Notes

Genetic Privacy in the "Big Biology" Era: The "Autonomous" Human Subject

MARILYN CECH[†]

What do the Golden State Killer, the Havasupai Tribe, and Henrietta Lacks have in common? None of these individuals gave informed consent for the particular research uses of their genetic material. Biotechnological advancements have made what was previously unimaginable—just decades or even years ago—a common reality. Unfortunately, the law evolves at a much slower rate than science. Thus, it may take a radical philosophical shift to make way for new legal frameworks that can provide adequate protections that keep up with scientific progress and withstand the test of time. Currently, a person's "bio-unique data," namely a person's biological material and genetic information, is neither protected as "personally identifiable information" nor "protected health information" under United States federal law. Therefore, our recent breakthroughs in DNA genotyping and sequencing leave individuals particularly vulnerable. This Note uses a discussion of the laws regulating research on human subjects, a group which the world has unanimously agreed must give informed consent, to propose a shift in privacy regulation towards a framework more equipped to handle the new challenges of genetic privacy.

[†] J.D. Candidate 2019, University of California, Hastings College of the Law; Senior Production Editor, *Hastings Law Journal*. Thank you to Tanya Wei and all of the Industry Contract Division at University of California, San Francisco, for providing the inspiration and guidance to begin this Note, and to Professor Lois Weithorn, Professor of Bioethics and the Law, for her invaluable feedback throughout the writing process.

TABLE OF CONTENTS

The voluntary consent of the human subject is absolutely essential.[1]

INTRODUCTION

GEDmatch hosts a public online genealogy database intended to help relatives find each other through similarities in their genetic profiles.[2] Users of the platform are required to create a profile and check a box certifying that they are authorized to upload the deoxyribonucleic acid (DNA) sample because it is either their own, they are the legal guardian of the person to whom the DNA belongs, or they have "obtained authorization" from the person to whom the DNA belongs.[3] This check-the-box certification did not prevent investigators from fabricating a profile to gain access to the platform and entering a DNA sample obtained from a crime scene decades earlier in the hopes of generating leads in a cold case.[4] GEDmatch then unwittingly provided the undercover investigators with a family tree that identified over one hundred potential relatives of the source of the DNA sample.[5]

After pursuing a couple of false leads, police eventually narrowed in on Joseph James DeAngelo, Jr., a former police officer who was the right age and had geographic ties to the communities affected by the "Golden State Killer."[6] While most are glad to see the alleged twelve-time murderer and fifty-time rapist who terrorized neighborhoods throughout California[7] behind bars, these events illustrate just one way in which a person's genetic privacy can be infringed.

Many people unintentionally expose themselves to the risk of DNA privacy breaches, for example, by leaving DNA at crime scenes,[8] by using direct-to-consumer DNA test at home kits,[9] or by donating tissue samples to science. This Note focuses on the recent threats to privacy using tissue sample donors as an example. These participants in human subject research should enjoy the protections of informed consent but are often uninformed as to the extent to which their genetic information may be used and scientists' new ability to re-

1. THE NUREMBERG CODE (1947), *reprinted in* BARRY R. FURROW ET AL., BIOETHICS: HEALTH CARE LAW AND ETHICS 506, 507 (7th ed. 2013).

2. *Your DNA Is Not Your Own: How the Golden State Killer Hunt Reveals the Limits of Medical Privacy*, ADVISORY BOARD (Apr. 30, 2018, 11:00 AM), https://www.advisory.com/daily-briefing/2018/04/30/dna.

3. *Id.*

4. *Id.*

5. Susan Scutti, *What the Golden State Killer Case Means for Your Genetic Privacy*, CNN (May 1, 2018, 12:01 AM), https://www.cnn.com/2018/04/27/health/golden-state-killer-genetic-privacy/index.html.

6. Benjamin Oreskes et al., *False Starts in Search for Golden State Killer Reveal the Pitfalls of DNA Testing*, L.A. TIMES (May 4, 2018, 5:00 AM), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-dna-20180504-story.html.

7. *See* Scutti, *supra* note 5.

8. *See* Elizabeth R. Pike, *Securing Sequences: Ensuring Adequate Protections for Genetic Samples in the Age of Big Data*, 37 CARDOZO L. REV. 1977, 2019 (2016). *See generally* Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN'S L.J. 3 (2010) (discussing the privacy implications of familial searches by law enforcement within criminal DNA databases).

9. *See generally* Deepthy Kishore, *Test at Your Own Risk: Your Genetic Report Card and the Direct-to-Consumer Duty to Secure Informed Consent*, 59 EMORY L.J. 1553 (2010) (proposing that courts impose a duty on genetic testing companies to give warnings to their customers akin to a physician's duty of informed consent).

identify anonymized samples. Further, this Note grapples with the question of whether increased transparency in scientific research would benefit individuals, and the community as a whole, or unduly burden scientific advancement.

Science is outpacing the legislature's awareness of and ability to pass appropriate regulations to manage the privacy risks facing both willing and unwitting[10] research participants. While scientists are revolutionizing medicine with the discovery of the human genome,[11] ethicists and the scientific community are beginning to question whether the escalating costs to the individual will continue to be worth the benefit to the community. Perhaps though, the question is not whether community welfare should be valued over individual autonomy, but whether society will recognize that human dignity, as a philosophical concept and fundamental right, requires respect for both the individual and humanity. If the "big data era" is indeed the "post-privacy age," where privacy is more of a myth than a reality, and the free exchange of information has valuable benefits,[12] it is our conception of human dignity, not individual autonomy, that needs to be safeguarded.

Universal principles of bioethics dictate that human experimentation requires the express, voluntary, and informed consent of human subjects.[13] In the context of human subject research, "informed consent" refers to participants giving permission to research subjects *only* after they understand the potential consequences of participation in the study, including any risks, benefits, or waivers of rights.[14] One big risk that researchers and participants alike tend to underestimate is breach of information privacy. Traditionally, and as the law developed, society was more concerned with cruel treatment by physical abuses to the bodies of fellow human beings.[15]

---

10. When a person goes to the doctor to have blood drawn or another medical procedure that requires the collection of a tissue sample, the leftover portions not needed for testing may be discarded or, as is often the case, may be retained in a biobank and made available for use by researchers. Pike, *supra* note 8, at 1988, 1992 (discussing the common misunderstanding of "medical waste" and suits against Texas and Minnesota brought by parents concerned with the unconsented research use of newborn bloodspot samples after mandatory screening for genetic diseases). While anonymous tissue samples used to pose little risk to individual privacy, that is certainly no longer the case with new DNA technology. *See, e.g.*, Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 SCIENCE 321, 321–24 (2013) (re-identifying the individuals who anonymously donated DNA samples to the HapMap project).

11. Edward S. Dove, *Biobanks, Data Sharing, and the Drive for a Global Privacy Governance Framework*, 43 J.L. MED. & ETHICS 675, 678 (2015) ("The [Human Genome Project] revealed more than 99% of the complex structure of the human genome through the successful sequencing and publication of its complete sequence.").

12. *See* ANDREAS WEIGEND, DATA FOR THE PEOPLE: HOW TO MAKE OUR POST-PRIVACY ECONOMY WORK FOR YOU 6 (2017) (advocating for increased transparency and agency for individuals in the use of their data because true privacy is no longer feasible in the age of big data).

13. *See* OFFICE OF THE SEC'Y, THE NAT'L COMM'N FOR THE PROT. OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAVIORAL RESEARCH, THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH (1979), https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf [hereinafter BELMONT REPORT] (applying its general ethics principles to the requirement of informed consent).

14. *What Is Informed Consent?*, NIH NAT'L LIBR. MED. (Feb. 19, 2019), https://ghr.nlm.nih.gov/primer/testing/informedconsent.

15. *See infra* Subpart I.A.1.

While the medical field has long recognized the sensitive and personal nature of health information, new research practices, medical initiatives, and biotechnology expand the categories of information that are sensitive and personal to unique individuals.[16] Recent breakthroughs in genetic research, such as "genome sequencing," generating code for the entire strand of DNA, have shown that a person's cells have the ability to reveal large amounts of "bio-unique information."[17] Additionally, advancements in technology make this information more easily accessible and easily shared;[18] thus, it is more vulnerable than it has ever been. Indeed, ensuring health information privacy may no longer be possible.[19]

Recent controversies illustrate that the framework of privacy laws in the United States is ill-equipped to confront the realities of the big data era, in which the collection, use, and exchange of a person's bio-unique data is widespread.[20] While the problem has not been overlooked, proposals for new methods and regulations to preserve individual autonomy and protect privacy either threaten to burden the exciting new path of medical discovery or offer little practical improvement.[21] The European Union (EU), however, has a privacy framework that is more comprehensive that includes informational privacy, recognizes data privacy as a fundamental right, provides stricter regulations for sharing personal information without consent, and has harsher penalties for data misuse.[22] The EU's data subject rights model embraces the rights to "personal dignity" and "informational self-determination,"[23] fundamental philosophies that make it a better starting point for the future of privacy regulation.[24] The United States must recognize the inadequacies in its privacy-informed consent framework in this

16. *See* Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7151 (Jan. 19, 2017) (codified at 45 C.F.R. pt. 46 (2018)).

17. *Id.* at 7151, 7163–64.

18. *Id.* at 7151.

19. Jeantine E. Lunshof et al., *From Genetic Privacy to Open Consent*, 9 NATURE 406, 406 (2008) ("Developments in both medical informatics and bioinformatics show that the guarantee of absolute privacy and confidentiality is not a promise that medical and scientific researchers can deliver any longer.").

20. *See* Wash. Univ. v. Catalona, 490 F.3d 667 (8th Cir. 2007) (ruling against patients who wanted to transfer their donated samples with the investigator to another university to continue the desired research); Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990) (holding that patient did not have a property right in his tissue after removal, but that physician breached his disclosure obligations in failing to disclose preexisting research and economic interests prior to obtaining consent to perform the medical procedure).

21. Jocelyn Kaiser, *Update: U.S. Abandons Controversial Consent Proposal on Using Human Research Samples*, SCI. MAG. (Jan. 18, 2017, 4:15 PM), http://www.sciencemag.org/news/2017/01/update-us-abandons-controversial-consent-proposal-using-human-research-samples.

22. LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW: PRACTICAL GUIDE AND COMMENTARY U.S. FEDERAL AND CALIFORNIA LAW § 1-5:4 (Joni N. McNeal ed., 3d ed. 2018).

23. James Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

24. *But see* Tal Z. Zarzky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 996 (2017) (arguing that the GDPR is utterly incompatible with the Big Data era, that it will soon be irrelevant in the EU, and that it will stall innovation in Europe without providing its citizens greater privacy protection).

age of advancing biotechnology to enable its laws to evolve as science progresses.

