Macalester College
DigitalCommons@Macalester College

International Studies Honors Projects | International Studies Department

Spring 4-2017

Defining Biometrics: Toward a Transnational Ethic of Personal Information

Nicola Morrow
Macalester College, nmorrow2695@gmail.com

Follow this and additional works at: http://digitalcommons.macalester.edu/intlstudies_honors

 Part of the Ethics and Political Philosophy Commons, International and Area Studies Commons, International Relations Commons, Internet Law Commons, and the Science and Technology Law Commons

Recommended Citation
Morrow, Nicola, "Defining Biometrics: Toward a Transnational Ethic of Personal Information" (2017). *International Studies Honors Projects*. 26.
http://digitalcommons.macalester.edu/intlstudies_honors/26

This Honors Project is brought to you for free and open access by the International Studies Department at DigitalCommons@Macalester College. It has been accepted for inclusion in International Studies Honors Projects by an authorized administrator of DigitalCommons@Macalester College. For more information, please contact scholarpub@macalester.edu.

Defining Biometrics

Defining Biometrics
Toward a Transnational Ethic of Personal Information

Nicola Morrow

Honors Thesis
Presented to the Department of International Studies
Macalester College
Saint Paul, MN, USA
Faculty Advisor: Dr. Samuel Asarnow
April 19th, 2017

Abstract

Innovations in biotechnology, computer science, and engineering throughout the late 20th and early 21st centuries dramatically expanded possible modes of data-based surveillance and personal identification. More specifically, new technologies facilitated enormous growth in the biometrics sector. The response to the explosion of biometric technologies was two-fold. While intelligence agencies, militaries, and multinational corporations embraced new opportunities to fortify and expand security measures, many individuals objected to what they perceived as serious threats to privacy and bodily autonomy. These reactions spurred both further technological innovation, and a simultaneous proliferation of hastily drafted policies, laws, and regulations governing the collection, use, and sharing of biometric data. In this paper, I argue that these policies are predicated on a fundamental misunderstanding of the nature of biometric information. Definitions of biometrics presume that "biologicalness" is binary. These definitions also imply, for a number of reasons, that biometric information is more dangerous than other kinds of personal information, therefore requiring stricter regulation. I propose an alternative explanation of biometrics, situating biometric information on a larger spectrum of personal information, rather than in a discrete category of its own. This revised definition of biometrics is necessary to effectively regulate personal information, particularly as the trend of rapid technological growth and change continues. I focus, in particular, on the implications of these findings in a transnational context, where transmission of personal information is largely unregulated, and has significant impact on international relations, security, and individual privacy.

To Gaga and Baba—for embodying boundless joy in the project of learning, for showing me the world, and for loving me deeply. I am infinitely lucky to be your granddaughter.

Acknowledgements

First and foremost, I would like to thank my thesis advisor, Sam Asarnow. You were generous with your enthusiasm, your sharp commentary, and your humor. You pushed me when I needed motivation, guided me when I needed direction, and reassured me when I felt lost and exhausted. I am thankful for the many hours I spent in your office this year; I always left feeling more excited about my work and more confident in my ability to do a good job. You are the reason that I love philosophy, and for that I will be forever grateful.

I would also like to thank the other members of my thesis committee, Christy Hanson and Martin Gunderson. Christy, you have been a mentor and friend to me throughout my time at Macalester. Your dedication to your professional work, your students, and your family is an inspiration. Thank you for your guidance. Professor Gunderson, thank you for graciously agreeing to share your significant expertise in bioethics. It is a privilege to have you on my thesis committee.

I am incredibly grateful to my parents. Throughout this year—and always—you have pushed me to do my best work, you have held me when I struggled, and you have loved me unconditionally. You gave me the greatest and most profound gift I can imagine: an education. I owe whatever I accomplish to both of you.

My sister has been a rock through the ups and downs of this year. Ali, your great sense of humor and your deep empathy provided me joy and comfort as I navigated the process of writing this thesis, and so much more. You really are the best sister in the world.

Finally, I would like to thank Zarine Kharazian. Without you, I would not have written this thesis. I am immensely grateful for the many hours you spent helping me hone my arguments, organize jumbled paragraphs and chapters, eliminate passive voice, and format footnotes. You inspired the grand vision for this paper and you held me accountable for the minutiae. You are insatiably curious, fiercely loving, and—without a doubt—the smartest person I know.

1. Introduction

On January 28, 2001, 71,921 football fans flooded into the Raymond James Stadium in Tampa, Florida.[1] The sports enthusiasts donned jerseys, painted their faces, purchased beer and nachos, and settled into their seats. They did not yet know that the Baltimore Ravens would win. They did not yet know that, seven months later, a major terrorist attack would devastate the United States and transform the nature of international security. And they did not yet know that their faces would be scanned, analyzed, and compared to a massive database of digital mug shots—all as part of large-scale operation to test the capacity of a new facial recognition software.[2]

This new facial recognition software, Facefinder, was developed by Viisage, Inc., Raytheon Co., and Graphco Technologies, Inc. Viisage, Inc.[3] Its collaborators loaned the system to the Tampa Police Department free of charge. The Police Department implemented the surveillance and data collection program, working with the Federal Bureau of Investigation to compare results to a large database of wanted criminals and terrorist suspects for comparison.[4] The Super Bowl provided a convenient testing ground for the new technology, although the Police Department and the FBI hoped that the program would effectively identify any

[1] "Super Bowl History," FootballDB.com, http://www.footballdb.com/seasons/super-bowls.html.
[2] John D. Woodward, "Super Bowl Surveillance: Facing Up to Biometrics," Santa Monica, CA: RAND Corporation, 2001. http://www.rand.org/pubs/issue_papers/IP209.html.
[3] Vickie Chachere, "Biometrics Used to Detect Criminals at Super Bowl," ABC News, http://abcnews.go.com/Technology/story?id=98871&page=1.
[4] John D. Woodward, "Super Bowl Surveillance."

suspected terrorists at an event they thought might be an easy attack target.[5] While the Tampa Police Department did not identify or apprehend any suspected terrorists, it did identify nineteen petty criminals with outstanding arrests. They did not detain or question the identified criminals, however, as the project's primary purpose was to test the capacity of the software.[6]

The press published details about the facial recognition operation a few days after the Baltimore Ravens defeated the New York Giants in Super Bowl XXXV. Randall Marshall, the legal director for the American Civil Liberties Union of Florida, commented to the New York Times: "This is yet another example of technology outpacing the protection of people's civil liberties. It has a very Big Brother feel to it."[7] Super Bowl attendees and concerned citizens alike seemed to agree with Marshall's sentiment, expressing concern about privacy violations and government control of personal information.[8]

The Super Bowl experiment constituted the first large-scale use of modern biometric technology on the American public. The FBI defines biometrics as "the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual."[9] Biometric technologies, then, are the tools used to capture, analyze, and disseminate biometric information.

---

[5] Dana Canedy, "Tampa Scans the Faces in Its Crowds for Criminals," *The New York Times*, July 03, 2001, http://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] "Fingerprints and Other Biometrics," FBI, May 03, 2016. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics.

While advances in biometrics excited the intelligence community, they concerned private citizens. The political and security ramifications of the 9/11 terrorist attacks, along with the rapid development of new biometric technologies, prompted a wave of research on biometrics. In 2001 and 2002, SEARCH, an American nonprofit research organization with an emphasis on privacy and information,[10] commissioned a survey on public attitudes toward the use of biometric technologies.[11] In more recent years, a number of organizations and agencies—ranging from the Consumer Technology Association[12] to the Pew Research Center[13] to the UK House of Commons[14]—have conducted public opinion surveys on biometrics, both within the United States and abroad.[15] While these surveys vary somewhat in their relative structures and emphases, they all reflect the general trends observed in the 2001 SEARCH survey: people generally express support for the use of biometric technologies in their capacity as anti-terrorism, public safety, and public welfare tools, whereas they disapprove of the use of biometric technologies to enable domestic surveillance or increase corporate efficiency. In 2016, for example, the International Biometrics Association found that 63% of U.S. adults were open to the use of biometrics for altruistic purposes

[10] "About Us," SEARCH, http://www.search.org/about-search/.
[11] *"Public Attitudes toward the Uses of Biometric Identification Technologies by Government and the Private Sector,"* Working Paper, *SEARCH*, 2002.
[12] "Recent Opinion Surveys on Public Perception of Biometrics," Issue Brief, *International Biometrics Identity Association*, 2017.
[13] Lee Rainie and Maeve Duggan, "Scenario: Workplace Security and Tracking," *Pew Research Center*, January 14, 2016, http://www.pewinternet.org/2016/01/14/scenario-workplace-security-and-tracking/.
[14] *Current and Future Uses of Biometric Data and Technologies*, Issue Brief. Science and Technology Committee, U.K. House of Commons, 2015.
[15] Most public opinion surveys on biometrics were conducted in the United States, Canada, the United Kingdom, and in a handful of other European Union countries. There does not appear to be survey data on public attitudes towards biometrics in non-American and non-European countries, even in places like China and India where the use of biometric technologies is widespread.

like medical research, while 70% of U.S. adults had neutral sentiments or were uncomfortable with regards to the commercial use of biometric technologies.[16]

On first examination, survey subjects appear to contradict themselves; they are untroubled by iris scanning software when it is used to identify potential terrorists, but are disturbed when the very same software is employed to store personal information about civilians. But these subtle differences in public attitudes reveal an important truth about biometric technology, and about information technology more broadly. Survey respondents are more interested in the *application* of a given technology than in its particular *form*. In other words, the type of information collected and the mode of collection matter less than do the subsequent management and use of that same information.

While individual survey respondents seem to understand that the particular mode of data collection matters less than its practical application, policymakers have yet to come to the same conclusions. Instead, policymakers and legislators tend to fixate on the type of technology used and the type of information collected, crafting narrowly tailored regulations to the technology of the moment rather than expanding and fortifying existing individual privacy protections.[17]

Biometric technologies continue to proliferate, but policy responses are inconsistent, and at times incoherent. This inconsistency in biometrics policy and law—both domestically, and even more so internationally—is likely related in part

---

[16] "Recent Opinion Surveys on Public Perception of Biometrics," *International Biometrics Identity Association*, 2017.

[17] Christopher Jensen, "The more things change, the more they stay the same: Copyright, digital technology, and social norms," *Stanford Law Review*, 2003, 531-570.

to the fact that the ethics discourse on biometrics is equally fragmented. As biometric technology becomes an increasingly quotidian component of our lives, and particularly as its role in multilateral intelligence relations calcifies, it is clear that we require a cogent understanding of what biometrics are, how biometric technologies work, and how biometric information should be collected, used, stored, and shared. Building this understanding involves examining not just the technologies themselves, but the theories underpinning and guiding social and political responses to them.

In this paper, I examine the assumptions underpinning the current definition and conception of biometric information as a unique class of personal information and identify the ways in which these assumptions are unsubstantiated and often misleading. I propose an alternative framework for understanding biometrics in the broader context of personal information. This framework situates biometric information on a spectrum of personal information, rather than in a discrete category of its own. In establishing this framework, I not only articulate a more comprehensive and logically consistent definition of biometric information, but I also suggest how this definition might help to inform the development of more coherent, consistent, and durable policies regulating personal information.

1.1 Why an Ethics Approach?

While I aim to bolster my arguments with empirical information and relevant case studies, this paper emphasizes the ethical dilemmas regarding biometric

technology, relying only tangentially on methods and research that fall more clearly in the realms of law and policy. I have two primary reasons for taking an ethics approach to the issue of biometric technology.

