union, in contrast to the United States, has attempted to get at this issue through the lens of regulating AI.[397] In 2023, the EU passed legislation which prohibits the creation of biometric categorization systems employing sensitive characteristics, such as political, religious, or philosophical beliefs, sexual orientation, or race.[398] It outlawed untargeted scraping of facial images either from the Internet or CCTV footage to create FRT databases, as well as the use of emotion recognition either in the workplace or educational institutions.[399] The law prohibits social scoring grounded in social behavior or personal characteristics.[400]

European efforts leave gaps. While the statute forbids using AI to manipulate human behavior to circumvent free will, for instance, it leaves open the possibility of certain forms of biomanipulation, such as where individuals believe it is in their best interests to conform. Say, for instance, that a woman believes the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* deprived her of her reproductive rights.[401] Let's assume, too, that a splinter group from the National Organization for Women (NOW) decides direct action is the only way to proceed. Having bought access to women's biometric data, NOW

393. *See* Thaler & Sunstein, *supra* note 93, at 175.

394. *See* Susser et al., *supra* note 15.

395. *See id.* at 4.

396. RAZ, *supra* note 56, at 372–73 ("If a person is to be maker or author of his own life then he must have the mental abilities to form intentions of a sufficiently complex kind, and plan their execution. These include minimum rationality, the ability to comprehend the means required to realize his goals, the mental faculties necessary to plan actions, etc. For a person to enjoy an autonomous life he must actually use these faculties to choose what life to have. There must in other words be adequate options available for him to choose from. Finally, his choice must be free from coercion and manipulation by others, he must be independent.").

397. *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at 1, COM (2021) 206 final (Apr. 21, 2021); European Parliament Press Release, Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI (Sept. 12, 2023, 12:04 AM) [https://perma.cc/G7MT-DRSY] [hereinafter EU AI Act].

398. EU AI Act, *supra* note 397.

399. *Id.*

400. *Id.*

401. *See* 597 U.S. 215 (2022).

can analyze the depth of emotion individuals evince whenever confronted by stimuli related to *Dobbs* or *Roe v. Wade* or similar information. Bombarded by articles, newsfeeds, advertisements, and images that reflect the target's beliefs, as well as media meant to increase fear associated with others controlling her body, that woman, and others similarly situated, may be directed to join a protest. Even if the action is in her own interests and consistent with her views, her will has been captured in some sense by third-party access to her biometric data.

The EU regulation leaves open the question of how to even think about free will in the context of new and emerging technologies. At what point are we free to act on stimuli when we are inherently unfree (under the current statutory provisions) even to set the bounds of where, when, and how information is delivered to us? Increasing attention is being paid to algorithms in this regard. This is one of the particular virtues of work by Professors Ryan Calo, Julie Cohen, and others.[402] In a world of big data and 24/7/60/60 consumer access, individuals have lost the ability to mediate not just their social boundaries, but their access to information about themselves and the world they inhabit.

The EU regulation prohibits the use of AI to exploit vulnerabilities tied to individuals' ages, disabilities, or social or economic situations. But it says nothing about vulnerabilities tied to an individual's beliefs, desires, or emotions—much less physiological or behavioral biometrics, all of which provide the centerpiece for biomanipulation. Like many of the other provisions in the statute, while these steps are welcome, they do not address myriad other vulnerabilities that can be exploited as part of biomanipulation.

To the extent that biometrics are merely billed as a way for consumers to verify their identity (and thus access devices or private information), targets may be unaware of what is being collected—much less what information it reveals or what can be inferred from it. They may not know whether (or not) the company shares the information or with whom, whether it has been sold and entered into a data broker stream, or how third parties then use it. The opacity extends to combined data: what is being used or what insights have been gleaned. Nor will targets be aware of how they are subsequently being manipulated—is it via music, colors, social media posts, changes in their online gaming experiences, or ads that pop up next to their email? Is it through family members, friends, or enemies? The opacity of the entire enterprise makes it virtually impossible for targets to ascribe responsibility.

The remote nature of collection further obscures the ability of users to know what is being obtained, much less how the feedback loop is being refined. And it

402. *See* Calo, *supra* note 15, at 1004 (observing that companies use compiled and stored information to "run complex algorithms to convert mere behavior into insight (and value)"); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 75 (2019) ("[N]ew political and epistemological dilemmas flow . . . from abundance and algorithmic intermediation. The problem is not scarcity but rather the need for new ways of cutting through the clutter, and the re-siting of power within platforms, databases, and algorithms means that meaning is easily manipulated.").

is not just users but non-users in the proximity, who similarly find themselves the target, making it irrelevant whether they decide to purchase the initial corporation's product. People who visit a friend's home which just happens to have automated home assistants do not themselves have to buy the device—making their subsequent decision whether or not to purchase products or services from the company irrelevant. The corporation can collect their biometric data regardless, with the voice signature or facial geometry or other biometric marker serving as the anchor to glean insight into the individual. Correlation becomes a feature, allowing for continued targeting without the individual ever purchasing anything. The absence of checks provides for the expansion of third party power, eroding individual autonomy.