Part I introduces the doctrine of informed consent, discusses its evolution, and recognizes some problems in current practice. Part II discusses the prominent U.S. federal privacy protections for health information and compares its patchwork of laws to the data privacy framework in the EU, particularly its new General Data Protection Regulation (GDPR). Part III examines how the fundamental differences in privacy philosophies between the EU and the United States better situate the EU for controlling information privacy. Finally, Part IV advocates for the treatment of health data as sensitive personal data, proposes the adoption of an EU data subject right privacy model, and recommends embracing technology and a big data solution with dynamic consent to address emerging privacy concerns.

I. INFORMED CONSENT

A. THE DOCTRINE OF INFORMED CONSENT

Informed consent necessitates that a human research subject authorizes the anticipated medical procedure or research study prior to its performance and requires that the permission be given voluntarily and with knowledge of the facts, risks, and benefits to the individual human research subject.[25] This is true in cases where there is a risk of bodily harm to the research subject, as the doctrine developed historically, and also where there are information privacy risks.[26] The idea that voluntary informed consent is a prerequisite to human experimentation is rooted in the bioethical principle of autonomy[27] and has been immortalized by the Supreme Court's reading of an individual's fundamental right to privacy in the Fifth Amendment of United States Constitution.[28]

1. The Basis of Informed Consent in the United States

The use of human subjects in biomedical research is invaluable. Yet, in practice, it is difficult to strike a balance between preserving the privacy rights of individual participants and minimizing administrative burdens on scientists, which impede scientific discoveries. Several ethical tragedies brought the concept of "informed consent" to the forefront of human subject research for the United States. Significantly, the Nuremberg Code of 1947 (the Code), also

25. *What Is Informed Consent?*, *supra* note 14.

26. *Id*.

27. *See, e.g.*, Schloendorff v. Soc'y of N.Y. Hosp., 105 N.E. 92, 93 (N.Y. 1914) ("Every human being of adult years and sound mind has a right to determine what shall be done with his own body . . . .").

28. Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (concluding that although privacy is not a right enumerated in the Constitution or the Bill of Rights, privacy is an overarching right created by the "penumbra" of enumerated rights that protect some aspect of privacy).

known as the "ten commandments of [human subject research]"[29] or "the most important document in the history of the ethics of medical research,"[30] was drafted in the aftermath of World War II during the Nuremberg War Crime Trials, in which Nazi doctors were charged with "conducting murderous and torturous human experiments in the concentration camps."[31] The Code declares: "The voluntary consent of the human subject is absolutely essential."[32] It further explains that voluntary consent requires that the subject "have legal capacity to give consent," "be able to exercise free power of choice," and "have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision."[33] Additionally, the Code warns researchers against accepting consent that is not informed, that is, consent lacking "the nature, duration, and purpose of the experiment; the method and means by which it is to be conducted; all inconveniences and hazards reasonably to be expected; and the effects upon his health or person which may possibly come from his participation in the experiment."[34]

The first federal U.S. policy for the protection of human subjects was established in 1953 for research conducted at the National Institutes of Health Clinical Center (NIH) or receiving federal funding for the objective prospective review of proposed research.[35] Then, following the publicity of the infamous Tuskegee Syphilis Study,[36] the enactment of the National Research Act of 1974 required the Department of Health, Education, and Welfare to codify its policy for the protection of human subjects and formed the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research to draft the Belmont Report.[37] The Belmont Report identifies three broad ethical principles to guide the conduct for research of human subjects and under which

29. Kristine M. Severyn, *The Nazi Doctors and the Nuremberg Code*, 4 J. PHARMACY & L. 167, 167 (1995) (reviewing GEORGE J. ANNAS & MICHAEL A. GRODIN, THE NAZI DOCTORS AND THE NUREMBERG CODE: HUMAN RIGHTS IN HUMAN EXPERIMENTATION (1992)).

30. Evelyne Shuster, *Fifty Years Later: The Significance of the Nuremberg Code*, 337 NEW ENG. J. MED. 1436, 1436 (1997).

31. *Id*.

32. THE NUREMBERG CODE, *supra* note 1, at 507.

33. *Id.*

34. *Id.*

35. OFFICE OF EXTRAMURAL RESEARCH, NAT'L INSTS. HEALTH, PROTECTING HUMAN RESEARCH PARTICIPANTS 6 (2018), https://grants.nih.gov/sites/default/files/PHRP_Archived_Course_Materials_English.pdf [hereinafter PROTECTING HUMAN RESEARCH PARTICIPANTS].

36. In the Tuskegee Syphilis Study (1932–1972), the U.S. Public Health Service selected and studied four hundred poor black males from the small town of Tuskegee, Alabama who were infected with syphilis. Walter T. Champion, Jr., *The Tuskegee Syphilis Study as a Paradigm for Illegal, Racist, and Unethical Human Experimentation*, 37 S.U. L. REV. 231, 231–32 (2010). Rather than treating the infected men, researchers observed the men to study the progression of the disease. *Id.* Participants gave consent which was not informed believing that they were receiving free treatment for their participation in the study, when in fact treatment was withheld when it became available so that the study could continue without interruption. *Id.*

37. PROTECTING HUMAN RESEARCH PARTICIPANTS, *supra* note 35, at 7, 11.

to formulate, criticize, and interpret new rules.[38] First, "respect for persons" mandates that individuals are treated as autonomous agents and states that all people are entitled to protection.[39] Second, "beneficence" emphasizes that people are to be "treated in an ethical manner not only by respecting their decisions and protecting them from harm, but also by making efforts to secure their well-being."[40] And third, "justice" discusses balancing the burden and benefit to the research subject and distributing such burdens and benefits fairly to society as a whole.[41]

2. The Pre-2018 Federal Common Rule

The ethical principles of the Nuremberg Code and the Belmont Report guided certain federal agencies to enact regulations to ensure the ethical treatment and protection of human subjects—namely the Department of Health and Human Services (HHS) Basic Policy for Protection of Human Research Subjects (the Common Rule)[42] and the Food and Drug Administration (FDA) Protections of Human Subjects.[43] The Common Rule was published in 1981 by HHS and codified in separate regulations by fourteen additional federal departments and agencies.[44] The Common Rule outlines the basic provisions for review of research proposals by institutional review boards, informed consent requirements, and ongoing review for compliance for federally funded studies.[45]

Under the pre-2018 Common Rule, informed consent is required only if a particular study involves direct contact with a "human subject."[46] Human subject means "a living individual about whom an investigator (whether professional or student) obtains (1) Data through intervention or interaction with the individual, or (2) Identifiable private information."[47] "Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator associated with the information) in order for obtaining the information to constitute research involving human subjects."[48]

Essentially, research that uses leftover tissue or data from prior research without information that identifies a particular person, does not involve direct contact or association with a person; thus is not "research involving human subjects."[49] Therefore, informed consent is typically not required before using or sharing a person's bio-unique information as long as their identity cannot

38. BELMONT REPORT, *supra* note 13.

39. *Id.*

40. *Id.*

41. *Id.*

42. 45 C.F.R. §§ 46.101–.124 (2009) (amended 2018).

43. 21 C.F.R. §§ 50.20–.27 (2009) (amended 2018).

44. *See* PROTECTING HUMAN RESEARCH PARTICIPANTS, *supra* note 35, at 8.

45. *Federal Policy for the Protection of Human Subjects ('Common Rule')*, OFF. HUM. RES. PROTECTIONS (Mar. 18, 2016), https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.

46. 45 C.F.R. § 46.102(f) (2009) (subject to certain exceptions as provided in § 46.101).

47. *Id.*

48. *Id.* (emphasis omitted).

49. *Id.*

"readily be ascertained."[50] This makes a person's informational privacy particularly vulnerable because sharing de-identified data is a common practice among researchers.

Notably, slight revisions have been made to these definitions "for clarity."[51] The definition of "human subject" replaced the term "data" with "information or biospecimens" and, in addition to "obtains," added "uses, studies, analyzes, or *generates*."[52] Additionally, "identifiable" is now properly defined as part of two new defined term "identifiable private information" and "identifiable biospecimen" although retaining the language in "private information" quoted above.[53] The gist of these changes was to include biospecimen in these definitions, a big (even if unintentional) step forward in acknowledging biospecimens as potentially identifiable.

On the other hand, the addition of the word *generates* potentially brings a new situation within the reach of the Common Rule—secondary research where a researcher obtains de-identified data not subject to the Common Rule, such as an anonymous biospecimen, and through manipulation of the specimen generates identifiable data. Before this addition, it was unclear if a researcher in this situation would be subject to the regulations and certainly it would be impracticable to comply with obtaining informed consent. Researchers often side-stepped this uncertainty by including a provision in their Material/Data Transfer Contracts containing a promise not to reidentify the data obtained.

Although the intent apparently was to keep the definitions substantively the same,[54] it has yet to be seen what practical effect these changes will have on informed consent requirements and whether they will be interpreted in favor of increased privacy protections for subjects who traditionally were not considered "human subjects" but whose rights are increasingly implicated nonetheless. Informed consent has become a tool to allow people to voluntarily consent to privacy risks, but it has also become apparent that the scope of the doctrine is both too narrow and too cumbersome in practice such that it is an inadequate formality, excluding scenarios where people would want informed consent and only requiring minimal disclosures that do not allow for a full understanding of the privacy the risks.[55]

50. *Id.*

51. *Common Rule 2019*, STAN. RES. COMPLIANCE OFF., https://researchcompliance.stanford.edu/panels/hs/common-rule#hs (last visited Mar. 19, 2019) [hereinafter *Common Rule 2019*].

52. 45 C.F.R § 46.102(e)(1) (2018) (emphasis added).

53. *Id.* § 46.102(e)(5)–(6).

54. *See Common Rule 2019*, *supra* note 51.

55. *See generally* Robert F. Weir & Jay R. Horton, *DNA Banking and Informed Consent: Part 1*, IRB: ETHICS & HUM. RES., July–Aug. 1995, at 1, 1–4 (1995) (examining what "the reasonable participant" expected to learn prior to participation where the genetic research projects involved DNA banking and storage); *Informed Consent for Genetics Research*, NIH NAT'L HUM. GENOME RES. INST., https://www.genome.gov/27026588/informed-consent-for-genomics-research (last updated Jan. 8, 2018) (noting that the NIH was the first to recognize a heightened standard for informed consent for genetics research despite the rejection of proposed changes in the NPRM and providing guidance for its own funded studies).