First, biometrics law and policy are in a nascent stage. The current smattering of U.S. state statutes,[18] international intelligence agreements,[19] and vague policy directives do not constitute a significant library of biometrics policy or law. While a review and analysis of this body of information might reveal information about the fragmented development of technology law, the landscape of law and policy is changing so rapidly that I have chosen instead to focus on the ethical underpinnings of these topical issues. As policymakers, legislators, diplomats, intelligence agencies, and software developers begin to consider how biometrics should be treated in domestic courts and international treaties, they will require a firm ethical foundation from which to construct a coherent and levelheaded biometrics policy framework.

The second reason that I chose to take an ethical approach to the issue of biometric technology has to do with its relationship to broader trends in the realm of personal information and privacy ethics. With biometrics as my focus, I hope to explore some of the fundamental ethical questions that govern our understanding of personal information. These questions include deep dilemmas about the nature of personal identity, accountability, and the persistent tension between

---

[18] (740 ILCS 14/10) Biometric Information Privacy Act.
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%20

[19] Five Eyes, the Anglophone intelligence network, developed a bilateral strategy for sharing biometric information between intelligence agencies.
United Kingdom. U.K. Border Agency. *Privacy Impact Assessment of High Value Data Sharing Protocol*. 2010.

individualism and collectivism. While a comprehensive exploration of each of these issues is beyond the scope of this paper, I hope that my analysis serves as a foundation from which to further investigate these questions.

1.2 International Implications

Social and natural scientists sometimes describe philosophy as an ivory tower discipline, one that isolates itself from material questions of the everyday world. While I bring the methods of philosophy—and ethics, in particular—to bear on the problem of biometric technology, I endeavor to engage with, rather than withdraw from, the political and social implications of my findings. In particular, I hope to highlight the transnational nature of these questions. Unlike the fields of law and policy, ethics is unconstrained by borders. It makes sense, therefore, that ethics constitutes the foundation of any inquiry into the undeniably global question of biometric technology.

While I reject the globalist assertion that we are on the brink of a borderless world, it is clear that exponential technological growth[20] has confused the traditional dynamics of international law and policy. In particular, military power and wealth are much less important to the creation and enforcement of international data protection laws than they are to other kinds of international policy. Because the digital world cannot be regulated according to traditional law enforcement methods, the regulation of personal information poses new and interesting challenges for international relations and policy. The transnational

[20] Robert R. Schaller, "Moore's Law: Past, Present and Future." *IEEE Spectrum* 34, no. 6 (1997): 52-59.

regulation of data collection and sharing is basically nonexistent.[21] This is in part because there is no transnational body that has the power to enforce the regulation of information flow. It is also in part because the most active collectors and traders of personal information are militaries and large multinational corporations, both powerful actors that tend to repel the kind of bureaucratic investigation that digital transgressions invite.

In this paper, I do not propose a solution to the problem of an unregulated, transnational flow of personal information. It is optimistic to presume that we will ever achieve global consensus regarding regulation of the collection, analysis, and use of personal information. It is even more optimistic to suggest the development of an effective international enforcer of those regulations. However, I do posit that universally consistent and durable definitions of biometrics and personal information—independent of specific geography or technology—will enable the formation of more comprehensible and enforceable standards, policies, and international agreements.

1.3 Roadmap

In this paper, I further explore the distinction between type and application of personal information. I argue that, contrary to the assumptions inherent in much of the policy and ethics literature on biometrics, there is no clear or substantive difference between biometric information and other kinds of personal information.

[21] Abraham L. Newman, "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive," *International Organization* 62, no. 01 (2008): 103-130.

I propose an alternative framework for understanding biometrics, which establishes a scalar model for interpreting different kinds of personal information. According to this model, biometric information does not constitute a discrete category, but rather describes one end of a more complex spectrum of information. I also suggest some practical ways that this framework might be integrated into the formation of information policy, particularly in the context of global politics.

The second chapter of this paper provides some background on biometrics. I review various definitions of "biometrics," briefly recount the definitions, categories, and history of biometric technology. The third chapter presents an evaluation of the ethical arguments related to the collection, use, and sharing of biometric information. In this section, I identify problematic assumptions that underpin existing definitions and ethical analyses of biometrics, explaining how these assumptions inevitably foment a fundamental misunderstanding of personal information. The fourth chapter presents an alternative model of personal information. This model situates personal information on a spectrum rather than in discrete categories. The fifth chapter presents a brief case study to illustrate the new model of personal information. Analysis of the case study highlights the ethical and policy implications of reinterpreting biometrics within the alternative model of personal information.

2. Background

2.1 Definitions

There is no universal consensus regarding the definition of "biometrics." The lack of a clear and consistent definition reflects not only a semantic incongruity, but also a deep substantive confusion about what biometrics is and what it represents. Some characterizations of biometrics focus on the specific type of information collected. Illinois and Texas, two of the few states that attempt to provide rigorous definitions related to biometrics, define "biometric identifiers" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[22] Illinois, however, explicitly excludes "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, [and] eye color,"[23] while Texas does not. These legal definitions promise to outlive their relevance quickly as new biometric technologies are developed.

Other definitions of biometric information are less concerned with the exact type of information, and more concerned with the capacity of certain information to identify individuals. A bill pending in the Washington State legislature defines a biometric identifier as a "characteristic, whether biological, behavioral, or both, that enables automated recognition of an individual and is

[22] (740 ILCS 14/10) Biometric Information Privacy Act, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57%20.
[23] Ibid.

inherently sensitive, including but not limited to fingerprints, DNA, hand geometry, palm print, and iris scan." The bill goes on to concede that this definition "also includes less sensitive identifiers, including, but not limited to facial imaging, voice, and gait when used specifically for identification purposes."[24] According to this definition, practically any type of information used for identification purposes might be governed under this biometrics bill. The FBI has a similar understanding, defining biometrics as "the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual."[25] The Biometrics Institute avoids any explicit definition of biometrics altogether, stating states that a biometric characteristic is the "biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition."[26]

It is clear that variation in definitions of "biometrics" does not simply involve the employment of different vocabularies, but also the use of entirely different standards. Some definitions pinpoint specific technologies or biometric identifiers, while others describe the ability of certain technologies to automatically identify or recognize individuals. While all of these definitions simulate specificity, the precision is largely superficial. Further examination reveals that the definitions are so vague that it is impossible to determine in practice what

[24] Washington State House Bill 1094, 2017, http://app.leg.wa.gov/billsummary?BillNumber=1094&Year=2015.
[25] "Fingerprints and Other Biometrics," FBI, May 03, 2016, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics.
[26] "Definition of biometrics," *Biometrics Institute*, http://www.biometricsinstitute.org/pages/definition-of-biometrics.html.

information counts as "biometric" and what information does not. It is worth noting that the definitions of biometrics described above are among the most robust. Law enforcement agencies and legislative bodies are forced to furnish definitions related to the statues they enforce and create. But in many contexts, particularly in the realm of academia, the word "biometrics" goes undefined. This definitional omission implies the existence of an uncontroversial and universal understanding of biometrics, such that the word does not warrant characterization. In neglecting to define the subject of their work, ethicists and other scholars miss a central question: what is biometrics?

2.2 Hard and Soft Biometrics

While there is no adequate definition of biometrics, scholars and engineers have proposed a definitional distinction between *types* of biometrics. Most existing definitions of biometrics imply that a biometric characteristic or identifier should uniquely identify an individual. But even this central concept is muddied when we consider the inclusion of "behavioral characteristics." Behavioral characteristics include typing rhythm, gait,[27] and voice,[28] many of which cannot reliably authenticate individual identities on their own, but which can reliably *verify* an

[27] Robertas Damaševičius, et al., "Smartphone User Identity Verification Using Gait Characteristics," *Symmetry* 8, no. 10 (2016): 100.
[28] Sahidullah, Md, "Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies," PhD Thesis, 2015.

individual's identity (e.g. based on recorded histories of typing patterns).[29] Researchers have recently coined the term, "behaviometrics," to more accurately describe this class of personal characteristics.[30] This term might be useful, but most scholars, legislators, and policymakers include both "biological" and "behavioral" information in their definitions of biometrics. When they do distinguish between types of information, they use the terms "hard" or "first generation" biometrics to describe purely "biological" information like fingerprints or iris scans, and "soft" or "second generation" biometrics to describe "behavioral" information, like gait and typing patterns.[31]

The distinction between hard and soft biometrics is not purely descriptive; it also has normative implications. In an article on the ethics of second-generation biometrics, Sutrop and Laas-Mikko (2012) argue that first generation biometric information is more conducive to neutral identification. In other words, first-generation biometrics are primarily collected and used to confer rights, responsibilities, and entitlements on a positively identified person. Sutrop and Laas-Mikko observe that second-generation biometrics, on the other hand, are less individually specific, and therefore more conducive to the classification and characterization of groups of people.[32]

---

[29] Nisenson, Mordechai, Ido Yariv, Ran El-Yaniv, and Ron Meir. "Towards behaviometric security systems: Learning to identify a typist." In *European Conference on Principles of Data Mining and Knowledge Discovery*, pp. 363-374. Springer Berlin Heidelberg, 2003.
[30] Ibid.
[31] Sutrop, Margit, and Katrin Laas-Mikko. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics." *Review of Policy Research* 29, no. 1 (2012): 21-36.
[32] Ibid.

According to Sutrop and Laas-Mikko, the divergence in application of these two classes of biometric information stems from the fact that first-generation biometrics measure individually unique biological traits, that if collected and analyzed correctly, can only be used to identify a single person. Second-generation biometrics involves traits that are not necessarily unique, and are therefore more conducive to characterization.[33] For example, a particular type of gait might be associated with a certain type of behavior, based on analysis of historical data. Sutrop and Laas-Mikko conclude that the expansion of second-generation biometrics could result in unjustified stigmatization and discrimination, whereas this risk is less potent with regard to first-generation biometrics.

Sutrop and Laas-Mikko do not rely on empirical arguments to make their claim, so it is unclear whether their conclusions about the relative discriminatory capacities of hard and soft biometrics are true. When they suggest that a characteristic such as gait might be used to characterize and unjustly target groups of people, they do not provide a specific example of this occurring, nor do they explain exactly how it would happen in reality. I return to their argument in a later section when I discuss theories about the body as a primary source of identity-based discrimination and stigmatization.

The soft-hard biometrics distinction is an attempt to resolve the imprecision of the word "biometrics." As biometric technologies expanded, allowing for the identification of people based on secondary traits like typing

[33] When they assert that second generation biometrics are not "unique," Sutrop and Laas-Mikko intend that the analysis of a person's gait is less reliable in the project of positively identifying an individual than it is in contributing to a more holistic characterization of a given person.

pattern and voice, it became unclear how these kinds of information—which were not strictly biological—fit into a definition of biometrics. It made sense to articulate the existence of sub-categories under the umbrella term, "biometrics." While the distinction is useful in some ways, it ultimately perpetuates a misunderstanding of the nature of personal information, and consequently generates confused and inconsistent ethical analyses and policy proposals.

My central argument revolves around the imprecision of the word, and the concept of, "biometrics." In this paper, I attempt to define biometrics to the best of my ability without committing to any particular institutional definition. As I develop my argument, I interrogate the definitions of biometrics described above, highlighting their inability to effectively and consistently identify specific technologies or kinds of information.

2.3 History of Biometric Technologies

The history of biometric technology begins with Alphonse Bertillon, a Parisian anthropologist and police desk clerk.[34] In the late 19th century, Bertillon developed a criminal identification system that involved the collection and comparison of specific biological markers. Bertillon relied on physiological measurements of bone structures and body parts, as well as on "soft biometric" identifiers such as birthmarks, tattoos and scars. He estimated that if fourteen independent traits were used, the odds of creating two identical records, and consequently

[34] John Pike, "History of Biometrics," *Global Security*, http://www.globalsecurity.org/security/systems/biometrics-history.htm.

misidentifying a suspected criminal, would be 286,435,456 to one.[35] Bertillon's system was arduous and time-consuming. It relied on fickle biometric identifiers that were challenging to measure precisely and frustratingly unstable throughout childhood and adolescence. Furthermore, none of these characteristics alone had the capacity to uniquely identify an individual. Only when aggregated could they reliably identify a suspect. Nevertheless, Bertillon's system, or "Bertillonage" as it was called, greatly influenced the development of biometric technologies and programs.