C. DISTRACTION AND EXPLOITATION

While direct attacks represent primary ways in which the liberal, democratic design can be undermined, a secondary impact, which can be labelled "distraction," can also operate to the detriment of the democratic state. The basic concern is that by manipulating citizens, corporate entities—or foreign governments or non-state actors—can use the power to direct the targets' interests away from important matters.

This, in fact, was one of the findings of researchers at Oxford University who undertook one of the first major studies of known IRA accounts, determining that Russia "sought to divert [African Americans'] political energy away from established institutions by preying on anger with structural inequalities faced . . ., including police violence, poverty, and disproportionate levels of incarceration."[403] The IRA sought to impress upon their targets that the best way to advance their cause and to express disapproval was to boycott the elections.[404] The approach attacked the liberal, democratic tenets of the state.

Exploitation also can take the form of selectively or publicly revealing the information obtained. There are innumerable ways in which inferences from BBCs can be used to the advantage of adversaries. Once again, this has already occurred in regard to less sensitive data.

As part of the Russian active measures campaign in 2016, for instance, Russian military intelligence (the GRU), like the IRA, undertook covert operations which ranged from stealing information to leaking and laundering it.[405] The first time it became public was two years after the election, when Facebook's former General Counsel, Colin Stretch, disclosed to SSCI that the GRU had been operating on its platforms.[406] "APT28," an organization linked by the U.S. intelligence community to the GRU, created fake personas to enable Russia "to seed stolen information to

403. PHILIP N. HOWARD ET AL., COMPUTATIONAL PROPAGANDA RSCH. PROJECT, THE IRA, SOCIAL MEDIA AND POLITICAL POLARIZATION IN THE UNITED STATES, 2012–2018, at 19 (2018), https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf [https://perma.cc/BMD9-KWFJ].

404. *Id.*

405. S. SELECT COMM. ON INTEL., *supra* note 364, at 24, 36.

406. *Social Media Hearing*, *supra* note 364, at 13.

journalists."[407] Two years later, a Grand Jury Indictment issued by DOJ's Special Counsel appointed to look into Russian interference in the elections detailed how eleven GRU operatives hacked computers and leaked stolen material.[408] Amongst their targets were the Democratic Congressional Campaign Committee and the Democratic National Committee.[409] The GRU monitored their computers, implanted malicious code, and stole documents. It then released certain documents to cast aspersions on both the organizations and individuals working for them, as well as on candidate Hillary Clinton.[410] By making private information public, the network could be disrupted. The GRU used fictitious accounts on Facebook and Twitter to disseminate it, with the documents eventually making their way to Wikileaks for publication.[411] A number of individuals, as a consequence, were forced to resign.

The 50,000 documents eventually released by Wikileaks represent official correspondence within and between political organizations. The type of information at stake in biomanipulation is far more invasive, with substance ranging from healthcare, religious beliefs, and sexual preferences to how individuals' minds work, emotional vulnerabilities, and fears. That so few, if any, limits are currently placed on the collection, analysis, and use of PBCs and BBCs, much less biomanipulation, should give us pause.

CONCLUSION

In 2022, computer scientist Louis Rosenberg, founder of Unanimous AI, labelled the metaverse "the most dangerous tool of persuasion that humanity will . . . ever create[]."[412] He decried its evolution:

> Metaverse platforms will be able to track where you go, what you do, where you look and how long your gaze lingers, your gait; they'll look at your posture and be able to infer your level of interest. They'll monitor your facial expressions, vocal inflections, vital signs, blood pressure, heart rate, blood flow patterns on your face.[413]

If anything, Rosenberg did not go far enough. It is not just in the metaverse that such collection is possible.

Over the past twenty years, the rapid expansion of PBCs and BBCs have catapulted the physical and VR worlds into the realm of biomanipulation. It is about to get worse: the shift from close-environment to open-environment ML will

407. *Id.* at 12 (response to questions for the record, Colin Stretch, General Counsel of Facebook, Inc. (now Meta)).

408. Indictment at 2, United States v. Netyksho, 18-cr-00215 (D.D.C. July 13, 2018).

409. *Id.*

410. *Id.* at 13–15.

411. *Id.* at 14–17; MUELLER REPORT, *supra* note 366, at 44.

412. Derek Robertson, *'The Most Dangerous Tool of Persuasion,'* POLITICO (Sept. 14, 2022, 4:00 PM), https://www.politico.com/newsletters/digital-future-daily/2022/09/14/metaverse-most-dangerous-tool-persuasion-00056681.

413. *Id.*

accelerate analytical capabilities.[414] The feedback loop matters. While catastrophic forgetting is possible where a deep neural network is only fed new data (rather than being reminded of all data received), emerging techniques train systems to give the appropriate weight to data, regardless of when it is received, isolating anomalies and integrating new classes of information. Soon systems will be able to identify classes of anomalies, thereby integrating information more effectively. Monitored over time, as long as targets' outlying data can be isolated and explained, and the known classes further developed, the ability of entities to engage in biomanipulation will only expand. As of right now, there is no federal backstop in place, and the few states that have attempted to move in this direction have fallen woefully short. What we are witnessing is something different in kind, not degree, from what has come before. The risks could not be more serious as we enter an era of biomanipulation.

414. *See* Zhi-Hua Zhou, *Open-Environment Machine Learning*, NAT'L SCI. REV., July 2022, at 1, 1.