3. Revised Common Rule

For almost three decades, the Common Rule was left untouched while the technology surrounding genome research advanced dramatically.[56] Traditionally common scientific practices, such as using leftover samples from medical procedures for research and data for secondary research, are starting to cause concern given the ability to match an anonymous sample with the original donor through DNA analysis and further derive meaning from the DNA.[57] In 2011, proposals to revise the Common Rule aimed to address new issues such as informed consent for biological samples and the increased vulnerability of health information inherent in decoding and analyzing uniquely individual DNA.[58] The revisions proposed in the Notice of Proposed Rulemaking (NPRM) in 2015 *might* have answered many of these newly emerging questions, but the most progressive revisions were not adopted.[59]

On January 19, 2017, the Office for Human Research Protections (OHRP) and the HHS published the revised Common Rule (or Final Rule) which purportedly aims to "modernize, strengthen, and make more effective" the regulations and is "intended to better protect human subjects involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators."[60] The effective date, originally January 19, 2018, has been delayed twice for periods of six months each—finally settled at January 21, 2019.[61]

Among the NPRM's exciting proposed revisions affecting the field of genomics were: (1) several alternative proposals for expanding the definition of "human subject" to cover research with all biospecimens regardless of identifiability, or if the intent was "to generate the genome or exome sequence" or "information unique to an individual;"[62] (2) expanding the definition of "identifiable private information" at the least to match the term "personally

56. Holly Fernandez Lynch, *A New Day for Oversight of Human Subjects Research*, HEALTH AFF.: HEALTH AFF. BLOG (Feb. 6, 2017), http://healthaffairs.org/blog/2017/02/06/a-new-day-for-oversight-of-human-subjects-research.

57. *See* John Bohannon, *Genealogy Databases Enable Naming of Anonymous DNA Donors*, 339 SCIENCE 262, 262 (2013); Gymrek et al., *supra* note 10, at 321–24.

58. Lynch, *supra* note 56.

59. *Id.*; *see also* Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7150 (Jan. 19, 2017) (codified at 45 C.F.R. pt. 46 (2018)) (summarizing proposals set forth in the NPRM that were not ultimately adopted in the final rule).

60. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. at 7149, 7232.

61. Federal Policy for the Protection of Human Subjects: Delay of the Revisions to the Federal Policy for the Protection of Human Subjects, 83 Fed. Reg. 2885 (Jan. 22, 2018); Federal Policy for the Protection of Human Subjects: Six Month Delay of the General Compliance Date of Revisions While Allowing the Use of Three Burden-Reducing Provisions During the Delay Period, 83 Fed. Reg. 28,497 (June 19, 2018). The second delay provides that institutions may elect to begin certain "burden-reducing" and institution-friendly provisions, while the *few* subject-friendly provisions that made it into the Final Rule are subject to the delay. *See id.*

62. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. at 7163–64, 7200–01 (Section III. Definitions for Purposes of this Policy and Section VI. Protection of Identifiable Private Information and Identifiable Biospecimens respectively).

identifiable information" used in some federal privacy statutes;[63] and (3) the addition of a new "basic element of [informed consent]" that requires a statement describing whether or not identifiers will be removed from information or biospecimens and used in future research without additional consent.[64] However, these proposals, which would have significantly increased the protection of genomic data used in research, were not adopted in the Final Rule.[65]

"[T]he proposal set off alarm bells [in the scientific community] because it would have imposed new rules for research using blood, urine, tissue, and other specimens leftover from clinical care or a specific research study."[66] Proponents of the expanded definition of "human subject" could not agree which alternative proposals were the best in terms of (1) planning for future technology, (2) balancing the Belmont Report's ethical principles of autonomy, beneficence, and justice, and (3) giving rights in the "bio-unique information" back to the subject.[67] Opponents of the changes argued that expanding the definitions of both "human subject" and "identifiable private information" would create huge costs and administrative burdens because they would require tracking informed consent for an exponentially growing number of participants, or alternatively, scaring away potential participants by asking for consent that is too broad.[68] They also argued that changes would create new privacy concerns because the samples would need to be linked to an informed consent tracking system, which would prevent the samples from ever truly being de-identified.[69] This argument is circular because the proposed new definition of "human subject" would have acknowledged that biospecimens are inherently unique and that removing donors' names will never be enough—that de-identification is not possible.

The biospecimen proposals were a reaction to infamous cases, such as those of Henrietta Lacks and the Havasupai Indians, which both involved the unauthorized but legal use of leftover samples.[70] Henrietta Lacks was an African American woman who was treated for cervical cancer at Johns Hopkins Medical Center.[71] A sample of cancerous tissue, taken during a biopsy and used for subsequent research without consent, proved to be infinitely valuable to scientific research because of her cells' rare ability to multiply infinitely.[72] This immortal cell line (named HeLa) played an important role in "research into the

63. *Id.*

64. *Id.* at 7214–15 (Section XIV. General Provisions for Informed Consent).

65. *See id.* at 7150 (summarizing proposals not adopted).

66. Kaiser, *supra* note 21.

67. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. at 7165–68.

68. *Id.* at 7168, 7202; Kaiser, *supra* note 21.

69. Kaiser, *supra* note 21.

70. *Id.*

71. *Henrietta Lacks*, LACKS FAMILY, http://www.lacksfamily.net/henrietta.php (last visited Mar. 19, 2019). *See generally* REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (2010) (telling the story of Henrietta Lacks through interviews with her family, scientists, and others affected by the HeLa cell line).

72. SKLOOT, *supra* note 71, at 4.

genes that cause cancer and those that suppress it; [and] helped develop drugs for treating herpes, leukemia, influenza, hemophilia, and Parkinson's disease" and have been influential in countless other studies.[73] In 2013, the HeLa cell's DNA sequence was published in a public database as part of the mandatory disclosure of data accompanying publication of a study.[74] This publication breached the privacy interests of the entire Lacks family due to genetic similarities within families.[75]

The Havasupai, an Arizona Native American tribe, gave specific consent when donating blood samples for research on the prevalence of diabetes within their tribe.[76] In 2010, the Havasupai "issued a 'banishment order' to keep Arizona State University employees from setting foot on their reservation"[77] when they learned that University researchers had used the tribe's blood samples for research beyond diabetes research,[78] including DNA research that revealed the geographical origins of the tribe subsequently devastating the tribe's Grand Canyon origin story.[79]

Harkening back to the Final Rule, there is one adopted provision that promises reform is coming, even if the scientific community is not receptive just yet:

> The Final Rule requires the Common Rule departments and agencies to re-examine the definition of the terms "identifiable private information" and "identifiable biospecimen." It also requires them to assess whether there are "analytic technologies and techniques that should be considered by investigators to generate identifiable private information or identifiable biospecimens."[80]

These reviews will occur at least once every four years, beginning one year from the effective date.[81] The resulting recommendations on consent, privacy, and data protections will then go through a public comment process.[82] "The preamble to the rule specifically notes that whole genome sequencing is expected to be one of the first technologies to be evaluated to determine if it should be on this list."[83]

B. PROBLEMS POSED BY ADVANCES IN BIOTECHNOLOGY

For decades, there has been a "robust anonymization assumption"—a supposition that if a sample is stripped of all personally identifying information,

---

73. *Id.*

74. John Arst, *Sharing the Whole HeLa Genome*, ASBMB TODAY, Feb. 2017, at 12, 13.

75. *Id.*

76. Amy Harmon, *Indian Tribe Wins Fight to Limit Research of Its DNA*, N.Y. TIMES (Apr. 21, 2010), http://www.nytimes.com/2010/04/22/us/22dna.html?pagewanted=all.

77. *Id.*

78. *Id.*

79. *Id.*

80. *Highlights of Revisions to the Common Rule*, NIH NAT'L HUM. GENOME RES. INST. (Mar. 7, 2017), https://www.genome.gov/27568212/highlights-of-revisions-to-the-common-rule.

81. *Id.*

82. *Id.*

83. *Id.*

such as names, dates, and locations, then it is not possible to link that sample back to the subject.[84] Thus, anonymization and de-identification were considered the best ways for researchers to make efficient and ongoing use of collected samples without compromising a subject's right to privacy.[85] However, de-identification can no longer ensure the protection of a participant's privacy by disassociating the person's identity from the study. Scientists, with the help of rapidly advancing biotechnology, can now decode DNA, making a person's unique DNA highly identifiable[86] and the sensitive information coded therein accessible to others. Genome sequencing preserves the connection between the participant and future research, so the practical definition of "direct" human contact needs to be expanded accordingly. The inability to truly disassociate the participant from the research poses a significant problem to privacy.

The concepts of privacy, consent, and autonomy are delicately intertwined. When giving informed consent, one gives permission for participation in research by weighing the benefits against the risks and consenting to the possible risks. Stronger privacy protections would decrease the risk of privacy breaches or the potential consequences of such breaches for the individual, such as genetic discrimination or stigma for carrying certain traits. Weaker privacy protections necessarily require the individual to consent to a greater risk of genetic information misuse. If people had control over their own information and could exercise their own autonomous choices about the uses of their bio-unique information, informed consent could be strong.

Currently, human subjects erroneously believe they are fully informed as to what will be done with their protected health information and genetic materials (and researchers think they are obtaining informed consent). However, many study participants cannot imagine, and are not actually provided with, a realistic idea of the sort of privacy risks, especially future risks, to which they are consenting. Therefore, the consent is not informed and is invalid. Furthermore, while confidentiality of information might feel like the best solution from the perspective of the participant, it also slows scientific progress. Thus, it is important to strike a compromise between the interests of the individual and the interests of society.

The practice of de-identification can also negatively impact volunteer research subjects.[87] De-identification limits research participants' ability to control their data, including making withdrawal from a research study nearly impossible.[88] It can also prevent researchers from being able to return individual

84. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706–07 (2010).

85. *Id.* at 1703–04.

86. *See, e.g.*, Gymrek et al., *supra* note 10 (conducting a study specifically to see if it is possible to reidentify de-identified samples from anonymous research participants and concluding that it is possible).