In the late 19th and early 20th centuries, a more accurate and streamlined method that used individual fingerprints supplanted Bertillonage.[36] While fingerprints have been used as personal signatures since the 14th century B.C.E in China, they were not understood to be unique physiological markers of identity until Dr. William Faulds and William Herschel separately and simultaneously came to the conclusion that fingerprints serve as a sort of unique individual code for each person. The Henry Classification system that is still used today was named after Edward Henry, who designed and first implemented the system in India in 1897.[37]

Biometric technologies proliferated in the late 20th and early 21st centuries. During this biometric boom, computing and information processing capacity exploded, biotechnology research expanded its reach, and concerns about international security emerged at the forefront of American and European politics.

[35] Ibid.
[36] Ibid.
[37] Ibid.

Iris scans, face scans, and hand geometries became integral components of security, both in public and private sectors.[38] New biometric technologies, particularly those measuring soft biometric characteristics like typing patterns, are rapidly becoming a part of the standard security toolbox.[39] It is likely that software developers and biotechnology researchers will refine the accuracy and overall efficacy of existing biometric technologies, while continuing to devise new methods for the collection, storage, and sharing of biometric information. In recent years, public pressure and internal concern about the security of biometric information has prompted an effort to develop technological safeguards against the accidental or intentional leaking or sharing of biometric information.[40]

Even as biometric technologies become increasingly sophisticated and secure, ethical understandings of these technologies remain confused and fragmented. As a result, biometric policy and law is inconsistent, and often unclear. The proliferation of biometric technologies across industries is unlikely to slow. In fact, the collection, analysis, and sharing of biometric information will permeate more sectors as time progresses. It is therefore essential that we pause for a moment to carefully define the problems that we face, so that we may better resolve those problems in a principled and comprehensive manner.

---

[38] Arun Ross et al., "Introduction to Multibiometrics," In *Handbook of Biometrics*, pp. 271-292. Springer US, 2008.
[39] Mordechai Nisenson, et al., "Towards Behaviometric Security Systems: Learning to Identify a Typist," In *European Conference on Principles of Data Mining and Knowledge Discovery*, pp. 363-374, Springer Berlin Heidelberg, 2003.
[40] "Protecting biometric data with Extended Access Control: Securing biometric datasets in electronic identification documents," Technical paper, *Entrust*, 2014.

In the section that follows, I describe the major ethical commentaries on biometrics, emphasizing the kinds of assumptions that these commentaries make. In doing this, I hope to show that these unsupported assumptions and inconsistencies stem from a fundamentally faulty understanding of biometrics and its relationship to personal information more broadly.

3. Arguments for "Biometrics" and Why They Fail

Literature on the technology of biometrics abounds. Biometrics is ubiquitous; it now undergirds the security infrastructure of countless industries, including banking, agriculture, social media, and national security. As the technologies become more sophisticated and as applications of these technologies broaden in scope, software developers and engineers increasingly publish their findings related specifically to the collection, analysis, and management of biometric information.

While there is plenty of technical material on biometrics, literature on the ethical and legal implication of biometrics is remarkably sparse. In general, technology tends to precede ethics and law.[41] It often takes decades to understand the implications of new technologies, and even longer to determine the appropriate legislative and ethical responses. The biometrics boom, while it has generated significant contributions to the literature on bioengineering, bio-statistics, and other related disciplines, has not yet initiated a robust and coherent scholarly conversation on the ethics of biometrics. The scholarly conversation—in its current nascent state—is fragmented and incomplete.

Much of the literature on biometrics, either implicitly or explicitly, asserts that biometric technology presents unique ethical issues. This analysis fails to 1) define biometrics, and 2) articulate the ethical and legal distinctions between biometric information, and other kinds of personal information. If biometric

[41] Vivek Wadhwa, "Laws and Ethics Can't Keep Pace with Technology," MIT Technology Review, September 19, 2014, https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

technologies present unique concerns, scholars must clearly articulate these concerns.

Biometrics scholarship also tends to be alarmist; scholars warn that biometrics pose significant ethical and practical threats, and some have even suggested a complete rejection of the suspect technologies until the ethical and practical threats have been addressed. These alarmist views do not represent the entirety of biometrics scholarship; there are positions that take a more moderate stance, balancing the practical benefits of biometric technologies against concerns about particular components of these technologies.

In this chapter, I aim to construct a map of the existing conversation on biometric ethics. In particular, I interrogate arguments that support the assumption that biometric information is categorically different than other kinds of personal information. Rather than review the topical issues with which scholars of biometric ethics concern themselves—including consent, privacy, and personal identity—I identify the primary fallacies that philosophers and ethicists make in their discourse on biometrics. After considering some of the most compelling arguments in support of special ethical standards for biometric information, I will be prepared to propose an alternative definition of biometrics.

First, I address the argument that biometric information facilitates discrimination. Next, I respond to the assertion that biometric information is uniquely related to bodily integrity. Finally, I interrogate the assumption that biometric information is fundamentally more personal, or more special, than other

kinds of personal information. For each claim, I present the argument in full and explain why it fails.

3.1 Discrimination

The ethics literature on biometrics is replete with warnings about the discriminatory potential of biometric technologies. According to these arguments, biometric information is fundamentally more conducive to discrimination than non-biometric information. Consequently, the collection and use of biometric information should be regulated separately, and more strictly, than the collection and use of non-biometric information. If the discrimination argument were true, it would be reasonable to advocate a separate and more stringent regulation of biometric information. However, I argue that the discrimination argument is incorrect. Because biometrics is not fundamentally discriminatory in nature, the discrimination argument does not give us a reason to conceive of biometric information as a distinct category.

3.1.1 The Discrimination Argument

The discrimination argument asserts that there is something unique about biometric information that lends itself to discriminatory applications. Some scholars make explicit arguments about the discriminatory potential of biometric information. For example, Sutrop and Laas-Mikko claim that biometric information—second-generation biometric information, in particular—will be used to identify "risk-positive" characteristics, build predictive models using those

characteristics, and discriminate against individuals according to broad classifications. [42] Jennifer Poudrier, in her contribution to a book on the social implications of surveillance, hypothesizes that the collection of biometric information for the purpose of social services might actually be used to discriminate against marginalized groups. She uses the example of health information collected on First Nations people in Canada to support her claim.[43] Other scholars, including Alterman (2003) and Van der Ploeg (2003), while they do not center the question of discrimination in their respective papers, make implicit assumptions about the discriminatory potential of biometrics information.

The discrimination argument involves two distinct questions. The first question is empirical in nature: is biometric information, in practice, used in more discriminatory ways than other types of personal information? Given that there is not sufficient data to defend or dismantle the argument that biometric information is applied in distinctly discriminatory ways, it is impossible to answer this empirical question. Conjectures about the *possible* discriminatory applications of biometric information, like the one that Poudrier makes in her paper about health information and First Nations people, do not furnish evidence in support of this empirical claim. To answer this question, it would be necessary to define each variable—biometric information, personal information, and discrimination—and to measure the discriminatory applications of each kind of information across

[42] Margit Sutrop and Katrin Laas-Mikko, "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics," *Review of Policy Research* 29, no. 1 (2012): 21-36.
[43] J. Poudrier, 'Racial' Categories and Health Risks. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 2003, 111.

sectors and industries. Because this study has not yet been conducted, we cannot draw conclusions with regards to this question.

The second question is more conceptual in nature: is there something fundamental about biometric information that lends itself to discriminatory applications? Many scholars, including Georgio Agamben (2004) and Emilio Mordini (2009), are confident that there *is* something fundamental about biometric information that lends itself to discriminatory applications. Claims that biometric information is more conducive to discrimination than other types of information tend to assume that identity—and therefore, prejudice—is rooted in biology and physiology. In other words, these authors are concerned that biometric information conveys essential facts about a person's identity (e.g. his race or gender), and therefore could easily be used in discriminatory ways, either intentionally or inadvertently. This assumption underlies not only philosophical ruminations on the dangers of biometrics, but also legislative decisions and public opinion.

3.1.2 Why the Discrimination Argument Fails

If the discrimination argument were true, there would be good reason to conceive of biometric information as an independent category of personal information, deserving of stricter regulation. However, it is clear that there is nothing special about biometric information that makes it fundamentally more discriminatory in nature. In fact, it is likely that other kinds of personal information have more

discriminatory potential. I first show why the discrimination argument fails, and I then suggest why other kinds of personal information might actually be *more* dangerous with regards to discrimination.

First, I want to reiterate that there is no empirical evidence in support of the discrimination argument. This means that we cannot know whether or not the use of biometric information is more discriminatory in practice than the use of other kinds of personal information. While we cannot answer the empirical question, we can interrogate the assumptions underpinning the conceptual claim that biometric information is fundamentally more discriminatory than other kinds of personal information.

The discrimination argument is built on a faulty logic that overestimates the biological and physiological bases of identity. The discrimination argument can be summarized as follows:

1. Discrimination occurs on the basis of identity.
2. Some marginalized identities are determined by biology and physiology. [44]
3. Biometric information, by definition, is biological and physiological.
4. Biometric information is fundamentally more conducive to discrimination than other types of personal information.

I accept (1). In general, discrimination—at least, the type of discrimination with which we are concerned—is perpetrated on the basis of identity. People are grouped based on their real or perceived characteristics and are treated differently according to their group membership. If (2) were correct, then (3) and (4) would

[44] Proponents of this argument do not assert that "identity" is *always* biological or physiological, but rather that particularly sensitive identities like race and gender, are biologically and physiologically determined.

naturally be true.[45] However, the logic of the discrimination argument falls apart in premise (2). There are, of course, many identity categories. Most ethicists concerned with the discriminatory potential of biometric information focus on race. In the discussion that follows, I focus my objections to this argument on race as well. It is worth noting, however, that my objections also apply to the question of gender discrimination.

While there are biological and physiological traits and characteristics associated with identity, biometric information alone cannot determine a person's identity. The assumption that biometric information communicates useful facts about a person's identity fails to acknowledge the complex and multifactorial nature of identity. Identity categories are fluid, and are more closely linked to social perception than they are to an objective biological reality. Sally Haslanger, in her seminal work on the definition of race and gender, construes both race and gender as *real* and *social* categories.[46] In other words, race and gender exist in the world; we know this because people are grouped on the basis of their race and gender every day. However, these groupings have much more to do with the social perception of identity than they do with any objective or biological fact about an individual.

Kwame Anthony Appiah makes a similar argument, explaining that racial categories are imagined. He writes, "In humans, however you define the major

[45] I actually do take issue with (3), although that premise is not relevant to my argument here. I argue that I think it is almost impossible to distinguish between "biological" and "non-biological" information. I will explore this dilemma later in this paper.
[46] Sally Haslanger, "Gender and Race: (What) Are They? (What) Do We Want Them To Be?" *Nous* 34, no. 1 (2000): 51.

races, the biological variability within them is almost as great as the biological variation within the species as a whole."[47] Evolutionary biologists confirm this claim. In fact, there is significantly more genetic variation *within* racial groups than there is *between* them.[48] This genetic variation does not appear exclusively in individual DNA, but also manifests in other biological and physiological identifiers. There are very few specific biometric identifiers that can accurately determine a person's race. For example, almost any person who is positive for sickle-cell anemia is likely to be black. However, it remains almost impossible to determine a person's race based *solely* on biological information.

Based on these analyses, it is clear that biometric information alone cannot reliably determine a person's race or gender. In general, biological and physiological information is not sufficient to assign a person to an identity group and to discriminate accordingly. It is therefore impossible that biometric information has *more* discriminatory potential than other kinds of personal information.

