Vanderbilt Journal of Entertainment & Technology Law

Volume 19
Issue 2 *Issue 2 - Winter 2016*

Article 2

2016

Power to the People: Data Citizens in the Age of Precision Medicine

Barbara J. Evans
University of Houston Law Center

Power to the People: Data Citizens in the Age of Precision Medicine

*Barbara J. Evans**

ABSTRACT

Twentieth-century bioethics celebrated individual autonomy but framed autonomy largely in terms of an individual's power to make decisions and act alone. The most pressing challenges of big data science in the twenty-first century can only be resolved through collective action and common purpose. This Article surveys some of these challenges and asks how common purpose can ever emerge on the present bioethical and regulatory landscape. The solution may lie in embracing a broader concept of autonomy that empowers individuals to protect their interests by exercising meaningful rights of data citizenship. This Article argues that twentieth-century bioethics was a paternalistic, top-down affair in which self-proclaimed ethics experts set standards to protect research subjects portrayed as autonomous yet too vulnerable and disorganized to protect themselves. The time may be ripe for BioEXIT, a popular uprising of regular people seeking a meaningful voice in establishing citizen-led ethical and privacy standards to advance big-data science while addressing the concerns people feel about the privacy of their health data.

TABLE OF CONTENTS

* Alumnae College Professor of Law and Director, Center for Biotechnology & Law, University of Houston Law Center, bjevans@central.uh.edu. This work received financial support from the Robert Wood Johnson Foundation's Health Data Exploration Project (Kevin Patrick, M.D., M.S., PI), http://hdexplore.calit2.net, with additional support from NIH/NHGRI/NCI grants U01HG006507 (GPJ) and U01HG007307-02S2 (GPJ).

I. INTRODUCTION

Very large datasets are the lifeblood of twenty-first century informational research, which studies people virtually by reprocessing their preexisting data.[1] The required datasets ideally should be highly inclusive, containing data for tens or even hundreds of millions of individuals[2] to reduce selection bias and provide results relevant to all population subgroups.[3] These data resources also should be deeply descriptive and capture diverse sources of data for each person included in the dataset. Potentially useful data include, for example, clinical data generated when people consume healthcare services during spells of illness, research data collected when people volunteer as research subjects, data describing wellness states—such as data from fitness trackers and direct-to-consumer genetic testing services—and data such as grocery store receipts that bear on lifestyle and environmental exposures.

Linking these diverse data streams together to form a longitudinal record for each person generally requires at least some access to identifying information. There are algorithms that can link incoming streams of data that have been de-identified by stripping away overt identifiers such as names and patient numbers, but the resulting linkages are probabilistic. Making sure that the linked data all relate to the same person thus requires at least some identifiers, at least temporarily, during the linkage process.[4] This fact arouses privacy concerns, as does the fact that the resulting longitudinal

1. Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53,933, 53,938 (Sept. 8, 2015).

2. *See generally* Brian H. Shirts et al., *Large Numbers of Individuals Are Required to Classify and Define Risk for Rare Variants in Known Cancer Risk Genes*, 16 GENETICS MED. 529, 529–34 (2014) (discussing the size of data resources required to draw inferences about the clinical significance of rare genetic variants).

3. Barbara J. Evans, *Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science*, 42 J.L. & MED. (forthcoming Feb. 2017), http://ssrn.com/abstract=2750347 [https://perma.cc/YLE3-MXWM].

4. *Id.*

records may be re-identifiable. Even if overt identifiers are discarded after the individual's data have been linked together to create a longitudinal health record, there may be only one person in the world for whom all of the parameters in the longitudinal record are a match.[5] The record itself is a unique identifier, like a health history fingerprint. There may be only one person who fell off a skateboard and cracked the upper right incisor at thirteen years, three months, and six days of age, while giving birth to a healthy daughter at twenty-six years, seven months, and eight days of age and developing dementia prematurely at the age of fifty-three. Deeply descriptive data display the irreproducibility of each of our life trajectories.

Americans are regularly admonished that access to our data is crucial to projects like the Obama Administration's Precision Medicine Initiative,[6] Cancer Moonshot,[7] and Brain Initiative.[8] Implementing a "learning health care system"[9] and inferring the clinical significance of human gene variants[10] also require very large data resources. Professors Faden, Kass, et al., note that the moral framework to support such efforts "will depart in important respects from contemporary conceptions of clinical and research ethics" and will require a new "norm of common purpose . . . a principle presiding over

5. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010) (noting that personally identifiable information and non-identifiable information are no longer distinct categories, given the potential for data to be re-identified); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 (2010) (discussing the potential for de-identified data to be re-identified); Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?*, 10 AM. J. BIOETHICS 3, 5 (2010) ("Despite using various measures to deidentify health records, it is possible to reidentify them in a surprisingly large number of cases.").