87. Dove, *supra* note 11, at 680–81.

88. *Id.*

results to participants.[89] Additionally, the more information about individuals available publicly or through other studies, the less effective "de-identifying" becomes because information previously stripped from the data to protect the individual's identity can be re-matched; thus the participant can be re-identified.[90]

1. Re-Identification from Genomic Data

While data sharing has opened up a whole new realm of research, it has also created a whole new realm of privacy concerns. Recently, researchers have proven the scientific community's worst fear: that the widespread public availability of personally identifying data paired with the technology to analyze DNA makes re-identification possible.[91]

In 2013, Melissa Gymrek and fellow researchers questioned whether anonymous participants from a previous study were really anonymous.[92] The study shows that "surnames can be recovered from personal genomes by profiling short tandem repeats on the Y chromosome (Y-STRs) and querying recreational genetic genealogy databases."[93] Using only a free public genealogy search engine and thirty-four identifiers on a Y chromosome as a test, the study "project[ed] a success rate of ~12% . . . in recovering surnames of U.S. Caucasian males" using just one search engine.[94] The other eighty-three percent were unknown because there were no matches in that particular search engine.[95] After uncovering the surname, the researchers were able to add demographic data to "narrow down the identity of the sample originator to just a few individuals."[96] The more identifiers that were added (such as age) the smaller the list of potential matches, many of which were within the same family.[97] While the study originally identified only male donors via matches of the Y chromosome, the information learned about family lines enabled the researchers to identify female donors too.[98]

Gymrek's study was not the first to raise alarms about the possibility of re-identifying DNA. For example, an older study used single nucleotide polymorphisms (SNPs), another unique identifier on DNA, to identify individuals from "seemingly anonymous pools of DNA data."[99] Additionally, "[i]n a number of public cases, male adoptees and descendants of anonymous

89. *Id.* Some research participants may want to be notified if a gene is discovered in their DNA which predisposes them to a disabling illness. Conversely, others may want to live without this knowledge.

90. *Id.*

91. *See generally* Gymrek et al., *supra* note 10.

92. *Id.*

93. *Id.* at 321.

94. *Id.* at 322.

95. *Id.*

96. *Id.*

97. *Id.*

98. Bohannon, *supra* note 57, at 262.

99. *Id.*

sperm donors used recreational genetic genealogy services to genotype their Y-chromosome haplotypes and to search the companies' databases" to determine the identity of their biological fathers.[100] If individuals are uniquely identifiable from matching patterns in only partially decoded DNA, then the danger is greater now that technology enables full DNA sequencing.

In response to Gymrek's study, the National Institutes of Health (NIH), which hosts public genome databases for use by researchers, decided to remove identifying information from some databases and restricted access to others.[101] Although there have been no reported cases of malicious DNA re-identifying to date, the future safety of DNA anonymity is uncertain.[102] There is a danger that it will become profitable to decode DNA or re-identify data for marketing, commercial, crime solving, or other purposes. While this process may require special knowledge and skill, re-identification likely will become easier with time as the wealth of publicly available data increases and technology improves.[103]

2. Scientific Research Practices Regarding Tissue Samples and Data

Scientific and technological advancements have facilitated the emergence of a whole new type of scientific research that promises to treat and cure many diseases that plague humankind. Genetic research provides information about humans in general, and information unique to individuals in particular. Modern pursuits in genetics could revolutionize medicine by allowing scientists to identify genes that predispose a person to a particular disease and tailor treatments to each individual person with Precision Medicine.[104]

Genome-wide association studies, and other large-scale studies, require amassing substantial amounts of genetic and health-related data so that patterns in the genomes of individuals can be identified.[105] Biobanks provide a great resource for scientists to access the enormous amounts of bio-specimens and data required for "large-scale genomic analysis," termed "big biology," a tip of

100. Gymrek et al., *supra* note 10, at 321.

101. *Id.*

102. One re-identification study targeted a particular individual. In 2010, MITgraduate student Latanya Sweeney was able to re-identify" Massachusetts Governor William Weld using knowledge that Weld had collapsed on stage while receiving an honorary doctorate from the Bentley College, a voter list, and "a dataset released by the Massachusetts Group Insurance Commission to improve healthcare and control[] costs." Mark Van Rijmenam, *The Re-Identification of Anonymous People with Big Data*, DATAFLOQ, https://datafloq.com/read/re-identifying-anonymous-people-with-big-data/228 (last visited Mar. 19, 2019).

103. Interestingly enough, maybe privacy has lagged so far behind scientific advancement that now we can use science and technology to address privacy concerns. In 2017, a study demonstrated that genomic diagnoses could be made while keeping more than ninety-nine percent of the most sensitive genetic information private. *See* Karthik A. Jagadeesh et al., *Deriving Genomic Diagnoses Without Revealing Patient Genomes*, 357 SCIENCE 692 (2017). This approach to achieving data privacy would require tremendous trust in the scientific community.

104. *See What Is Precision Medicine?*, NIH NAT'L LIBR. MED. (Feb. 19, 2019), https://ghr.nlm.nih.gov/primer/precisionmedicine/definition.

105. *Genome-Wide Association Studies*, NIH NAT'L HUM. GENOME RES. INST., https://www.genome.gov/20019523/genomewide-association-studies-fact-sheet/ (last updated Aug. 27, 2015).

the hat to the big data era.[106] Biobanks are "designed and operated to collect, store, analyze, curate, and distribute biological specimens and data for future, as-yet unspecified research as approved by an ethics committee or a comparable body."[107]

Sharing data and results among researchers is essential to the efficacy of this new age of research, but it also poses a two-fold problem. First, privacy and informed consent regulations apply differently to different types of organizations (that is, private or public, government-funded, foreign entities)[108] and to different types of samples, which creates a maze of often confusing regulations and guidelines, undesirable gaps in protection, and a lack of redress in cases of privacy breaches.[109] Second, when a participant gives consent for his specimen or data to be stored in a biobank for use in research, he must agree broadly to unspecified future research.[110] Broad consent is worrisome because the participant loses control over and knowledge about who has access to his information and future research uses.

Some of the misunderstandings between the researcher and the participant regarding privacy expectations might stem from the underlying traditional physician-patient relationship and the implied duty of confidentiality. "The finding that the confidentiality of genetic data cannot be guaranteed suggests that a research participant's consent might not be valid when it is conditioned on the assurance or even the unchallenged expectation of full genetic secrecy."[111] "[C]ommon and widely used consent practices might in fact result in disingenuous consent, at least insofar as they are based on untenable promises of privacy and confidentiality."[112]

The problem of re-identification and the potential for DNA to be a unique identifier of individuals is neither a secret nor lost on the scientific community.

> [A]nything approaching a comprehensive genotype or phenotype (including molecular phenotypes) ultimately reveals subjects' identities . . . such as a name and social security number would. The American Society of Human Genetics (ASHG) declares the following in a statement on genome-wide association studies: "[the ASHG is] acutely aware that the most accurate individual identifier is the DNA sequence itself or its surrogate here, genotypes across the genome."[113]

106. Mark A. Rothstein et al., *Comparative Approaches to Biobanks and Privacy*, 44 J.L. MED. & ETHICS 161, 161 (2016).

107. *Id.*

108. The examination of how the differences of privacy law between countries affect international transfers of data is beyond the scope of this Note. Nonetheless, it is a relevant and important consideration in developing a reformed national system that is compatible with and facilitates cooperation with foreign scientists. *See generally* Dove, *supra* note 11 (discussing the harmonization of international privacy frameworks in the context of facilitating data sharing between international biobanks).

109. *Id.* at 682; Rothstein et al., *supra* note 106, at 169.

110. Rothstein et al., *supra* note 106, at 163–64.

111. Lunshof et al., *supra* note 19, at 408.

112. *Id.* at 409.

113. *Id.* (alteration in original) (quoting AM. SOC'Y OF HUMAN GENETICS, POLICY STATEMENT: ASHG RESPONSE TO NIH ON GENOME-WIDE ASSOCIATION STUDIES (2006), http://www.ashg.org/pdf/policy/ASHG_PS_November2006.pdf).

However, attempts to directly address the issue have been hindered by a reluctance to admit the extent of the problem, hesitancy to impede scientific progress, and disagreement about the best next course of action as we saw in the Common Rule revision process.[114]

II. A COMPARISON OF PRIVACY REGULATIONS IN THE UNITED STATES AND THE EUROPEAN UNION

There are several glaring differences between the treatment of privacy regulations in the United States compared to the European Union. First, the EU has an omnibus privacy statute that governs all matters related to information privacy, whereas the United States uses many laws covering particular information sectors.[115] Second, the United States has no default prohibition on data processing, meaning it is legal to collect, process, use, and sell personal data from almost any source.[116] There are limitations only where expressly called out by statute. In contrast, the EU prohibits data processing by default in the absence of the data subject's consent, unless a company can provide a specific legal justification for the processing.[117]

A third key difference is that the United States has no general data minimization concept.[118] The EU limits processing of personal data "to what is necessary in relation to the purposes for which [it is] processed."[119] In comparison to the United States, companies can collect as much data as they want and retain it as long as they want, "so long as they comply with applicable consent, notice and security requirements."[120] Finally, there are no restrictions on international transfers of data.[121]

A. FEDERAL PRIVACY REGULATIONS IN THE UNITED STATES

The United States does not have an overarching privacy law.[122] In fact, the federal regulations in this area are so piecemeal that nearly every state has enacted its own regulations to provide additional privacy protections for

114. *See generally* Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7150 (Jan. 19, 2017) (codified at 45 C.F.R. pt. 46 (2018)) (summarizing public comments on the Notice of Proposed Rulemaking).

115. DETERMANN, *supra* note 22, § 1-5:4.

116. *Id.*

117. *Id*.

118. *Id*.

119. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 5(1)(c), 2016 O.J. (L 119) 1 [hereinafter GDPR].

120. *Id.*

121. *Id.*

122. *Id.*

personal data, health information, and genetic information.[123] The federal sector-specific privacy laws (such as separate online privacy, data breach notification, health information privacy, and consumer protection laws) developed largely reactively to solve then-current privacy issues, rather than as preventative or advisory measures.[124] This may be a function of the U.S. judicial system, which resolves individual "cases and controversies," specific problems with particular facts.[125]

1. The Health Insurance Portability and Accountability Act

The HHS issued the Standards for Privacy of Individually Identifiable Health Information, (the Privacy Rule) as a part of the Health Insurance Portability and Accountability Act (HIPAA).[126] The Privacy Rule set forth regulations for the management of electronic health care information and incorporated new standards for the privacy and security of individually identifiable health information, also known as "protected health information" (PHI).[127] In 2013, the Omnibus Final Rule amended the Privacy Rule specifically to bring genetic information within the definition of PHI.[128] The Privacy Rule provides protections against (1) discrimination based on a patient's health information by "covered entities," and (2) disclosures of patients' private

123. R. HAKIMIAN ET AL., NAT'L CANCER INST., 50-STATE SURVEY OF LAWS REGULATING THE COLLECTION, STORAGE, AND USE OF HUMAN TISSUE SPECIMENS AND ASSOCIATED DATA FOR RESEARCH 3–8 (2004). *See generally* Scott Smith et al., *Genetic Privacy Laws: 50 State Survey*, 5 J. HEALTH & LIFE SCI. L. 75 (2011). While state laws are beyond the scope of this Note, it is interesting to note that the most protective of the state genetic privacy statutes (until the California Consumer Privacy Act of 2018) is actively being challenged.