Some scholars, including Sutrop and Laas-Mikko (2012) concede that hard biometric information may not be discriminatory, but claim that soft biometric information is the central concern. In other words, they are not concerned with the pure biological and physiological identifiers like fingerprints, DNA, and iris scans, but they are worried about identifiers like gait, typing patterns, and face

---

[47] K.A. Appiah, "Race, Culture, Identity: Misunderstood Connections," *Tanner Lectures on Human Values*, 1996, 17, 95

[48] Lynn B. Jorde, and Stephen P. Wooding, "Genetic Variation, Classification and 'Race'," *Nature Genetics* 36 (2004): S28-S33.

geometry. I argue that in making this argument, these scholars actually argue *against* the claim that biometric information is fundamentally dangerous. Instead, they gesture towards the many ways in which other kinds of personal information can be used in discriminatory fashions.

Algorithmic bias is a popular topic in technology scholarship today and the literature is replete with tales of discriminatory outputs from supposedly objective tools. One particularly egregious example that surfaced in the summer of 2016 received intense media attention. This story involved the classification of black individuals as "gorillas" by Google Photos facial recognition software.[49] The people who had mistakenly been labeled "gorillas" in a picture on Google photos complained publicly about the offense, prompting an immediate response from Google. The company apologized for the mistake and removed the "gorilla" tag from their software. Despite the swift response, the event inspired a backlash against the use of biometric technologies more broadly.

While Google's program created racist outputs, the origin of the bias remains unclear. Even though Google promised to work on the algorithm itself to improve its accuracy and to eliminate the problematic tagging feature, web developers were unable to ascertain why their program had produced such a specifically racist result.[50] It is unclear whether or not Google has since addressed

---

[49] Alistair Barr, "Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms," *The Wall Street Journal*, July 02, 2015, http://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

[50] The Google Photos software relies on machine learning, a type of artificial intelligence that relies on exposure to information to accurately distinguish between objects. Google proposes that their system simply hadn't had enough time to learn the difference between gorillas and of black people to accurately distinguish between the two. This conclusion, however, does not explain why white people were not inaccurately

the underlying issue, but according to the information that is publicly available, Google simply resorted to deleting the "gorilla" tag altogether.

The Google case is an example of how soft biometric might be used in a discriminatory fashion. Scholars like Sutrop and Laas-Mikko (2012) warn that this is exactly the kind of thing that will happen if we do not carefully monitor and regulate the application of soft biometric technologies. However, Sutrop and Laas-Mikko—and the many other scholars who share their concerns about soft biometrics—make a category mistake. If biometric information is understood to be biological or physiological information that uniquely identifies an individual, then "soft biometrics" does not fall clearly into the definition of biometrics at all. The color of a person's face (as in the Google case) is not a biological fact alone. Skin color certainly has biological determinants, but it is also affected by environmental factors like time spent in the sun, tanning products, lighting when the picture was captured, and so on. Other soft biometric identifiers are even less biological; consider typing patterns and gait, for example.

In claiming that soft biometrics are more dangerous than hard biometrics, these scholars essentially admit that it is not the biological nature of the information that is dangerous (as they assert elsewhere in their argument), but that as we move farther away from "hard biometrics," it becomes easier to discriminate on the basis of identity.

---

identified as polar bears. It is possible that the stock images Google used to inform its AI software did not include many photographs of people with black and brown skin, which resulted in software that assumed an equation between "human" and "white."

This conclusion supports my assertion that not only is biological information *not* especially discriminatory in nature, but that it is actually *less* discriminatory than other kinds of personal information. For example, a person's zip code is much more likely to betray his race than his fingerprint, or even his face geometry. A person's search history or social media presence is more likely to betray his gender than a fingerprint, or even a DNA sample. Because, as Haslanger and Appiah assert, identity is primarily socially constructed and socially perceived, *social* and *environmental* information about a person's life will be much more telling than purely biological and physiological information in attempting to determine a person's identity.

Based on this analysis, I conclude that hard biometric data do not fundamentally facilitate discrimination. Furthermore, I demonstrate that soft biometric information is not solely biological, and therefore falls more clearly into the category of "other personal information." Finally, I contend that non-biometric, or "soft biometric," information is actually more conducive to discriminatory applications than is biometric information.

3.2 Bodily Integrity

I have now established that biometric information is not especially conducive to discrimination. However, there is a different kind of argument related to biometrics and discrimination. Some scholars, including Georgio Agamben and Irma van der Ploeg, assert that whether or not biometric information is more likely

than other kinds of personal information to be applied in discriminatory ways, it is especially *bad* to discriminate on the basis of biometric information. This argument has less to do with the discriminatory potential of one type of information over another, and more to do with the intrinsic nature of that information.

Proponents of the bodily integrity argument contend that control over one's own biometric information equates to control over one's bodily integrity. According to this argument, biometric information—because it has to do with a person's body—is innately more valuable than other kinds of information. As a consequence, it is more dangerous—both morally and practically—if other people have access to an individual's biometric information. The collection, analysis, and sharing of biometric information has the potential to compromise a person's fundamental bodily integrity. If the bodily integrity argument were true, then it would make sense to conceive of biometric information as a distinct category of personal information, and to regulate it accordingly. However, I argue that the bodily integrity argument is incorrect, and therefore does not provide a justification for the distinct conception and regulation of biometric information.

3.2.1 The Bodily Integrity Argument

Scholars defend the bodily integrity argument by appealing to a variety of justifications. However, their central claim is that there is something inexplicable and inviolable about the physical body that deserves special respect. Irma van der Ploeg and Anton Alterman, for example, both assert that there is something

unique and deeply personal about biometric information. Van der Ploeg states, "Embodiment is central to individuality and identity in a way that a person's social security number, or…car rental records are not."[51] In other words, she believes that information about her body has to do with her very existence in the world, while information about where she lives or how the government identifies her is simply meta-data about her life. Anton Alterman makes a similar claim, appealing to an individual's right to privacy. He argues that there is value in cohesion between the "psychological" and "biological" self, and that for this cohesion to exist, an individual must be the sole proprietor and controller of information about his own body.[52] Giorgio Agamben, a vocal opponent of biometrics, expresses concern about "bio-political tattooing," or the association of certain biometric variables with a person's identity, a practice that he associates with treatment of the Jews during the Holocaust.[53] Agamben, van der Ploeg, and Alterman all agree that there is something unique and inviolable about the body, and that the collection, analysis, and sharing of biometric information contravenes a person's bodily integrity.

The bodily integrity argument rests on the assumption that biometric information *is* the body. In other words, if Person A controls Person B's biometric information, Person A controls Person B's *body*. If this were true, the collection, analysis, and sharing of biometric information would be deeply problematic. This argument leads to the natural conclusion that any manipulation of biometric

---

[51] Irma Van der Ploeg, "Biometrics and the Body as Information," *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, edited by David Lyon, 2003, 68.
[52] Anton Alterman, "'A Piece of Yourself': Ethical Issues in Biometric Identification." *Ethics and Information Technology* 5, no. 3 (2003): 139-50.
[53] Georgio Agamben, "No to Biopolitical Tattooing." *Le Monde*, January 10, 2004.

information is inherently bad, regardless of whether or not it produces discriminatory effects. Bodily integrity is perhaps the most important moral good, and so there is something deeply wrong about another entity controlling an individual's body.

3.2.2 Why The Bodily Integrity Argument Fails

If the bodily integrity argument were true, it would be a compelling justification for a special consideration of biometric information. However, I argue that this argument rests on a faulty assumption, and is therefore insufficient to support a distinct conception and regulation of biometric information.

The bodily integrity argument can be summarized as follows:

1. Autonomy is a fundamental moral good.
2. Bodily integrity is an essential component of autonomy.
3. Control over one's own body is the definition of bodily integrity.
4. Control over one's own body is equivalent to control over information *about* one's own body.
5. Biometric information is information about an individual's body.
6. The collection, analysis, and sharing of biometric information constitutes a fundamental violation of bodily integrity.
7. Biometric information should be conceived of and regulated as a unique category of personal information.

I accept (1), (2), and (3). Autonomy, or freedom, has been defined in a variety of ways, depending upon context. John Stuart Mill describes what autonomy, or liberty, means in the following terms: "The only part of the conduct of anyone for which he is amenable to society is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself,

over his own body and mind, the individual is sovereign."[54] In other words, an individual must fully control his own body and mind in order to be considered autonomous. This conception of autonomy supports the first three premises of this argument, but is irrelevant to the remainder of the bodily integrity argument.

The bodily integrity argument fails on premise (4); how can it be that control over one's own body is equivalent to control over *information* about one's own body? In constructing this equivalency, Alterman, Agamben, and van der Ploeg misunderstand what biometric information is. Implicit in each of their arguments is the assumption that biometric information is simply a digital rendering of the body. Emilio Mordini, in his handbook on biometric technology, describes this as "informatization of the body."[55] However, biometrics technologies do not simply transform a physical human body into a digital human body.

Biometrics measure one specific physical attribute of a person and transform that attribute (or some sub-part of that attribute) into numerical code. Take fingerprints, for example. When a person is "fingerprinted," he does not relinquish his bodily integrity. To store a fingerprint, the police capture an image of the actual fingerprint. They then enhance this image so that the exact details of the fingerprint become visible. Then, an algorithm extracts information related to the "minutiae points" of the fingerprint, which include ridge endings and

---

[54] John Stuart Mill, *On Liberty,* Longmans, Green, Reader, and Dyer, 1869.
[55] Emilio Mordini, "Ethics and Policy of Biometrics," *Advances in Pattern Recognition Handbook of Remote Biometrics*, 2009, 293-309.

bifurcations. This information is translated into numerical code, which the police can later use to positively identify an individual.[56]

While there are certainly reasons that it would be bad for police to have the capacity to uniquely identify an individual, there is no reason to believe that ownership of numerical code that relates to specific information about a person's fingerprint in any way violates that person's bodily integrity. If Person A has been fingerprinted, he still has full control of his own body. He can do whatever he wishes with his fingers. He alone decides where and how to move his body in the world; he even has the power to remove his own fingers if he desires. The police, on the other hand (or whatever entity has a numerical code that represents his fingerprints) cannot do anything with Person A's fingers. They do not control his body. The owners of Person A's numerical fingerprint code can *only* use that information to positively identify Person A *if* he is apprehended and fingerprinted again. Identification does not constitute a violation of bodily integrity.

It is clear that a person need not have complete control over information about his body in order to have complete control over his body itself. Consequently, the bodily integrity argument fails. This conclusion has two consequences. First, it indicates that the bodily integrity argument is insufficient to justify a distinct conception and regulation of biometric information. Second, this conclusion dismantles another argument that follows from the bodily integrity argument.

---

[56] Arun Ross, Jidnya Shah, and Anil K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE transactions on pattern analysis and machine intelligence* 29, no. 4, 2007.

The bodily integrity argument deals with the fundamental nature of biometric information. According to this argument, biometric information is sacred in a way that non-biometric information is not. Accordingly, Sutrop and Laas-Mikko, along with some of their peers, argue that it is especially *bad* to use biometric information to discriminate.[57] This argument is distinct from the discrimination argument in that it does not attempt to class technologies based on their inherent discriminatory potential, but rather makes a normative claim about the discriminatory use of specifically biological and physiological information, as compared to other types of information. According to this argument, if all else is equal, the type of information used to discriminate is consequential.

Consider the following scenario: a risk-assessment algorithm used to determine criminal sentences incorrectly classifies black individuals as high-risk at a higher rate than it classifies white individuals as high-risk. In one case, the program uses biometric information, like face geometry or gait. In another case, the program uses non-biometric personal information, like zip code and employment history. Both programs are equally discriminatory. Proponents of the bodily integrity argument would assert that because there is something fundamentally invasive about using biometric information, it is *worse* to use biometric information than non-biometric information, even if the two programs have the same effect. Because I reject the claim that the collection, use, and sharing of biometric information violate bodily integrity, I argue that neither

[57] Margit Sutrop and Katrin Laas-Mikko, "From Identity Verification to Behavior Prediction."

program is morally worse than the other. The moral issue is the discriminatory output, not the type of information input.