6. *See The Precision Medicine Initiative*, THE WHITE HOUSE, https://www.whitehouse.gov/precision-medicine [https://perma.cc/P4JF-NFSY] (last visited Nov. 16, 2016).

7. *See Fact Sheet: Investing in the National Cancer Moonshot*, THE WHITE HOUSE (Feb. 1, 2016), https://www.whitehouse.gov/the-press-office/2016/02/01/fact-sheet-investing-national-cancer-moonshot [https://perma.cc/8SV4-6QTU].

8. *See The Brain Initiative*, THE WHITE HOUSE, https://www.whitehouse.gov/brain [https://perma.cc/8S5T-9DXJ] (last visited Nov. 16, 2016).

9. LEIGHANNE OLSEN ET AL., INSTITUTE OF MEDICINE, IOM ROUNDTABLE ON EVIDENCE-BASED MEDICINE, THE LEARNING HEALTHCARE SYSTEM 6 (LeighAnne Olsen et al. eds., 2007).

10. *See* U.S. FOOD & DRUG ADMIN., USE OF DATABASES FOR ESTABLISHING THE CLINICAL RELEVANCE OF HUMAN GENETIC VARIANTS 2 (2015), http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM467421.pdf [https://perma.cc/69M7-464E]; *see also* Barbara J. Evans, Wylie Burke & Gail P. Jarvik, *FDA and Genomic Tests: Getting Regulation Right*, 372 NEW ENG. J. MED. 2258, 2260 (2015).

matters that affect the interests of everyone . . . a shared social purpose that we cannot as individuals achieve."[11]

This Article explores whether it is realistic to expect that common purpose can emerge on the present bioethical and regulatory landscape that celebrates individual autonomy. It reaches an optimistic conclusion that common purpose may be achievable, but only if we liberate the concept of autonomy from the narrow straitjacket in which twentieth-century bioethics put it. Twentieth-century bioethics embraced a Kantian, atomistic concept of individual autonomy that portrays individuals as individualistic and alone yet self-reliant in the sense of being able to protect their interests through their own decision making.[12] This concept resembles Richard Fallon's "ascriptive" autonomy,[13] which recognizes each person's sovereignty over her moral choices. The atomistic concept of autonomy is not the only way autonomy can be framed and—this Article argues—it is an impoverished concept that threatens to backfire in the setting of twenty-first-century informational research because it disempowers the very people that bioethics aims to protect.[14]

The twentieth-century bioethics movement emphasized the right of individuals to make their own choices through a right of informed consent, as reflected in state medical practice statutes, in hospital accreditation standards, and in privacy and research regulations, such as the Common Rule,[15] Food and Drug Administration (FDA) human-subject protections,[16] and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.[17] A criticism of this framework is that it empowers individuals to make decisions *only* as individuals and fails to equip them with institutions for collective action and shared decision-making.[18] It conceives patients and research subjects as weak, vulnerable, alone, disorganized, and in need of paternalistic protectors—for example,

---

11. Ruth R. Faden et al., *An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics*, 43 HASTINGS CTR. REP. S16, S16 (2013).

12. ALFRED I. TAUBER, PATIENT AUTONOMY AND THE ETHICS OF RESPONSIBILITY 117 (2005).

13. Richard H. Fallon, Jr., *Two Senses of Autonomy*, 46 STAN. L. REV. 875, 890–93 (1994).

14. *See id.* at 875; *see also* Evans, *supra* note 3, at 28.

15. 45 C.F.R. § 46.116 (2016).

16. 21 C.F.R. §§ 50.20, 56.101 (2016).

17. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in §§ 18 U.S.C., 26 U.S.C, 29 U.S.C, 42 U.S.C.); *see also* Privacy Rule, 45 C.F.R. § 164 (2010).

18. Evans, *supra* note 3, at 26.

ethicists and Institutional Review Boards (IRBs). Individuals are cast as cowering "subjects," too disempowered to negotiate the ethical and privacy protections they desire. There is a striking disconnect between empirical surveys that show most people—up to eighty percent of Americans—feel favorably about letting researchers use their data[19] and the low rates at which people actually consent for their data to be used. Existing ethical and privacy regulations, designed with little direct, organized, collective public engagement, apparently fail to reassure people that it is safe to contribute their data.

Regulations like the Common Rule and HIPAA Privacy Rule reject the approach of organizing and empowering individuals to protect themselves, for example, by unionizing research subjects to defend their own interests through collective bargaining. This approach has worked well in certain other contexts—labor relations, for example—where law seeks to protect vulnerable individuals who face disparities in bargaining power. Autonomy, in this setting, is not the autonomy of the hapless, go-it-alone individual. It is the autonomy of self-governing data citizens whose autonomy encompasses a power to bind themselves to collective ventures that afford stronger protection than one person, alone, can achieve.