> The Alaska Genetic Privacy Act S18.13.010-100, is [the most] comprehensive [state] genetic privacy law. It strictly limits genetic testing as well as access to, retention and disclosure of genetic data without the "informed and written consent" of the individual. The law also recognizes that both the genetic information and the DNA samples collected are the property of the individual . . . .

State Genetic Privacy Policy, ELECTION PRIVACY INFO. CTR., https://epic.org/state-policy/genetic-privacy (last visited Mar. 19, 2019). Plaintiff, commercial genetic testing company Gene by Gene, Ltd., "assert[s] that the statute is unconstitutionally vague in its definitions of 'DNA analysis' and 'genetic characteristics' and in its failure to define 'disclose' and 'informed and written consent.'" Jennifer K. Wagner, *A Constitutional Challenge to Alaska's Genetic Privacy Statute*, PRIVACY REP. (July 18, 2017), https://theprivacyreport.com/2017/07/18/a-constitutional-challenge-to-alaskas-genetic-privacy-statute/. However, as of August 21, 2018, the Ninth Circuit Court of Appeals affirmed the denial of the class certification. Cole v. Gene by Gene, Ltd., 735 F. App'x 368 (9th Cir. 2018) (mem.), *aff'g* 322 F.R.D. 500 (D. Alaska 2017).

124. DETERMANN, *supra* note 22, § 1-5:4 ("The U.S. Congress decided against European-style omnibus data protection legislation in the 1970s. California has taken a similar approach and only enacted privacy legislation regarding specific threats, industries and groups of data subjects." (footnote omitted)).

125. U.S. CONST. art. III, § 2, cl. 1.

126. PROTECTING HUMAN RESEARCH PARTICIPANTS, *supra* note 35, at 9.

127. *HIPAA for Professionals*, U.S. DEP'T HEALTH & HUM. SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/index.html.

128. FOLEY & LARDNER LLP, PRIVACY ISSUES IN THE SHARING OF GENETIC INFORMATION (2014), https://www.foley.com/files/Publication/7465587b-5df9-4f85-996968ce1b4c39af/Presentation/PublicationAttachment/88ba6035-c031-4ff4-b4e2-6ad15030b17d/PrivacyIssuesintheSharingofGeneticInformation.pdf.

health information without consent; however, it is by no means all-encompassing.[129]

The Privacy Rule only applies to certain "covered entities," including health plans and health care providers, to limit disclosure of information, and it only applies to some receiving entities, such as health insurance companies, to prohibit their unauthorized use of the information.[130] Importantly, the Privacy Rule does not apply if the information is "de-identified," "anonymous," or in the public domain.[131] Consequently, hospitals and research institutions can disclose health information freely so long as it is stripped of certain identifiers. And insurance companies can use customers' information to discriminate if they get the information from the public domain. Discrimination based on health information is a problem because a lot of de-identified data is now available in the public domain in data repositories.[132] It only takes someone with the motive, skill, and financial resources to re-identify the data and an improper motive to exploit that information.

The Privacy Rule protects PHI defined as individually identifiable health information

> that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual *or for which there is a reasonable basis to believe it can be used to identify the individual*.[133]

Until recently, there have been almost no restrictions on the use or disclosure of de-identified health information[134] because the traditionally accepted view is that "[d]e-identified health information neither identifies nor provides a reasonable basis to identify an individual."[135] However, as Gymrek's study demonstrates, this is no longer true.

2. The Genetic Information Non-Discrimination Act

The Genetic Information Nondiscrimination Act of 2008 (GINA) was passed on May 21, 2008, in order to provide a federal regulation to supplement individual state privacy regulations and the protections provided under HIPAA.[136] "GINA was designed to protect individuals from discrimination on

129. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

130. *Id.*

131. *Id.*

132. Pike, *supra* note 8, at 1981. Many journals require researchers to submit their data, including genetic sequences, to public databases as a prerequisite to publishing an article in the journal. *Id.* Internet technology has made access to these databases readily available.

133. *Summary of the HIPPA Privacy Rule*, *supra* note 129 (emphasis added).

134. *Id.*

135. *Id.*

136. Amy L. McGuire & Mary Anderlik Majumder, *Two Cheers for GINA?*, 1 GENOME MED. 6.1, 6.1 (2009).

the basis of genetic information with respect to health insurance and employment," particularly including information about genetic tests as they relate to individuals, families, and family history.[137] "Supporters of GINA . . . hope that it will alleviate the public's concerns about genetic discrimination, which many believe have discouraged the utilization of medically necessary genetic services and participation in important genetic research."[138] "Critics worry that GINA does not provide adequate protection because it fails to address discrimination on the basis of non-genetic health-related information, and it only regulates the use of genetic information in health insurance and employment."[139] For example, GINA does not protect against discrimination for mental health consultations or actual manifestation of a disorder and would not prevent discrimination by other types of insurance companies.[140]

B. PRIVACY REGULATIONS IN THE EUROPEAN UNION

The EU has expanded the traditional scope of privacy rights, recognizing "an explicit fundamental 'right to the protection of personal data.'"[141] Under the law in the EU, "personal data can be collected only under strict conditions and for a legitimate purpose."[142] The highly anticipated GDPR 2016/679 became effective as of May 25, 2018, yet holds true to the key principles of the progressive Data Protection Directive 1995/46/EC (Directive).[143] The GDPR provides more regulatory power for greater consistency between the EU member states.[144]

1. The Data Protection Directive

The Directive incorporated health data and technological use data into the same protective regulations, creating a holistic approach to privacy and defining personal data as any information that relates to an identified or *identifiable*

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.* at 6.2.

141. Dove, *supra* note 11, at 679 (quoting Charter of Fundamental Rights of the European Union, art. 8(1), 2010 O.J. (C 83) 389, 393 [hereinafter Charter of Rights]).

142. Daniel Dimov, *Differences Between the Privacy Laws in the EU and the U.S.*, INFOSEC INST. (Jan. 10, 2013), http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/#gref.

143. *GDPR Key Changes*, EU GDPR.ORG, https://eugdpr.org/the-regulation/ (last visited Mar. 19, 2019).

144. The Directive was progressive for 1995, however, "as per European Union Law, Directives allow each member state some discretion as to how to achieve the result of data protection in a way that accords with national legal traditions." Dove, *supra* note 11, at 683. A Regulation, on the other hand, "is transposed and directly applicable across the European Union" binding as law upon each state. *Id.* "The direct applicability of a Regulation . . . will reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core rules, improving the protection of fundamental rights of individuals." *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 5–6, COM (2012) 11 final (Jan. 25, 2012).

natural person "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[145] The Directive outlined seven fundamental privacy principles for the governance of personal data: necessity, finality, transparency, legitimacy, proportionality, data accuracy, and security carried over to the GDPR.[146] "These principles define the rights of individual data subjects and the responsibilities of data controllers in the context of processing personal data, regardless of the context."[147]

A key difference between U.S. and EU privacy regulations is that the language in the EU Directive specifies that even information that *could be* identifiable falls within its protections. For example, an x-ray of a person's foot, even if not labeled with information that would allow it to be easily matched to a person, like name, date of birth, or zip code, is identifiable information because if you went around x-raying feet, eventually you would find a match, making that piece of information identifiable. Genetic information, because it is specific to a unique individual, regardless of the ease with which it could be matched back to a particular person, is identifiable personal information. The Article 29 Data Protection Working Party (Working Party) issued an opinion confirming that genetic data is, by definition, personal data and further opined that "genetic data is entitled to heightened protection as "particularly sensitive data" under the Directive.[148] "[S]ensitive data . . . may only be processed in exceptional circumstances."[149]

2. General Data Protection Regulation

The GDPR "is a dramatic shift to data transparency and empowerment of data subjects."[150] It revised and strengthened the requirements for consent; "companies are no longer able to use long illegible terms and conditions full of legalese. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent."[151] It expands the right to access, giving data subjects the right to know

145. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (L 281) 31, 38.

146. Nancy J. King et al., *Workplace Privacy and Discrimination Issues Related to Genetic Data: A Comparative Law Study of the European Union and the United States*, 43 AM. BUS. L.J. 79, 162 (2006).

147. *Id.* at 147.

148. Article 29 Data Protection Working Party, Working Document on Genetic Data, 12178/03/EN, WP 91, at 5 (Mar. 17, 2004) (emphasis omitted) [hereinafter Working Document on Genetic Data]. The Data Protection Working Party, established by Article 29 of the Directive, "provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States." *Article 29 Working Party*, EUR. DATA PROTECTION SUPERVISOR, https://edps.europa.eu/node/3095#articlewp (last visited Mar. 19, 2019).

149. Working Document on Genetic Data, *supra* note 148, at 5–6.

150. *GDPR Key Changes*, *supra* note 143.

151. *Id.*

whether information is being processed about them and the right to receive a copy free of charge.[152] The right to be forgotten "entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data," particularly if "the data [is] no longer . . . relevant to original purposes for processing" or the data subject wants to withdraw consent.[153] However, "this right requires controllers to compare the subjects' rights to 'the public interest in the availability of the data' when considering such requests."[154] Data portability gives data subjects the right to request and transfer to another party the information collected about them.[155] Privacy by design "calls for the inclusion of data protection from the onset of the designing of systems" and finally, data minimization "calls for controllers to hold and process only the data absolutely necessary for the completion of its duties."[156]

The Working Party explicitly mapped the Directive's seven fundamental privacy principles—necessity, finality, transparency, legitimacy, proportionality, data accuracy, and security—onto their application to genetic data.[157] In doing so, the Working Party stated,

> Considering the complexity and the sensitivity of the genetic information, there is a great risk of misuse and/or re-use for various purposes by the data controller or third parties. Risks of re-use might occur e.g. using the genetic information already extracted, or through additional analysis of the underlying material (e.g. blood sample). . . .
>
> . . . Genetic data may only be used if adequate, relevant and not excessive.[158]

The Working Party recognized that genetic data can be easily obtained without the knowledge of the individual, is unique to the individual, is particularly personal comparable to health data, and can impact the individual's immediate family, and even a whole group, or ethnic community to which the data subject belongs. For these reasons, genetic information is particularly sensitive making the groups to which the information pertain particularly vulnerable.[159] The opinion warns that "mankind should not be reduced to its genetic characteristics only, to its sole genetic cartography, which . . . does not constitute the ultimate universal explanation of human life."[160]

---

152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.*
157. Working Document on Genetic Data, *supra* note 148, at 2.
158. *Id.* at 6.
159. *Id.* at 4; *see also* Donna M. Gitter, *Informed Consent and Privacy of Non-Identified Bio-Specimens and Estimated Data: Lessons from Iceland and the United States in an Era of Computational Genomics*, 38 CARDOZO L. REV. 1251, 1261 (2017) (discussing how population-wide database studies such as those in Iceland and Utah allow researchers to develop "estimated data" about non-consenting families and communities of those individuals who did consent to participate in the research).
160. Working Document on Genetic Data, *supra* note 148, at 4.