The bodily integrity argument fails because control over one's own body is not equivalent to control over information about one's body. This analysis confirms that there is nothing fundamentally wrong about the collection, use, and sharing of biometric information. Furthermore, if a biometric technology has a discriminatory effect, that is problematic because discrimination is wrong, not because biometric information is inherently more valuable than other kinds of personal information. Therefore, the bodily integrity argument does not furnish sufficient justification for the distinct conception and regulation of biometric information.

3.3 Personal Identity

The personal identity argument is closely related to the bodily integrity argument, and shares many of the same defenses, although the two are sufficiently unique to require separate consideration. The personal identity argument asserts that biometric information is fundamentally more *personal* than non-biometric information. In other words, biometric information is central to an individual's identity in a way that other information is not. Because biometric information differs from non-biometric information in its value to the individual and in its capacity to define a person's core identity, it should be considered as a separate class of personal information and regulated accordingly.

Proponents of the personal identity argument include Irma van der Ploeg and Emilio Mordini, both of whom assert that there is something deeply personal about biological information. Anton Alterman and Georgio Agamben also imply that biometric information is personal in a way that non-biometric information is not. I argue that there is nothing special about biometric information that renders it *more* personal than any other kind of personal information. In doing this, I reject the personal identity argument, the last of the main arguments in support of an independent and uniquely regulated class of biometric information.

3.3.1 The Personal Identity Argument

The personal identity argument asserts that biological and physiological information are the most personal kinds of information. The argument is generally grounded in the reductionist belief that we *are* our bodies. There is no further fact of identity. As such, it must be true that information *about* our bodies is most closely linked to personal identity. Therefore, biometric information—or information about our bodies—constitutes a distinct category of personal information and should be regulated according to different principles.

The personal identity argument rests upon the assumptions 1) that there is an objective means of determining what is more or less personal to an individual, and 2) that given a universal and objective determination of "personal-ness," biometric information must be the most personal because persons, first and foremost, are concrete, physical beings in the world. I reject both of these assumptions.

3.3.2 Why The Personal Identity Argument Fails

The personal identity argument is the least compelling of the three main justifications for a distinct conception and regulation of biometric information. However, it is worth considering the argument for two reasons. First, if the personal identity argument were true, it would constitute a justification (if a weak one) for the separate classification of biometric information. Second, the personal identity argument reveals a common misconception about the relationship between the physical body and personal identity.

The personal identity argument can be summarized as follows:

1. Persons are physical, concrete beings.
2. Persons *are* their bodies.
3. Bodies are represented by biological and physiological information.
4. Biological and physiological information are the most *personal* kinds of information.
5. Biometric information is biological and physiological.
6. Biometric information is more personal than non-biometric information.
7. Biometric information should be conceived of and regulated as a unique category of personal information.

This argument fails on more than one premise. I am willing to grant (1) and (2), although these premises are not uncontroversial in themselves. The argument falls apart in (3) and (4), where it is asserted that bodies are represented, in their most personal form, by biological and physiological information. If a reductionist conception of personal identity is true, then *all* information about a person's body is, in some way, physical and concrete. This does not mean, however, that all information about a person's body is biological or physiological. Furthermore, a person's existence as a concrete, physical being does not justify the claim that

biometric information is fundamentally more personal than non-biometric information.

Van der Ploeg, in her defense of the personal identity argument, asserts that because she feels more connected to her body than to her rental car record, it must be true that biometric information is more personal than non-biometric information. It may be that Irma van der Ploeg actually does feel this way, but I would first like to challenge the way that she makes her argument. Van der Ploeg describes biometric information in vague terms, using the word "embodiment" to talk about the use of biometric technologies. She compares "embodiment" to specific examples of non-biometric personal information, like her social security number and her rental car records. This is an asymmetrical comparison. "Embodiment" is not the same kind of thing as a social security number. A more balanced account would compare an iris scan to a social security number, for example.

Van der Ploeg also fails to acknowledge that some types of non-biometric information can be deeply personal. Information about where we live, the communities to which we are connected, the books we have read, the work we have produced, and so on. In fact, I would postulate that van der Ploeg might consider her own body of scholarship as an essential component of her personal identity, perhaps even more so than a collection of biological information (for example: a fingerprint, an iris scan, and a face scan).

I do not argue that non-biometric information is *necessarily* more personal than biometric information, but rather that the determination of how personal a certain kind of information is, is inherently subjective, and therefore cannot follow the kind of logic fundamental to the personal identity argument. I also argue that even if there were an objective means of determining what kind of personal information is the *most* personal, it is not intuitive that biometric information would be more personal than non-biometric information. Therefore, the personal identity argument does not justify the distinct conception and regulation of biometric information.

3.4 Conclusions

In this chapter, I reviewed three of the most compelling arguments in support of a distinct class of biometric information and explained why they are mistaken.

First, I described the discrimination argument, which posits that biometric information is inherently more capable of discriminatory applications than other kinds of personal information. I demonstrated that this argument rests on the mistaken assumption that biology and physiology determine identity.

Second, I described the bodily integrity argument, which asserts that the collection, use, and sharing of biometric information constitutes a violation of bodily integrity and individual autonomy. I showed that this argument is insolvent because it makes a false equivalency between control over one's own body and control over information *about* one's own body.

Finally, I described the personal identity argument, which contends that biometric information is fundamentally more personal than non-biometric information. I established that this argument fails to support its implied claim that there is an objective means of determining the "personal-ness" of information. I also explained that biological and physiological information is not any more meaningfully related to a person's identity than other information. In many cases, non-biometric information is actually more personal.

I outlined the most compelling arguments in support of a distinct conception and regulation of biometric information. I objected to each one, showing why and how it fails. In doing this, I also supported my argument that we should be more concerned with the application of personal information than the type of personal information used. Having demonstrated why it is unreasonable to conceive of biometric information as a discrete class of personal information, I now propose an alternative definition of biometrics.

4. An Alternative Framework

Most philosophical reflections on biometrics tend to emphasize one issue over others—race and gender, personal identity, bodily integrity, or something else—offering critical analysis of a narrow question, but failing to reflect on biometrics as a concept. While these commentaries are useful, they lack context. In order to fully understand these critiques—and more importantly, in order to apply them effectively in the realm of policy—we must organize them within a unified theory of biometric information. In other words, we need to develop a foundational understanding of what biometric information *is* before determining how it should be used. Complex critical analyses of biometric technologies will be useful only when they relate to a coherent conception of biometrics.

While the FBI and many other agencies and institutions have already developed definitions of biometrics, these definitions remain inconsistent and imprecise. They fail to account for the distinction between hard and soft biometrics, first and second-generation biometrics, physiological and behavioral biometrics, and so on. The existing definitions of biometrics definitions might appear on their face to be complete and clear, but they quickly fall apart under interrogation.

In this chapter, I propose an alternative model for understanding biometrics within the framework of personal information. First, I argue that "biologicalness" is not a binary property. Second, I show that "soft biometrics" do not resolve the inconsistencies inherent in current definitions of biometrics.

Finally, I develop a scalar model of personal information that accommodates biometric information.

I have already argued that we should regulate personal information according to *use* rather than *type*. If we accept this position, then it might be unclear why we need a new framework or typology of personal information. There are three main reasons that this framework is useful. First, it serves to further bolster my argument in defense of an application-based approach to the regulation of personal information. A scalar model of personal information divorces the independent characteristics of personal information and demonstrates why it is misleading and unhelpful to group personal information into discrete categories. Second, this scalar model of personal information, while it should not and cannot be used to distinguish between kinds of personal information for the purpose of regulation, might be used to more precisely describe and compare different pieces of personal information. For example, biologists, social scientists, and government programs might find it useful to have the tools and vocabulary to determine which piece of information is more unique, which piece of information is more biological, which piece of information is more permanent, and so on. Finally, the scalar model of personal information that I propose helps unravel the metaphysics of personal information, independent of its application in the realms of policy and law. There is something intrinsically interesting and important about how personal information represents us, what its constituent attributes are, and how these might be used to describe us.

4.1 The Biology Mistake

All definitions of biometrics assume a binary definition of "biological." Some definitions distinguish between "biological" and "behavioral" identifiers; while

others make the tacit assumption that all of the biometric identifiers listed are, by nature, "biological." I argue that despite the language employed by various agencies and institutions to describe biometrics, "biological information" does not constitute a discrete category.

It might seem obvious that a fingerprint or a DNA sample is biological and that a phone number is not. But upon further investigation, we can see that this is not entirely true. A fingerprint is mostly, but not exclusively, determined by biological factors. For example, professional violinists sometimes wear the pads of their fingers down so much that their fingerprints are unreadable by fingerprint identification technologies.[58] Severe burns can have the same effect.

There exist more obvious "borderline cases" than the fingerprint example. Take, for example, human voice patterns. It is unclear whether voice is an example of biological or non-biological information. Biological factors, including the size of a person's diaphragm, the configuration of his vocal cords, and the shape of his larynx all contribute to a person's voice patterns. However, social factors, including affect, accent, age, smoking status, and personality also influence a person's voice patterns. Voice seems to be neither purely biological, nor purely non-biological.

Voice is by no means the only borderline case. Other "biometric" identifiers, like gait, keystroke, body modifications, and hair color, all belong to this in-between category. These examples illustrate the ambiguity of the word "biological." If we define "biological"—in the context of biometrics—as information related to

[58] Based on a conversation with a professional violinist, corroborated by an online message board. "1st Finger Scar." Violinist.com. http://www.violinist.com/discussion/response.cfm?ID=23209.

the human body, then we could consider almost any piece of personal information biological. This is clearly too broad a definition of the word.

For the purpose of this discussion, I define "biological information" as information that is *biologically determined.* It is conceivable that we might someday develop a way to identify a person's exact location based on his brain scans. However, the ability to *measure* a certain characteristic using secondary information about a person's body is not sufficient to classify that characteristic as biological information. Location is not a piece of biological information. Biological information, at least with regard to biometric information, does not mean traits that are measurable through physical analysis of a person's body. Instead, biological information means traits that are biologically *determined.* Fingerprints are primarily related to genetic factors, and are therefore primarily biological in nature. Social security numbers, on the other hand, are primarily related to environmental and social factors, and are therefore primarily non-biological in nature.

This distinction, between biologically measurable and biologically determined traits, helps narrow our definition of biological information. We understand that fingerprints are mostly biologically determined and that phone numbers are mostly not. Traits like voice, gait, and hair color all have a combination of biological and non-biological determinants. Voice, as I described previously, is in part determined by factors like the shape of a person's larynx, but is also influenced by factors like geographic region. Gait is determined by a

person's physiology, but also by profession, age, injury status, and even personality. Hair color has genetic factors, but can also be influenced by time spent in the sun and artificial dye. When philosophers, policymakers, and bioengineers write about biometric information, I think they generally mean biologically determined information. At least, I argue that this is closest to what they intend when they use the words "biological" or "non-biological." Their mistake is in construing these categories as discrete. I call this "the biology mistake."

4.2 Why "Soft Biometrics" Fails to Resolve the Biology Mistake

To account for the borderline cases—the biometric identifiers that are not easily described as either "biological" or "non-biological"—policymakers, scholars, and developers of biometric technologies developed a new category of information: soft biometrics. This new category of information was intended to capture all of the in-between biometric characteristics.