Compared to the privacy protections in the United States offered by HIPAA and GINA, the EU's GDPR is more comprehensive with a broader definition of protected identifiable information, and specifically calls out genetic information as included within this definition. Although HIPAA and GINA do provide protection for genetic information, their regulations apply narrowly and fail to make the jump classifying genetic information as inherently identifiable. Additionally, the EU's privacy framework contemplates all types of data created by an individual and specifically works to provide better information and more choice to the individual as an integrated policy, whereas the United States' privacy regulations and informed consent regulations are very much fragmented and do not seem to contemplate how the two ideas so harmoniously complement each other.

III. FROM HUMAN DIGNITY TO AUTONOMY

The United States emphasizes independence, privacy, and an individual's right to make life decisions in its liberal concept of autonomy, which, perhaps inadvertently, has fostered distrust of the scientific institution. On the other hand, the EU's more communitarian conception is based on an individual's fundamental right to human dignity, which embodies an underlying trust in people to be inherently good. Compared to the EU's "highly comprehensive" fundamental data privacy right,[161] the United States' privacy patchwork seems lacking.[162] The EU considers the privacy regulations in the United States to be presumptively inadequate, as evidenced in the EU's enactment and overruling of the U.S.-EU Safe Harbor for commercial transfers of information,[163] and then the enactment and threatened suspension of the Privacy Shield replacement.[164]

161. Justin Kent Holcombe, *Solutions for Regulating Offshore Outsourcing in the Service Sector: Using the Law, Market, International Mechanisms, and Collective Organization as Building Blocks*, 7 U. PA. J. LAB. & EMP. L. 539, 552 (2005).

162. Dimov, *supra* note 142 ("Under EU law, personal data can be collected only under strict conditions and for a legitimate purpose. . . . The different approaches of the EU and US towards data protection probably stem from history. In Europe, where people have had dictatorships, data protection is declared as a human right and regulated by comprehensive data protection legislation. . . . In contrast, in the US, the attitude towards data protection is governed mainly by market forces.").

163. Rothstein et al., *supra* note 106, at 167–68; *see also* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 657 (Sept. 23, 2015) (holding the US-EU Safe-Harbor invalid because an adequate level of protection must be understood to be "essentially equivalent" to that within the European Union).

164. *See* European Parliament Resolution of 5 July 2018 on the Adequacy of the Protection Afforded by the EU-US Privacy Shield, 2018 RSP 2645 (2018) ("[The Parliament] [c]onsiders that, unless the U.S. is fully compliant by 1 September 2018, the Commission has failed to act in accordance with Article 45(5) GDPR; calls therefore on the Commission to suspend the Privacy Shield until the U.S. authorities comply with its terms."). After the United States missed the compliance deadline, the Commission granted the United States until February 28, 2019 to at least appoint a permanent Privacy Shield ombudsman or it would take "appropriate measures." Rebecca Hill, *Looks Like Uncle Sam Has Pulled its Finger out and Appointed a Privacy Shield Ombusdsperson*, REGISTER (Jan. 22, 2019, 4:30 PM), https://www.theregister.co.uk/2019/01/22/privacy_

A critical comparison of privacy laws between the two governmental systems suggests that the EU's human dignity formulation of autonomy is more compatible with technological trends and might ultimately provide a truer exercise of autonomy. Re-examining the American view of autonomy may better situate the United States to receive a privacy solution that would promote scientific advancement while respecting its individual citizens.

A. FUNDAMENTAL RIGHT TO HUMAN DIGNITY

"Protecting Human dignity is the central tenet of the international human rights framework."[165] The de-humanizing atrocities of ruthless experimentation on human subjects that took place during World War II acted as the impetus for human subjects' rights in research in Europe and, arguably, the rest of the world, as it did in the United States. The United Nations Charter "enshrines the notion of human dignity, [and was] followed in 1948 by the Universal Declaration of Human Rights (UDHR)."[166] The United Nation's Charter begins: "We the Peoples of the United Nations Determined . . . to reaffirm faith in fundamental human rights, in the dignity and worth of the human person."[167] The Charter of Fundamental Rights of the European Union ("the Charter") "brings together in a single document the fundamental rights protected in the EU . . . [in a] modern codification [that] includes 'third generation' fundamental rights, such as: data protection; guarantees on bioethics; and transparent administration."[168]

"Human dignity means 'being accorded the respect and status appropriate to a human being, being treated in a way that allows or enables one to live a becoming existence.'"[169] This recognition of a fundamental right to human dignity[170] is the foundation upon which many of the other fundamental rights are built upon including, the right to life, the right to the physical and mental integrity of the person (including "[i]n the fields of medicine and biology . . . [requiring] free and informed consent"), the right to liberty and security, respect for private and family life, right to the *protection of personal protection of data*, and the right of access to preventative health care and the right to benefit from medical treatment.[171]

---

shield_ombudsperson/ (internal quotation marks omitted). At the end of January 2019, President Donald Trump finally nominated someone to the position. *Id.*

165. King et al., *supra* note 146, at 101.

166. *Id.* (footnote omitted).

167. U.N. Charter pmbl.

168. *EU Charter of Fundamental Rights*, EUR. COMMISSION, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en (last visited Mar. 19, 2019); *see also* Charter of Rights, *supra* note 141, pmbl.

169. King et al., *supra* note 146, at 97 (quoting William A. Wines & Michael P. Fronmueller, *American Workers Increase Efforts to Establish a Legal Right to Privacy as Civility Declines in U.S. Society: Some Observations on the Effort and Its Social Context*, 78 NEB. L. REV. 606 (1999)).

170. "Human dignity is inviolable. It must be respected and protected." Charter of Rights, *supra* note 141, art. 1.

171. *Id.* arts. 1–3, 6–8, 35.

The EU's fundamental rights culminate in "respect for the person," which is, in its essence, different than the Belmont Report's respect for autonomy, beneficence, or non-maleficence. Respect for the person connotes all of these principles except, at its primary level, it is theoretically different, not bestowing an affirmative right on the individual, but establishing an order for the value of a person's life. Nancy King argues that "individual privacy rights in the United States are not based on a concept of fundamental rights. American notions of privacy are reflected in the concept of 'rugged individualism.' Individual autonomy and liberty are revered, as is apparent in the jurisprudence of decisional privacy."[172] She conceptualizes the right to privacy in the United States as "akin to personal property," which "may be traded away by the individual in exchange for something of commensurate value."[173] But within the human dignity framework, the right to privacy is not so much a property right, but rather considered to inhere in every individual by virtue of their humanity.[174] "[H]uman dignity is not generated by the individual, but is instead created by one's community and bestowed upon the individual."[175]

B. LIBERAL INDIVIDUALISM VERSUS COMMUNITARIAN AUTONOMY

The concept of autonomy in the EU is not as narrowly tailored as it is in the United States. In the United States., autonomy is a liberty right that allows people to realize their true individuality by making decisions that affect their persons through an entitlement to privacy in making those decisions.[176] However, this decision-making right is just one component that allows a person to realize the full potential in his life. Scholars term this version of autonomy "liberal individualism" in order to contrast it with a broader conceptualization of autonomy that recognizes the well-being of the individual as the essential groundwork to realize true autonomy, "communitarian autonomy."[177] Although the "communitarian" version of autonomy encapsulates the ideas of community well-being, solidarity, and public interest, it should not be thought of as doing-away with individualistic liberty in favor of a utilitarian common good. It is an alternative understanding of the principle of autonomy that fits harmoniously with the ethical principles of beneficence and justice.[178]

172. King et al., *supra* note 146, at 96 (footnote omitted) (citing Jay P. Kesan, *Cyber-Working or Cyber-Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 306 (2002)).

173. *Id.* at 96–97 (applying to the context of exchanging the right to privacy for the value of having a job).

174. *Id.* at 101.

175. *Id.* at 97.

176. *See generally* Margit Sutrop, *Changing Ethical Frameworks: From Individual Rights to the Common Good?*, 20 CAMBRIDGE Q. HEALTHCARE ETHICS 533 (2011).

177. *See, e.g.*, Theda Rehbock, *Limits of Autonomy in Biomedical Ethics? Conceptual Clarifications*, 20 CAMBRIDGE Q. HEALTHCARE ETHICS 524, 526 (2011).

178. Theda Rehbock argues that, "what we need is a more precise, broader, and more differentiated understanding of the concept of autonomy and of its relation to other ethical principles." *Id.* at 524. Margit Sutrop suggests, "[t]his polarization may have occurred because of overly narrow notions of autonomy and the common

Rather than viewing autonomy as the most important and overriding ethics principle, as tends to be the view in the United States, it is necessary to recognize that autonomy cannot be "respected and applied adequately unless . . . the other principles are respected and applied as well."[179] Respect for autonomy will not be truly realized until the individual is a fully informed partner in research. The more participants are "able to identify with, approve of, and support the goals of the research . . . . the more it can be expected that participants would be willing, at least afterward, to accept and consent, if necessary, to a certain degree of deception or risk."[180]

C. A KANTIAN PERSPECTIVE

Theda Rehbock addresses the differing conceptions of autonomy from a philosophical perspective with roots going back to the writings of Immanuel Kant, John Stuart Mill, and Aristotle.[181] While she criticizes the Aristotelian approach for being too utilitarian and threatening "a relapse into the old paternalism," she argues for reexamination of the Kantian perspective, which presupposes a *moral* autonomy underlying individual liberty.[182] "Respect for autonomy should not be reduced to 'respect for autonomous choices' and, thereby, to respect for the mental capacity ('competence') to make such choices through informed consent procedures. Rather, it has to be understood in a much broader sense as respect for the *will* of the person."[183] Kantian "moral autonomy means *self-legislation* or *self-commitment*, according to moral norms that are to be followed not because of external command or authority but because of one's own rational insight."[184] "The rational will is one's own will, not an egoistical will, but a general will, which is concerned not only with one's own liberty and happiness, but also with the liberty and happiness of others."[185] "Kant's non-individualistic notion of moral autonomy could be a bridge between ancient and modern ethics."[186]

To truly be autonomous, the individual is dependent upon others to receive information to aid in decision-making.[187] Kant specifies that human dignity imposes a positive "duty to help and support others to live their life," rather than

---

good, which make it difficult to see their close relationship." Sutrop, *supra* note 176, at 534. "This notion has arguably become overshadowed by narrow interpretations of individual autonomy, which interpret consent not only as one of its manifestations, but also as a quasi-synonym for autonomy itself." Barbara Prainsack & Alena Buyx, *A Solidarity-Based Approach to the Governance of Research Biobanks*, 21 MED. L. REV. 71, 78 (2013).