The construction of a new category of biometrics, however, does not resolve the definitional problem. In fact, the soft biometrics category exacerbates the ambiguity already present in definitions of biometrics. "Soft biometrics" supposedly includes physiological and behavioral information. But as with the distinction between "biological" and "non-biological," it is unclear what is the difference between "physiological" and "biological." Similarly, there is no clear boundary between "behavioral information" and "non-biometric information." In

adopting a more granular view of personal information, we further confuse, rather than clarify, the definition of biometrics.

The organization of personal information into categories—hard biometrics, soft biometrics, and non-biometric personal information—contributes to a fundamental misunderstanding of personal information more broadly. Discrete categories imply that there are substantive differences between the kinds of information belonging to each category. It follows that those differences necessitate tailored policies and regulations. I argue that this understanding of personal information is faulty, and that it facilitates the creation and implementation of inconsistent and unsustainable policies as well as regulations.

4.3 A Scalar Model of Personal Information

There are many instances in which the organization of information or objects into discrete categories is useful, even if it is not accurate. For example, color exists along a spectrum. There is an unidentifiable point at which blue becomes green. Of course, we name colors that fall somewhere between blue and green: aqua, teal, and turquoise. (These blue-green words are analogous to "soft biometrics," the term that describes information between biometric and non-biometric.) However, these names are crude, and fail to capture the infinity of colors that exist in the space between blue and green. This generalization is acceptable, though, because it enables us to communicate with each other and to describe our world.

Humans artificially constructed almost every category in our world. In the words of Jaegwon Kim, most categories are not natural kinds.[59] We group people according to their race, gender, sexual orientation, and so on, despite the fact that few of these categories are uncontroversially discrete. The U.S. Census, for example, presents race categorically. A person can identify as White, Black or African-American, Asian, American Indian or Alaska Native, Native Hawaiian or Other Pacific Islander, Two or More Races, or Some Other Race. Quayshawn Spencer claims that these racial categories roughly mirror the population distribution of sub-species. Even if this is true, the categories are sufficiently broad to reflect what Spencer terms "fuzzy group membership."[60] In other words, the racial groups are clusters rather than discrete categories. Not every person belongs to a distinct racial identification. Regardless of how or why human awareness of racial groupings arose, the distinctions are important in our society today. We use the vocabulary of race to talk about opportunity, oppression, and discrimination. People of color often find it useful to identify with certain racial groups as a means of expressing solidarity.[61]

We classify personal information in discrete categories: hard biometric information, soft biometric information, and non-biometric information. The creation of these categories represents an unsuccessful attempt to "carve nature at

---

[59] Jaegwon Kim, "Concepts of supervenience," *Philosophy and phenomenological research* 45, no. 2, 1984, 153-176.
[60] Quayshawn Spencer, "Philosophy of race meets population genetics," *Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences*, 2015, 46-55.
[61] Dennis Chong and Reuel Rogers, "Racial solidarity and political participation," *Political Behavior* 27, no. 4, 2005, 347-374.

its joints." But even a preliminary investigation reveals that these categories do not constitute natural kinds. The theory of natural kinds asserts that some kinds, or groupings, occur naturally in the world. Other kinds are artificially constructed and group things according to human interest rather than natural reality. In describing the ambiguity of the existing classifications of personal information, I hope I have effectively argued that "hard biometric information," "soft biometric information," and "non-biometric information" are not natural kinds.

However, even if we accept that these groupings of information are not natural kinds, one could argue that they are still useful. We artificially group things in the world all the time. Many of these groupings are very useful in practice. For example, "tables" are not a natural kind, but that does not invalidate the use of the "table" category to identify a certain kind of thing that we encounter regularly in our lives. I do not wish to imply that artificial groupings are always unproductive. It is evident that artificial groupings are often useful. Rather, I wish to distinguish between artificial kinds and natural kinds. Because biometric information is not a natural kind, we must evaluate whether or not this *particular* artificial grouping is useful.

There is not sufficient evidence to indicate that the artificial grouping of personal information is helpful. The grouping of personal information is founded upon, and perpetuates, false assumptions about the normative value of different kinds of information. For example, biometric information—or information about the physical body—is assumed to be more personal and more easily manipulated

for the purposes of discrimination. Furthermore, the artificially constructed categories of personal information facilitate the development of narrowly tailored policies and laws, most of which are inconsistent and unsustainable.

If personal information is scalar, as I argue below, it cannot be regulated according to type or category. Because personal information is a kind in and of itself—albeit with infinite variations—it should be regulated according to the use of personal information, rather than the "type" of information. The artificial grouping of personal information by type is unhelpful because it produces a specific legal and regulatory response that is predicated upon imprecise categories. Formal legislation and regulation regarding the collection, analysis, and sharing of "biometric information" is relatively new. Biometric policies and laws attempt to assign particular standards to "biometric information," distinguishing it from other kinds of personal information. In practice, these regulations and policies will fall apart, especially as it becomes clear that it is impossible to distinguish biometric information from non-biometric information. I return to the practical implications of narrowly tailored legal standards for biometric information in the next chapter.

While the artificial grouping of personal information by *type* is not useful, I do not make the same argument for the categorization of *use,* or application. Because the regulation of personal information should be legislated based on application rather than type of information, it makes sense to distinguish between different kinds of applications. For example, we might distinguish between applications that discriminate against individuals based on their identities,

applications that infringe on individuals' right to privacy, and applications that help individuals protect their personal information. Like all artificial kinds, these are not clear-cut categories and will require definition and interpretation by lawmakers and judges. Despite the challenge of delineating between these kinds of applications, these distinctions will be much more useful in regulation *how* personal information is used than the classification of *types* of personal information.

I argue for a scalar model of personal information. According to this model, there are no distinctions between "hard biometrics," "soft biometrics," and non-biometric personal information. Instead, personal information is characterized by four factors: biologicalness, uniqueness, permanence, and personalness. These factors are related, but not interdependent. I propose a model in which each factor is weighted according to a ratio of determinants, or scale of magnitude. I acknowledge that the ratio method I propose is simplistic and does not account for the potency of each determinant. For example, it is possible that voice has a handful of biological determinants and dozens of non-biological determinants. This does not necessarily mean that voice is more non-biological than biological; diaphragm size might be the primary determinant of voice, even if there are many more social and environmental factors that contribute to a person's voice pattern. If we are to use this scalar model in practice, we must find a way to account for the potency or magnitude of each determinant. However, for the purposes of describing the theory of this model, I will assume that each determinant

contributes equally to the character of each piece of personal information. Despite this simplification, the model that I describe below clearly illustrates the scalar nature of personal information, demonstrating that it does not naturally or easily fall into discrete categories.

4.3.1 Biologicalness

Biologicalness is the degree to which a piece of personal information is defined by biological determinants. Biological determinants, as I explained above, are factors related directly to the body. The ratio of biological to non-biological determinants establishes the biologicalness of a given piece of information. For example, hair color is determined by DNA (a biological determinant) and by sun exposure, diet, and the application of hair dye (non-biological determinants). The ratio of these determinants measures the biologicalness of a piece of personal information. A 1:0 ratio of biological to non-biological determinants indicates that a piece of information is very biological. A 0:1 ration of biological to non-biological determinants indicates that a piece of information is not biological at all.

4.3.2 Uniqueness

Uniqueness is the degree to which a singular piece of information can uniquely identify an individual. Something like hair color, for example, cannot uniquely identify an individual. There are billions of brunettes in the world. Something like a social security number, however, can uniquely identify an individual. A social security number is very unique. A zip code is moderately unique. Hair color is not

unique at all. We can measure uniqueness according to the approximate number of people that a given piece of information can identify. To simplify the measure, we place all 7 billion humans on a scale from 1-100. A piece of information that identifies only one unique individual receives a uniqueness score of 1. A piece of information that identifies all 7 billion individuals receives a uniqueness score of 100. A piece of personal information that identifies some number of people between 1 and 7 billion receives a uniqueness score somewhere in between 1 and 100.

4.3.3 Permanence

Permanence is the degree to which a piece of personal information persists, unchanged, over time. Something like a DNA sequence, for example, is very permanent. It never changes. Something like weight, on the other hand, is not permanent at all. Weight changes constantly. According to this metric, DNA is very permanent. Hair color is somewhat permanent. Address is not very permanent. Weight is not permanent at all. We can measure permanence according to the number of years that a piece of personal information remains unchanged. To simplify the measure, we place time on a scale from 1-100. A piece of information that changes constantly receives a score of 1. A piece of information that never changes receives a score of 100. A piece of information that changes over the course of a person's life receives a score somewhere between 1 and 100.

4.3.4 Personalness

Personalness is the degree to which a person considers a piece of information fundamental to his personal identity. This factor differs from the others in that it is subjective. However, it is still possible to measure the personalness of a piece of information. Ask an individual to consider all personal information according to the magnitude of its relevance to his personal identity. The personal information that is least relevant to an individual's personal identity receives a score of 1. The personal information that is most relevant to an individual's personal identity receives a score of 100. If I consider something like my phone number irrelevant to my personal identity, that piece of information receives a score of 1. If I consider the library of books that I have read throughout my life the most fundamental to my identity, that piece of information receives a score of 100. Information that is somewhat relevant to my personal identity receives a score somewhere between 1 and 100.

4.4 Conclusions

In this chapter, I described the Biology Mistake. Policymakers, ethicists, and software developers tend to conceive of "biological" as a binary descriptor of personal information. In fact, personal information is neither biological nor non-biological; it tends to fall somewhere between two ends of the spectrum. The Biology Mistake is the mistaken assumption that biological information is binary,

and therefore that biometric information constitutes a discrete category of personal information.

"Soft biometrics" fails to resolve the Biology Mistake. The definition of "soft biometrics" is as ill defined as the definition of "hard biometrics," and is therefore unhelpful in categorizing personal information and determining how best to regulate it.

Finally, I introduced the scalar model of personal information. This model consists of four factors: biologicalness, uniqueness, permanence, and personalness. Each factor is measured by degree. In separating these factors, I demonstrate that while they may be related, they are not interdependent. Furthermore, the attributes belonging to a piece of personal information do not necessarily carry normative value. This supports my claim that personal information should be regulated not by its descriptive attributes, but by the way in which it is used.

5. Implications

In Chapter 3, I identified the most compelling arguments in support of a categorical model of personal information. I addressed these arguments, explaining why each one fails. In Chapter 4, I proposed an alternative model of personal information, one in which biometric information does not constitute a discrete category. I contended that personal information is defined by four attributes, each of which can be measured according to a ratio or a scale of magnitude. In disentangling these attributes from one another, I demonstrated that "biometrics"—and more specific groupings of personal information, such as "hard biometrics" and "soft biometrics"—are unhelpful and inaccurate. I suggested that this model of personal information provides insight into how we might begin develop more consistent and sustainable policies and laws.

In this chapter, I illustrate the theoretical arguments that I defended in Chapters 3 and 4. In particular, I focus on the implications of my findings for the international regulation of personal information. First, I compare two case studies in order to show that intuitions regarding the collection, use, and analysis of different kinds of personal information are not necessarily logical or helpful. I also use these case studies to demonstrate how a scalar model better describes and interprets the use of personal information.

Second, I suggest how we might integrate a scalar model of personal information into information policy and law. I argue against narrow biometrics legislation and in favor of a more principled, consequentialist approach to

information policy and law. I then extend these conclusions to the realm of international information policy.

5.1 Case Studies

I present two case studies to ground my theoretical arguments in the real world. The first describes U.S. military "biometric" intelligence programs in Afghanistan. The second briefly describes U.S. military "non-biometric" intelligence programs in Afghanistan. A comparative analysis of these cases reveals that the differences between the two programs—and by extension, differences between types of information collected—are not substantively or normatively significant. Furthermore, these case studies support a neutral approach to interpretation and regulation of information technology.