179. Rehbock, *supra* note 177, at 524.

180. *Id.* at 528.

181. *Id.* at 525–26.

182. *Id.*

183. *Id.* at 526; s*ee also* Onora O'Neill, *Some Limits of Informed Consent*, 29 J. MED. ETHICS 4 (2003). *But cf.* Tom L. Beauchamp, *Informed Consent: Its History, Meaning, and Present Challenges*, 20 CAMBRIDGE Q. HEALTHCARE ETHICS 515, 519 (2011) (arguing that broad consent is "not an adequately informed consent").

184. Rehbock, *supra* note 177, at 527.

185. *Id.*

186. *Id.*

187. *Id.* at 529.

just a negative duty to not interfere with other's autonomy, which he refers to as the "universal duty of human beings."[188] The EU Charter protects "human dignity" as a fundamental right. The EU human dignity conceptualization of autonomy, as juxtaposed to the liberal individual conceptualization of autonomy implied in the U.S. Constitution, provides a basis for understanding why the privacy frameworks in each country differ.[189] While both fundamental rights focus upon "autonomy," the difference is embedded in differing philosophical ideals.

D. NORMALIZING TRUST

Transparency facilitates trust. However, in science, minimal involvement of the subject is less burdensome on the scientists and the study, and so is common practice. The attitude of "us versus them" (scientists versus subjects) instead of all of us partners in discovery for humankind has created a cycle of distrust.[190] The emphasis on the liberal individualistic autonomy in the United States comes from the perceived need of a person to look after his own interests, but distrust actually erodes a person's autonomy. If providing people with information about research will make them less likely to participate, deception facilitates research and beneficence seemingly justifies this deception as long as the results are for the benefit of the common good.

On the other hand, including participants in the research by treating them as partners, may make them feel empowered enabling participants to embrace their communitarian autonomy rather than selfish individual needs.[191] Developing and normalizing a public trust in the scientific community will not happen immediately. At first there will be shock and more distrust as the current practice come to light, but people will eventually come to terms with the reality of the advancement of biotechnology and realize that the benefits are enormous. Trust requires relinquishing some control over the immediate, but it ultimately facilitates more autonomous control over quality of life.

IV. RECOMMENDATIONS

A. TECHNOLOGY MAKES ALTERNATIVE CONSENT MODELS FEASIBLE

"Current developments in genomics challenge the established framework of biomedical ethics because the empirical facts of the genomic science change too fast for the reflections of ethics to keep pace."[192] The move towards

188. *Id.*

189. Dove, *supra* note 11, at 680 ("Reliance on specific consent in this biobanking context falls into a fallacy of sufficiency: no participant can be sufficiently informed at the initial stage about the range of unknown actors and uncertain events to follow . . . .").

190. Rehbock, *supra* note 177, at 528.

191. *Id.*

192. Lunshof et al., *supra* note 19, at 406.

bioinformatics, gathering and studying personal data, and decoding genetic data to determine unique characteristics makes individual participants vulnerable to re-identification, "puts the validity of the existing consent protocols into question."[193] Therefore, alternative consent models have been offered to replace the traditional specific informed consent model.[194] Because information stored in biobanks is meant to be available to countless researchers for unspecified research, the scope of which will be ever-changing as science progresses, some researchers ask participants to give a general consent to *any* type of future research; this is known as a "blanket consent."[195] While blanket consents provide a simple solution from the researcher's perspective, other types of consent that offer more layers of protection for the participant, are now feasible with the advancement of technology.

"Broad consent" similarly asks for "one-time consent for future research," but requires external review by an ethics committee or authority to ensure that the research satisfies the stated mission of the future research.[196] This is the method used (or proposed for use) by most biobanks.[197] "Tiered consent" is given when "participants are given a menu of different types of research (e.g., cancer; heart disease)" and they can select different categories of research for which they give consent.[198] "Dynamic consent" asks for initial consent and is followed up with subsequent opportunities to opt in or out of future specific research uses.[199] "Open consent" involves agreeing to unrestricted future usage where "[d]ata, whether anonymized or not, are posted on the internet and available to any-one in the world."[200] Open consent is the least protective of the consent models, but acknowledges the researcher's intent to make the participant's private information public and involves the participant as a fully informed research partner.

The open consent model was implemented in the Personal Genome Project (PGP), revolutionizing the relationship between researchers and research subjects in the areas of valid consent, veracity and participation, transparency, and the ongoing participation of the subject.[201] The PGP "aim[ed] to sequence the genotypic and phenotypic information of 100,000 informed volunteers and display it publicly online in an extensive public database."[202] Open consent implies that research participants accept that any data given is shared in a public access database, they have no guarantees regarding anonymity or privacy, their

193. *Id.*
194. Rothstein et al., *supra* note 106.
195. *Id*.
196. *Id.* at 163–64.
197. *Id.*
198. *Id.* at 166 tbl.2.
199. *Id.*
200. *Id.*
201. *Id.*
202. LATANYA SWEENEY ET AL., IDENTIFYING PARTICIPANTS IN THE PERSONAL GENOME PROJECT BY NAME 1 (2013).

participation might involve risks to themselves or families, they get no direct benefit individually from the study, and ongoing participation in the study is required.[203] While the participant may technically withdraw at any time, complete removal of information from the public domain may not be possible.[204]

"The moral goal of open consent is to obtain valid consent by effectuating veracity as a precondition for valid consent and effectuating voluntariness through strict eligibility criteria, as a precondition for substantial informed consent."[205] PGP employed several innovative features to ensure that participants had the special knowledge required to truly understand the risks of sharing genetic information and making sensitive health information accessible to the public.[206] The participants in the first study cohort were required to "have a master's degree in genetics or equivalent, and [were] presented from the outset with a straightforward description of the risks of participation and the harm they might experience as a consequence of the loss of privacy through public disclosure of identification."[207] In addition, the study employed "[i]nteractive online education and an entrance test . . . [ensured] valid consent [when] the participation [opened] to the broader public."[208]

Since the researchers recognized that the "promise of secrecy" is not one that can be kept in the realm of genetic research, transparency was deemed "the hallmark of [the] project."[209] The PGP found that the open consent model allowed its research participants to cultivate a sense of community through their collective involvement; this was a huge benefit stemming from the fact that "participants [were] no longer isolated."[210] Participants in PGP were not promised any direct benefit from their participation; "a high degree of 'information altruism' [was] required, thereby introducing a strong moral motive."[211] This model supports the idea of a "solidarity" approach to biobank governance proposed by Barbara Prainsack and Alena Buyx.[212] Several ideas from this approach to biobank governance ring true: "recogni[zing] people's willingness to participate in a public research biobank, and [a] stronger emphasis on harm mitigation."[213] "It also allows moving beyond overly restrictive and burdensome, exclusively autonomy-based governance towards governance that

203. Lunshof et al., *supra* note 19, at 409 box 3.

204. *Id.*

205. *Id.*

206. Madeleine P. Ball et al., *Harvard Personal Genome Project: Lessons from Participatory Public Research*, 6 GENOME MED. 1, 2 (2014).

207. Lunshof et al., *supra* note 19, at 409.

208. *Id.* at 410.

209. *Id.* at 409.

210. Ball et al., *supra* note 206, at 5.

211. Lunshof et al., *supra* note 19, at 410 (footnote omitted); *see also* Ball et al., *supra* note 206, at 2.

212. *See generally* Prainsack & Buyx, *supra* note 178. Solidarity is a practice or set of practices that "manifest[] . . . people's willingness to carry costs (financial, social, emotional, or otherwise) to assist others." *Id.* at 75 (internal quotation marks omitted).

213. *Id.* at 71.

is reflective of people's willingness to accept costs and to assist others."[214] However, this model asks too much of people too quickly. Therefore, a dynamic consent model is the most practical, yet feasible type of consent model for the big data age because it promises the participant control over the scope of data sharing, instead of relying solely on his altruism, while technology offerings researchers an easy way to elicit renewed consent on an ongoing basis.

Dynamic consent is a "proposal that seeks to continually communicate with participants and allow for individually tailored control."[215] It entails getting initial consent from participants and following up with "electronic notification of each proposed use of [the participant's] specimens and data, and participants can opt out of any specific research use."[216] Critics argue that obtaining dynamic consent is not feasible for biobanks that lack the resources needed to handle the administrative burdens that the dynamic consent model imposes.[217] It is understandable that the development of an interactive platform for participants and the initial set up of profiles for millions of samples is a huge endeavor. But these are worthwhile undertakings that stand to accommodate scientific research and increase administrative efficiency in the long run by providing a common link between data sets, creating an invaluable resource for scientists, and allowing for automation of menial tasks such as sending notifications to research participants and getting renewed consent.[218] Indeed, an automated system could be set up under either an opt-in or an opt-out consent model, depending on the level of risk or according to current regulations.[219]

The dynamic consent system addresses, and provides a platform for solving many complicated ethical and moral issues surrounding invalid consent. To that point, the absence of a major public uproar concerning the use of DNA samples likely stems from a general lack of knowledge about common practices within the scientific community, which allows DNA to be used and re-used over and over without any additional consent. This needs to change before people find out about these practices in a way that makes them feel deceived, disrespected, or otherwise aggrieved, which could result in backlash against the scientific community and cause the whole system to crash. Fostering extreme distrust in science could cause irreparable harm.

The use of dynamic consent would provide transparency, letting people know how their data is being used; autonomy, whether through an opt-in or opt-out model, letting people decide if they want to participate; fosters a collaborative environment where people feel like they are voluntary participants in research contributing to the common good; and it relieves researchers of some of the ethical responsibility because it gives participants the information to make

214. *Id.*
215. Dove, *supra* note 11, at 680.
216. Rothstein et al., *supra* note 106, at 166 tbl. 2.
217. Dove, *supra* note 11, at 680.
218. *See* Rothstein et al., *supra* note 106, at 166.
219. *Id.*

their own decisions regarding participation. Moreover, rather than creating unmanageable privacy concerns, a dynamic consent system would call attention to the inadequacies in privacy regulation, which has been quickly outpaced by biotechnological advances, by creating concrete problems and a platform on which to solve them.[220]

B. HEALTH DATA AS SENSITIVE PERSONAL DATA

A dynamic consent platform is consistent with a theory of whole person data management. In the age of big data—an age in which people are creating an ever-increasing amount of data about themselves and commercial data refineries are collecting and capitalizing on the information contained therein—health data should be treated as a particularly sensitive type of personal data, and regulated under one overarching privacy framework. In the United States, the idea of treating genetic information as personally identifiable has not been widely accepted or put into practice.[221] The HIPAA Omnibus Rule considers genetic information as "personally identifiable" but the traditional elements of PHI still must be met.[222] On the other hand, the EU has recognized the heightened sensitivity of both health data and genetic health data *and considers genetic data inherently identifiable*.[223]

Genetic information, including any material that genetic information can be derived from, including blood, tissue, or other bodily samples, and including DNA sequences or patterns should be treated as inherently identifiable personal information. Even if anonymous, the ability to re-identify the source of this material now exists, and we have not yet reached the limits on our ability to derive more meaning from genetic sequences. If genetic data and biological materials are considered inherently identifiable, it then makes sense to treat those categories of information as sensitive personal data within a larger privacy framework designed to protect the privacy rights of individuals concerning all types of data.[224]

220. *See, e.g.*, Sutrop, *supra* note 176, at 538–43 (discussing the Estonia Electronic Health Record which demonstrates one such technological platform that provides individuals with transparency about the data collected about them and gives them control over the use of that data).