5.1.1 "Biometric" Intelligence in Afghanistan

In 2012, the Economist published a story about the U.S. military and its use of biometrics in Afghanistan. The article described a "ghoulish ritual" in which U.S. soldiers capture fingerprints and iris scans from the corpses of Taliban fighters and enter them into a massive database.[62] This was not the first article to report on the use of biometric surveillance tactics by the U.S. military. However, its tone and focus reflected American discomfort with biometrics; the article casts the new program as part of an invasive surveillance agenda commandeered by a soulless, dystopian, sci-fi military.

[62] "The eyes have it," The Economist, July 07, 2012, http://www.economist.com/node/21558263.

In 2007, General David H. Petraeus commanded a "biometric surge" in Afghanistan. Under Petraeus, the United States military rolled out a massive data collection program.[63] The ultimate goal of the program was "identity dominance," or the "ability to identify and track every single human being in the country and, in the process, make it impossible for the Taliban and other insurgents to live undetected among civilian populations."[64] While the U.S. military has not yet achieved identity dominance in Afghanistan, the Department of Defense biometric database, as of 2010, had stored information about almost one million Afghan citizens.[65] The Department of Defense shares this information with the Department of Homeland Security, the Federal Bureau of Investigation, and intelligence agencies in other nations with which the U.S. has intelligence sharing partnerships.[66] There is little to no oversight of inter-agency and transnational data sharing.

According to a report by Public Intelligence, "there is no formal doctrine or universally accepted tactics, techniques, and procedures for using biometrics throughout the U.S. military."[67] This information is presented as extraordinary—likely because it deals specifically with *biometric* information—even though it does

[63] Thom Shanker, "To Track Militants, U.S. Has System That Never Forgets a Face," The New York Times, July 13, 2011, http://www.nytimes.com/2011/07/14/world/asia/14identity.html.
[64] Sean Gallagher, "Military looks to upgrade its "tactical biometrics" with Identity Dominance System 2," Ars Technica, October 09, 2015, https://arstechnica.com/information-technology/2015/10/military-looks-to-upgrade-its-tactical-biometrics-with-identity-dominance-system-2/.
[65] Jon Boone, "US army amasses biometric data in Afghanistan," The Guardian, October 27, 2010, https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan.
[66] "Identity Dominance: The U.S. Military's Biometric War in Afghanistan," Public Intelligence, April 24, 2014, https://publicintelligence.net/identity-dominance/.
[67] Ibid.

not represent a departure from the protocols (or lack thereof) governing any other military intelligence program.

Not only is the biometric "doctrine" remarkably vague, but the scope of the data-collection program is also ill-defined. General Petraeus ordered a "biometric surge," but the program included the collection of fingerprints, iris scans, facial images, and biographical data and additional imagery, including "name, age, height, weight, birthplace, nationality, scars, marks, and tattoos," according to Marine Corps documents.[68] This information is by no means universally "biological" in nature; the identifiers include a large range of personal information.

It is important to note that the Afghan government also contributes significantly to this massive data collection program. A study published in the National Defense University's Joint Force Quarterly described the Afghan National Security Court as a "model for successful use of biometric evidence in criminal prosecutions."[69] This Court relies heavily on "biometric" evidence to link defendants to forensic evidence. The U.S. has encouraged the Afghan government to expand its biometric program, urging Hamid Karzai, the former Afghan president, to collect fingerprints and iris scans for all Afghan citizens, starting at age 16.[70] It is clear that the U.S. Department of Defense has guided the creation

[68] Sean Gallagher, "Military looks to upgrade its "tactical biometrics" with Identity Dominance System 2," Ars Technica, October 09, 2015, https://arstechnica.com/information-technology/2015/10/military-looks-to-upgrade-its-tactical-biometrics-with-identity-dominance-system-2/.
[69] Ibid.
[70] Jon Boone, "US army amasses biometric data in Afghanistan," The Guardian, October 27, 2010, https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan.

and management of Afghanistan's domestic biometric program, and has absolute access to the national database.

Afghan government officials have justified the biometric surveillance project, in a country where individual identification programs were practically nonexistent prior to U.S. military intervention, by appealing to its potential to curb fraud and corruption.[71] The commander of the U.S. Army's Task Force on Biometrics, Colonel Craig Osborne, said that the collection of biometric data is not useful only for the identification of terrorists and criminals, but that "it can be used to enable progress in society and has countless applications for the provision of services to the citizens of Afghanistan."[72] These endorsements of the new surveillance systems represent an attempt to justify the military program by demonstrating its potential benefits to civil society.

Despite claims that widespread biometric surveillance is a public good, skeptics assert that Afghanistan's "shaky commitment to the rule of law" means that the identifiers collected could easily be turned into weapons.[73] In Iraq, where the U.S. has rolled out a similar "biometric surge," privacy advocates worry that the biometrics database might be repurposed as a military hit list, especially because of widespread corruption, fraud, and malice in local police forces and military units.[74] Privacy advocates in the United States also mounted significant resistance

---

[71] Thom Shanker, "To Track Militants, U.S. Has System That Never Forgets a Face," The New York Times, July 13, 2011, http://www.nytimes.com/2011/07/14/world/asia/14identity.html.
[72] "Identity Dominance: The U.S. Military's Biometric War in Afghanistan," Public Intelligence, April 24, 2014, https://publicintelligence.net/identity-dominance/.
[73] Spencer Ackerman, "U.S. Scans Afghan Inmates for Biometric Database," Wired, August 25, 2010, https://www.wired.com/2010/08/military-prison-builds-big-afghan-biometric-database/.
[74] Ibid.

to the military's biometric program, and have vehemently opposed its imposition on American citizens.[75]

The "biometric" intelligence program in Afghanistan, whatever its normative implications, generated more discourse, both domestically and abroad, than almost any other military intelligence program. Apart from the implementation of some new technologies, the "biometric surge" in Afghanistan does not differ significantly from other intelligence efforts. As such, the rhetoric surrounding this program reflects, at the very least, heightened public interest in "biometrics."

5.1.2 "Non-Biometric" Intelligence in Afghanistan

While civilians in both the United States and Afghanistan paid significant attention to the "biometric surge" in Afghanistan, similar intelligence programs had been quietly underway in the Middle East and elsewhere for many years. Since World War II—perhaps even since World War I—U.S. intelligence agencies have relied on both human and signals intelligence to collect information on the ground and to inform military strategy. Apart from occasional outrage related to the use of "enhanced interrogation tactics," most military intelligence work goes largely unnoticed by the public.

The pursuit of Osama bin Laden involved cooperation between the CIA, the FBI, the NSA, Afghan intelligence agencies, and Pakistani intelligence agencies.

---

[75] Thom Shanker, "To Track Militants, U.S. Has System That Never Forgets a Face," The New York Times, July 13, 2011, http://www.nytimes.com/2011/07/14/world/asia/14identity.html.

This information was also shared with Australia, the United Kingdom, New Zealand, and Canada through the Five Eyes multilateral intelligence network.[76] Intelligence strategies included "enhanced interrogation techniques" (i.e. torture), the widespread surveillance of cellphone communications, and targeted human intelligence.[77]

In Afghanistan, the so-called "non-biometric" intelligence strategies involve the extensive collection of information about both military insurgents and regular civilians for the purpose of achieving military objectives. Intelligence operatives collect personal information, including photographs, names, physical characteristics, and many other identifiers that were classified as "biometric" in the discourse on the Afghan "biometric surge." The difference between "biometric" intelligence programs in Afghanistan and "non-biometric" intelligence programs in Afghanistan was primarily terminological.

5.1.3 A Comparative Analysis

Even a cursory analysis of these two case studies reveals two important facts. First, there is no substantive or normative difference in the kind of information collected. The "biometric" intelligence program included the collection of information ranging from fingerprint to tribal affiliation. Similarly, the "non-biometric" intelligence program included the collection of information ranging birthmarks to

---

[76] "Australian-US intelligence relations – Afghanistan and Iraq," Nautilus Institute for Security and Sustainability, December 21, 2011, http://nautilus.org/publications/books/australian-forces-abroad/afghanistan/intel-relations-afghan-iraq/.
[77] Fred Burton, "The Bin Laden Operation: Tapping Human Intelligence," Stratfor, May 26, 2011, https://www.stratfor.com/weekly/bin-laden-operation-tapping-human-intelligence.

cell phone records. In effect, the two programs are indistinguishable. They both involve the collection, use, and sharing of all different kinds of personal information.

The second fact that comparative analysis of these case studies reveals is that the problems associated with the widespread collection of information has more to do with the method of data collection and the practice of data analysis and sharing than with the kind of information collected. In some cases, the collection of information was ethically problematic (e.g. taking iris scans from corpses and using "enhanced interrogation techniques"). In all cases, the collection, use, and sharing of personal information was almost entirely driven by the U.S. military and unregulated by any external authority. However, these problems did not derive from the *type* of information collected, but rather from the method of information collection and the practices of information sharing.

Melvin Kranzberg, a leading technology theorist, best explains the intuitive objection to supposedly "biometric" technologies. Kranzberg finds that people often laud or abhor certain practices *because* they are new technologies. He argues that the justifications for these reactions are mistaken. According to Kranzberg's First Law of Technology, "technology is neither good nor bad; nor is it neutral."[78] In other words, technology is an empty vessel created by and for humans, and consequently has no inherent normative value. This analysis extends to our discussion of biometrics. The biologicalness of a piece of information is a non-

[78] Melvin Kranzberg, "Technology and History:" Kranzberg's Laws," *Technology and culture* 27, no. 3, 1986, 545.

normative fact. That information alone does not render a piece of information more or less dangerous.

5.3 Biometrics and Information Policy

My primary goal is to redefine "biometrics" within a scalar model of personal information. Specific policy and legislative applications are beyond the scope of this paper. However, I want to suggest how my scalar model of personal information might be relevant to information policy, particularly in an international context. First, I explain why narrow biometric policies and laws are inconsistent and unsustainable. Next, I propose how a universal understanding of biometrics will facilitate a more consistent transnational ethic of personal information. Even if international regulations contradict each other, it is useful to have a more explicit model for understanding and classifying personal information.

5.3.1 Against Narrow Legislation

Several states in the U.S. have passed bills regulating the collection and use of biometric information. Texas and Illinois both have both recently passed specific biometrics bills. Washington State is in the process of passing its own biometrics bill. Each of these laws defines biometrics in slightly different terms. But even if the definitions of biometrics were identical, it would soon become evident that it is impossible to coherently and consistently apply these laws. A piece of legislation that concerns *only* biometric information requires law enforcement agents and courts to distinguish between biometric and non-biometric information. These

laws do not apply to non-biometric information. However, because biometric information is not a discrete category, this is an impossible task. The application of these bills will result in inconsistent case law. Legislatures will have to revise the laws constantly as new technologies emerge.

There is an alternative to this option. Legislatures can develop principled regulations of personal information that concern the methods of collection, the effects of application, and the standards for sharing. In creating broader regulations, the laws will clearly reflect the values of the governing bodies. Furthermore, they will persist over time and evolve alongside the development of new technologies and the emergence of new "kinds" of personal information.

5.3.2 International Biometrics Regulation

The question of how to define biometrics, and how to govern the collection, use, and sharing of personal information more broadly, is inherently transnational in nature. Data are not limited by borders, and are therefore immune to most national protections. There are many contexts in which personal information is collected and shared internationally. My case studies focused on military intelligence, but personal data are also collected and shared by private entities such as multinational corporations, banks, and social media platforms.

It is wildly optimistic to presume that a consistent model of personal information will translate to a consistent model of transnational information policy and regulation. At the very least, however, a model of personal information that accommodates all different kinds of information, and that can evolve

alongside new technologies and new information pathways will facilitate clear communication—across borders as well as cultures—about the regulation of personal information.

5.4 Conclusions

In this chapter, I illustrated the practical implications of the theoretical arguments I defended in Chapters 3 and 4. I compared two case studies of military intelligence in Afghanistan to show how the *type* of personal information is irrelevant to the normative implications of the collection, use, and sharing of personal information. Furthermore, it is almost impossible to determine what is considered "biometric" and is considered "non-biometric" information. This is because "biometric information" does not constitute a discrete category of personal information.