221. Rothstein et al., *supra* note 106, at 167 ("In 2014, the U.S. National Institutes of Health issued a policy statement requiring the sharing of genomic data under a broad consent approach as a condition of the funding."). However, a proposal for a similar change to the common rule was rejected. It would have required "the prospective collection of any tissues (even if deidentified) [to] require consent." *Id.*

222. FOLEY & LARDNER LLP, *supra* note 128.

223. *See generally* Ana Gomes, *Fundamental Rights and Big Data: Striking a Balance*, PARLIAMENT MAG. (Mar. 17, 2017), https://www.theparliamentmagazine.eu/articles/opinion/fundamental-rights-and-big-data-striking-balance (discussing the non-legislative resolution she drafted for the European Parliament about "the fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement").

224. In the United States, there has been some reference to health information generally as sensitive data or identifiable sensitive data in legislation proposals, but no explicit reference to genetic information fitting within that definition. 21st Century Cures Act, 42 U.S.C. § 241(d) (Supp. IV 2016). The 21st Century Cures Act

C. BIG DATA APPROACH TO PRIVACY

Operating under the assumption that genetic information is health information and health information is data about a unique person, then the management and protection of all data can properly be addressed within the big data framework. "Most definitions [of big data] reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data."[225] If you assume that all people are generating countless amounts of data, and some data is inherently more sensitive than other data, and once you delineate the categories of sensitivity, an overarching regulation or set of regulation is the best way to ensure that all data is accounted for and protected. The creation and sharing of health data is becoming more akin to the creation of other personal informational data, "real-time 'flows' of data" as opposed to "point-to-point 'data transfers'" as originally "envisioned in data privacy regulation."[226] Theories for reform of big data provide ways to keep afloat the essential principles of informed consent. In the post-privacy era, the United States needs to take a comprehensive big data approach to maximize the privacy protection of the individual without hindering scientific advancement—interestingly, whether completely successful or not, what the EU has done with its implementation of the GDPR.

1. Data Subject Rights Model

The GDPR is only one implementation of ideas to increase transparency and individual choice when it comes to this huge generation of data. Andreas Weigend, in his book *Data for the People*, argues for an increase in transparency and agency, or autonomy, to allow all individuals to become data literate.[227] He

requires certificates of confidentiality for NIH funded research or by application by the participant for "identifiable, sensitive information." *Id.* Section 241(d) defines "identifiable, sensitive information" as information "(A) through which an individual is identified; or (B) for which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual," the second definition leaving open the possibility of genetic information falling within that category. *Id.*

The FTC referred to health information specifically as "sensitive information" within its big data protection framework: "Sensitive data deserves stronger protections than other kinds of personal data, including more rigorous security and more robust notice and choice before collection." Julie Brill, Comm'r, FTC, Keynote Address at the Columbia University Data Science Institute Symposium on "Data on a Mission: Transforming Privacy, Cities, and Finance": Navigating the "Trackless Ocean": Privacy and Fairness in Big Data Research and Decision Making (Apr. 1, 2015). *See generally* Ohm, *supra* note 84 (proposing to classify genetic information as "sensitive information," develop a multi-factor test for assessing sensitivity, and recommending a new "threat modeling" approach to assessing risk of harm in privacy law which borrows from the computer security literature and extends the idea of sensitive information to other unprotected types of personal data).

225. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 2 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. The White House, under the Obama Administration, released the Big Data Privacy Report based on the findings of the Big Data and Privacy Working Group Review. *Id.*

226. Dove, *supra* note 11, at 682.

227. *See* WEIGEND, *supra* note 12.

proposes six data rights to "empower people to make better decisions" regarding data created about themselves: (1) the right to access data, (2) the right to inspect data refineries, (3) the right to amend data, (4) the right to blur data out, (5) the right to experiment with the refineries, (6) the right to port data.[228] The six data rights—two transparency and four autonomy rights[229]—closely resemble the seven data privacy principles recognized in the GDPR and are even reminiscent of the Belmont Report's bioethics principles. Weigend's post-privacy paradigm for big data provides an excellent framework for thinking about how to organize a system to protect health data privacy rights.

A significant problem with informed consent in the United States is that participants are ignorant as to the true scope of how their information will be used. The scientific community currently informs potential subjects as though they are educated researchers themselves and already understand the basic risks. However, the public at large likely has very little idea of how tissue samples and the information generated from research of them are handled. Weigend describes this as "data illiteracy" and advocates for widespread data literacy in understanding the methods of collection and the uses data.[230] The concept holds true for genetic data.

Data literacy and true informed consent require research participants to know germane facts about scientific practices, including: (1) leftover samples taken during medical procedures are considered a donation to the hospital and can be de-identified and used in research;[231] (2) once tissue is separated from your body (abandoned) you lose property rights in it;[232] (3) leftover tissue or the data from analysis of that tissue can, and probably will, be shared with other researchers; (4) your samples will likely be de-identified to protect your identity and private health information, but HIPAA privacy protection does not extend to secondary research done with de-identified samples or information in the public domain; (5) there are no restrictions on sharing de-identified samples even though re-identification is possible; and (6) the risks of research participation that can be told today are just some of the risks we might know tomorrow.

While transparency alone could potentially scare off volunteers, the Six Data Rights approach may facilitate a trusting relationship between the scientific community and research participants after the initial shock in discovering the

228. *Id.* at 6–11.

229. *Id.*

230. *Id.* at 34.

231. Kayte Spector-Bagdady, *The Privacy Debate over Research with Your Blood and Tissue*, CONVERSATION (Jan. 25, 2017, 7:49 PM), http://theconversation.com/the-privacy-debate-over-research-with-your-blood-and-tissue-71523.

232. *See* Wash. Univ. v. Catalona, 490 F.3d 667 (8th Cir. 2007) (ruling against patients who wanted to transfer their donated samples with the investigator to another university to continue the desired research); Moore v. Regents of the Univ. of California, 793 P.2d 479 (Cal. 1990) (holding that patient did not have a property right in his tissue after removed).

knowledge gap. If participants have access to the data generated about them, they can learn what they want in the amount they want, they can correct incorrect data, and they can see for what other studies their data might be used, so participants can feel like partners contributing to science and discovery rather than exploited test subjects.

2. The 2018 California Consumer Privacy Act

The passage of the 2018 California Consumer Privacy Act (CCPA) is a big step toward embracing this all-inclusive privacy regime, largely influenced by the GDPR data subject rights model though just on a state scale.[233] The CCPA sets out new regulations for the protection and processing of "personal information" of California residents.[234] "Personal information" is defined as any "information that . . . relates to . . . a particular consumer or household."[235] This definition appears to broadly protect all non-public information that is capable of being associated directly or indirectly with a particular consumer or household,[236] a broader definition than the term "personal data" under the GDPR, which only protects "any information relating to an identified or identifiable natural person."[237]

Although the CCPA uses slightly different terminology than the GDPR, it follows a very similar model setting out rights for "consumers" to protect their "personal information."[238] The new rights afforded under the CCPA give consumers a level of transparency and access to their data not offered by the former privacy laws. The five central individual rights are: (1) the right to know what personal information is being collected about oneself; (2) the right to know whether one's personal information is sold or disclosed and to whom; (3) the right to say no to the sale of one's personal information (the right to opt-out of data collection and processing); (4) the right to access one's own personal information; and (5) the right to be free from discrimination in exercising of one's privacy rights.[239] Now California just needs to work out the kinks in its law and implement a system that can handle giving its consumer data subjects all of these rights (and of course hop on board with classifying genetic data as

233. Purvi G. Patel et al., *The 2018 California Consumer Privacy Act: California Scraps Ballot Initiative and Passes Sweeping Data Privacy Regulation*, MORRISON & FOERSTER LLP (June 29, 2018), https://www.mofo.com/resources/publications/180629-california-consumer-privacy-act-2018.html. Before the January 1, 2020 effective date, we can expect to see "technical fixes and substantive amendments" from negotiations between businesses and the legislature that will impact the CCPA's scope and its interpretation. *Id.*

234. Lothar Determann, *Analysis: The California Consumer Privacy Act of 2018*, INT'L ASS'N PRIVACY PROFS. (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/#.

235. CAL. CIV. CODE § 1798.140(o)(1) (West 2018).

236. *Id.* § 1798.140(o)(2).

237. GDPR, *supra* note 119, art. 4(1).

238. California Consumer Privacy Act of 2018, A.B. 375, 2018 Assemb., Reg. Sess. § 2(i) (Cal. 2018) (an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy).

239. *Id.*

inherently identifiable personal information) to be on its way to implementing a big data approach to genetic privacy law.

While the GDPR provides a good starting place for thinking about the problems inherent in data privacy and especially the privacy of highly sensitive genetic data, it does not solve every problem and it was not designed to tackle the unique problems of genetic data specifically. Its data rights model provides a good framework for the next generation to create a system that allows participants to have some control over information generated about them which has the potential to dramatically influence their lives. If we use technology to create a dynamic platform to engage every person as a partner to contribute to the genetic research revolution, we can use technology to advance technology rather than allow fear of technology to stagnate its advancement.

CONCLUSION

There are approaches to advancing U.S. privacy and informed consent regulations that will allow the law to keep pace with scientific development while protecting an individual's unique-biodata and at the same time fostering rather than burdening the future of medicine. With the rapid expansion and development of biotechnology, both privacy concerns and the potential harmful uses of human genome data cannot be overlooked by the United States for much longer and soon a wholly new framework will be required to provide participants with adequate informed consent consistent with our society's ethical values. The EU holds a more encompassing view of privacy and has classified more information as sensitive health data deserving of greater protection. In developing its future privacy framework, the United States should embrace the EU's data subject rights model to create and implement a holistic approach to data privacy regulation. Further, the United States should look to dynamic consent models and technology to facilitate its implementation.

***