I also proposed how a scalar model of personal information might inform information policy and law. I argued against narrow biometrics legislation and suggest that broader, more principled laws will be more consistent and sustainable. I then argued that while no model of personal information will resolve the problem of international fragmentation in law enforcement, a consistent and coherent model of personal information would, at the very least, guide communication about the transnational regulation of personal information.

6. Conclusion

On January 28, 2001, 71,921 people cheered and booed in the Raymond James Stadium in Tampa, Florida. They were football fans; none of them yet knew or cared that their faces were scanned, transformed into code, and deposited in a database of digital mug shots. Later, when the news broke that the FBI had used the Super Bowl as a testing ground for its new biometric software, technology policy analysts, lawyers, and concerned citizens would express their outrage at the mass collection of biometric information.

But their response was misdirected. While the public had every right to take issue with the FBI program, they should have realized that the fundamental problem had nothing to do with the *type* of information collected. The FBI could have gathered the fingerprints, addresses, or even political identification of each fan. It would not have mattered. It is the method of data collection, the use of personal information, and the storage of that personal information with which the public should have been concerned. The FBI might have violated principles of consent. They might have used the data in ways that infringed upon the constitutional rights of American citizens. They might have stored personal information in a system with insufficient protections. These are all dilemmas worth considering and addressing.

In this paper, I argued that biometric information does not constitute a discrete class of personal information. More broadly, I showed that the *type* of information collected is irrelevant to the legal and ethical consideration of a

personal information technology or program. I proposed a scalar model of personal information that describes each piece of data according to the magnitude of its biologicalness, uniqueness, permanence, and personalness. At the very least, this model provides a common vocabulary and the necessary tools to accurately describe the nature of personal information.

My findings here are preliminary. I have developed a model that might give us some of the necessary tools to build a more consistent and durable regulatory framework, both domestically and internationally. Looking forward, we can consider how to incorporate a more scalar model of personal information into statutory law, how to apply it in the nebulous and secretive context of military intelligence, and how to use it to effectively regulate the transnational flow of personal information.

Bibliography

"1st Finger Scar." Violinist.com. http://www.violinist.com/discussion/response.cfm?ID=23209.yea

"About Us." SEARCH. http://www.search.org/about-search/.

Ackerman, Spencer. "U.S. Scans Afghan Inmates for Biometric Database." Wired. August 25, 2010. https://www.wired.com/2010/08/military-prison-builds-big-afghan-biometric-database/.

Agamben, Georgio. "No to Biopolitical Tattooing." *Le Monde*, January 10, 2004.

Alterman, Anton. "'A piece of yourself': Ethical issues in biometric identification." *Ethics and Information Technology* 5, no. 3 (2003): 139-50.

Appiah, K. Anthony. "Race, culture, identity: Misunderstood connections." *Tanner Lectures on Human Values* 17 (1996): 51-136.

"Australian-US intelligence relations – Afghanistan and Iraq." Nautilus Institute for Security and Sustainability. December 21, 2011. http://nautilus.org/publications/books/australian-forces-abroad/afghanistan/intel-relations-afghan-iraq/.

Barr, Alistair. "Google Mistakenly Tags Black People as 'Gorillas,' Showing Limits of Algorithms." The Wall Street Journal. July 02, 2015. http://blogs.wsj.com/digits/2015/07/01/google-mistakenly-tags-black-people-as-gorillas-showing-limits-of-algorithms/.

"Biometric Security Poses Huge Privacy Risks." *Scientific American.* N.p., 2014. Web. https://www.scientificamerican.com/article/biometric-security-poses-huge-privacy-risks/.

Boone, Jon. "US army amasses biometric data in Afghanistan." The Guardian. October 27, 2010. https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan.

Burton, Fred. "The Bin Laden Operation: Tapping Human Intelligence." Stratfor. May 26, 2011. https://www.stratfor.com/weekly/bin-laden-operation-tapping-human-intelligence.

Canedy, Dana. "Tampa Scans the Faces in Its Crowds for Criminals." The New York Times. July 03, 2001. http://www.nytimes.com/2001/07/04/us/tampa-scans-the-faces-in-its-crowds-for-criminals.html.

Chachere, Vickie. "Biometrics Used to Detect Criminals at Super Bowl." ABC News. http://abcnews.go.com/Technology/story?id=98871&page=1.

Chong, Dennis, and Reuel Rogers. "Racial solidarity and political participation." *Political Behavior* 27, no. 4 (2005): 347-374.

Current and future uses of biometric data and technologies. Issue brief. Science and Technology Committee, U.K. House of Commons. 2015.

Damaševičius, Robertas, Rytis Maskeliūnas, Algimantas Venčkauskas, and Marcin Woźniak. "Smartphone User Identity Verification Using Gait Characteristics." *Symmetry* 8, no. 10 (2016): 100.

"Definition of biometrics." Definition of biometrics. http://www.biometricsinstitute.org/pages/definition-of-biometrics.html.

"Fingerprints and Other Biometrics." FBI. May 03, 2016. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics.

Floridi, Luciano. "The informational nature of personal identity." *Minds and machines* 21, no. 4 (2011): 549.

Gallagher, Sean. "Military looks to upgrade its "tactical biometrics" with Identity Dominance System 2." Ars Technica. October 09, 2015. https://arstechnica.com/information-technology/2015/10/military-looks-to-upgrade-its-tactical-biometrics-with-identity-dominance-system-2/.

Goldman, Kara. "Biometric Passwords and the Privilege against Self-Incrimination." *Cardozo Arts & Ent. LJ* 33 (2015): 211.

Haslanger, Sally. "Gender and Race: (What) Are They? (What) Do We Want Them To Be?" *Nous* 34, no. 1 (2000): 31-55.

"Identity Dominance: The U.S. Military's Biometric War in Afghanistan." Public Intelligence. April 24, 2014. https://publicintelligence.net/identity-dominance/.

Introna, Lucas, and David Wood. "Picturing algorithmic surveillance: The politics of facial recognition systems." *Surveillance & Society* 2, no. 2/3 (2004): 177-198.

Jensen, Christopher. "The more things change, the more they stay the same: Copyright, digital technology, and social norms." *Stanford Law Review* (2003): 531-570.

Jorde, Lynn B., and Stephen P. Wooding. "Genetic variation, classification and 'race'." *Nature genetics* 36 (2004): S28-S33.

Kim, Jaegwon. "Concepts of supervenience." *Philosophy and phenomenological research* 45, no. 2 (1984): 153-176.

Kranzberg, Melvin. "Technology and History:" Kranzberg's Laws"." *Technology and culture* 27, no. 3 (1986): 544-560.

Lyon, David. "Biometrics, Identification And Surveillance." *Bioethics* 22, no. 9 (2008): 499-508.

Lyon, David. *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press, 2003.

Manson, Neil C., and Onora O'Neill. *Rethinking informed consent in bioethics*. Cambridge University Press, 2007.

Mill, John Stuart. *On liberty*. Longmans, Green, Reader, and Dyer, 1869.

Mordini, Emilio. "Ethics and Policy of Biometrics." *Advances in Pattern Recognition Handbook of Remote Biometrics*, 2009, 293-309.

Mordini, Emilio and Sonia Massari. "Body, biometrics and identity." *Bioethics* 22, no. 9 (2008): 488-498.

Newman, Abraham L. "Building transnational civil liberties: Transgovernmental entrepreneurs and the European Data Privacy Directive." *International Organization* 62, no. 01 (2008): 103-130.

Nisenson, Mordechai, Ido Yariv, Ran El-Yaniv, and Ron Meir. "Towards behaviometric security systems: Learning to identify a typist." In *European Conference on Principles of Data Mining and Knowledge Discovery*, pp. 363-374. Springer Berlin Heidelberg, 2003.

Nordland, Rod. "Afghanistan Has Big Plans for Biometric Data." The New York Times. November 19, 2011. http://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html.

Penny, Wayne. "Biometrics: A double edged sword-security and privacy." *SANS Institute* (2002).

Pike, John. "History of Biometrics." Global Security. http://www.globalsecurity.org/security/systems/biometrics-history.htm.

Poudrier, J., 2003. 'Racial' Categories and Health Risks. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, edited by David Lyon, 111.

Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric recognition: Security and privacy concerns." *IEEE security & privacy* 99, no. 2 (2003): 33-42.

Protecting biometric data with Extended Access Control: Securing biometric datasets in electronic identification documents. Technical paper. Entrust, 2014.

Public Attitudes Toward the Uses of Public Attitudes Toward the Uses of Biometric Identification Biometric Identification Technologies by Government Technologies by Government and the Private Sector. Working paper. SEARCH. ORC, 2002.

Rainie, Lee, and Maeve Duggan. "Scenario: Workplace security and tracking." Pew Research Center: Internet, Science & Tech. January 14, 2016. http://www.pewinternet.org/2016/01/14/scenario-workplace-security-and-tracking/.

Recent Opinion Surveys on Public Perception of Biometrics. Issue brief. International Biometrics Identity Association. 2017.

Riley, Chris, Kathy Buckner, Graham Johnson, and David Benyon. "Culture & biometrics: regional differences in the perception of biometric authentication technologies." *AI & society* 24, no. 3 (2009): 295-306.

Ross, Arun, Jidnya Shah, and Anil K. Jain. "From template to image: Reconstructing fingerprints from minutiae points." *IEEE transactions on pattern analysis and machine intelligence* 29, no. 4 (2007).

Ross, Arun, Karthik Nandakumar, and Anil K. Jain. "Introduction to multibiometrics." In *Handbook of Biometrics*, pp. 271-292. Springer US, 2008.

Ross, James. "Datamigrants: Biometrics and the global security complex." 2006.

Sacasas, Michael. "Kranzberg's Six Laws of Technology, a Metaphor, and a Story." L.M. Sacasas. November 17, 2011.

https://thefrailestthing.com/2011/08/25/kranzbergs-six-laws-of-technology-a-metaphor-and-a-story/.

Sahidullah, Md. “Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies". PhD Thesis, 2015.

Schaller, Robert R. "Moore's law: past, present and future." *IEEE spectrum* 34, no. 6 (1997): 52-59.

Shanker, Thom. "To Track Militants, U.S. Has System That Never Forgets a Face." The New York Times. July 13, 2011. http://www.nytimes.com/2011/07/14/world/asia/14identity.html.

Spencer, Quayshawn. "Philosophy of race meets population genetics." *Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences* 52 (2015): 46-55.

"Super Bowl History." FootballDB.com. http://www.footballdb.com/seasons/super-bowls.html.

Sutrop, Margit, and Katrin Laas-Mikko. "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics." *Review of Policy Research* 29, no. 1 (2012): 21-36.

"The eyes have it." The Economist. July 07, 2012. http://www.economist.com/node/21558263.

United Kingdom. U.K. Border Agency. *Privacy Impact Assessment of High Value Data Sharing Protocol*. 2010.

Van der Ploeg, Irma. 2003. "Biometrics and the body as information." *Surveillance as social sorting: Privacy, risk and digital discrimination*, edited by David Lyon. 57-73.

Wadhwa, Vivek. "Laws and Ethics Can't Keep Pace with Technology." MIT Technology Review. September 19, 2014. https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/.

Woodward, John D. "Biometrics: Privacy's foe or privacy's friend?" *Proceedings of the IEEE* 85, no. 9 (1997): 1480-1492.

Woodward, John D. Super Bowl Surveillance: Facing Up to Biometrics. Santa Monica, CA: RAND Corporation, 2001. http://www.rand.org/pubs/issue_papers/IP209.html.

Yanikoglu, Berrin, and Alisher Kholmatov. "Combining multiple biometrics to protect privacy." In *Proc. ICPR-BCTP Workshop*, pp. 43-46. 2004.