II. THE RISE AND IMPENDING FALL OF GO-IT-ALONE AUTONOMY

At its inception in the mid-twentieth century, the field of bioethics sought to protect the rights of individuals facing binary, us-versus-them challenges: the patient against the physician in a paternalistic health-care system[20] or the scientifically naïve human research subject against the more sophisticated investigator in clinical research settings. The Kantian, atomistic concept of autonomy was a

19. COMM. ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFO.: THE HIPAA PRIVACY RULE, INST. OF MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 209–14 (Sharyl J. Nass, Laura A. Levit & Lawrence O. Gostin eds., 2009) [hereinafter IOM, PRIVACY REPORT] ("[A] majority of consumers are positive about health research and, if asked in general terms, support their medical information being made available for research."); *see also* HEALTH DATA EXPLORATION PROJECT, PERSONAL HEALTH DATA FOR THE PUBLIC GOOD: NEW OPPORTUNITIES TO ENRICH UNDERSTANDING OF INDIVIDUAL AND POPULATION HEALTH 13 (2014), http://hdexplore.calit2.net/wp-content/uploads/2015/08/hdx_final_report_small.pdf [https://perma.cc/5XRH-5JKQ] (discussing individuals' willingness to participate in research in the context of data from mobile and wearable devices); Leonard J. Kish & Eric J. Topol, *Unpatients—Why Patients Should Own Their Medical Data*, 33 NATURE BIOTECHNOLOGY 921, 923 (2015) (discussing individuals' willingness to participate in research); Eric J. Topol, *The Big Medical Data Miss: Challenges in Establishing an Open Medical Resource*, 16 NATURE REV. GENETICS 253, 254 (2015) (same).

20. *See* TAUBER, *supra* note 12, at 14–15.

"powerful antidote to the threats to personhood that result"[21] in these David-versus-Goliath settings where there are disparities in expertise and bargaining power. Individual informed consent has, however, been criticized as a weak way to protect the autonomy of people whose data are used in research.[22] People may grant access to their data too casually and, having done so, cede control over subsequent uses of their data. Regulations like the Common Rule rely heavily on informed consent while neglecting data security requirements and other practical measures to manage privacy risks in an informational setting.[23] Informed consent, as traditionally conceived, gives people a take-it-or-leave-it right to refuse to let their data be used in research if they dislike the research protocol or distrust the privacy and ethical protections that others have set for them.[24] Even this modest right to refuse can be waived by an IRB,[25] usually staffed by employees of the institutions that wish to use or share the people's data, and whom the people never elected to represent their interests.[26]

In response to criticisms of the informed consent framework, there has been a recurring *déjà vu* of calls for individual data ownership—often based on a fairy tale[27] notion that legal property ownership would empower people to veto[28] unwanted uses of their data and render the individual immune to countervailing public interests in data access. Jacqueline Lipton usefully points out that legal ownership, in reality, supplies a bundle of rights, limitations on the rights, and duties,[29] so that data ownership would not confer the degree of control many of its proponents desire. Earlier works by Evans[30] have explored problems with individual data ownership and

---

21. *Id.* at 14.

22. *See, e.g.*, Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765, 1797 (2010) ("Consent requirements [imposed by the HIPAA Privacy Rule] not only impede health research, but may actually undermine privacy interests.").

23. *Id.* at 1773.

24. *See* Evans, *supra* note 3, at 8.

25. 45 C.F.R. § 164.512(i) (2016) (HIPAA waiver provision); 45 C.F.R. § 46.116(d) (2016) (Common Rule waiver provision).

26. *See* Carl H. Coleman, *Rationalizing Risk Assessment in Human Subject Research*, 46 ARIZ. L. REV. 1, 7–8 (2004).

27. Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 804 (2004) (citing Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1297–98 (2000)).

28. *See, e.g.*, Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26–41 (1996).

29. Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. Rev. 135, 173 (2004).

30. *See* Evans, *supra* note 3, at 11–16 (discussing problems with the metaphor of individual data ownership); *see also* Barbara J. Evans, *Much Ado About Data Ownership*, 25

this essay resists the temptation to re-plow that old ground. Two points, however, are relevant to this discussion.

First, many parties other than the individual have legitimate interests in a person's health data. These include, for example, the physician whose intellectual effort generated diagnostic information contained in a patient's medical record; care providers that need copies of patients' data to defend themselves from malpractice claims; clinics and laboratories that are required by law to maintain copies of patients' records and test results; and insurers that must maintain records for auditing, regulatory, and fraud prevention purposes.[31] Legal ownership of health data, if it existed, would necessarily be non-exclusive,[32] perhaps resembling the shared ownership frameworks Ostrom and Schlager described in natural resource settings.[33] In shared ownership schemes, the individual does not enjoy "sole and despotic dominion"[34] of the resource, but instead has various entitlements such as rights of access and use and a voice in collective governance of the resource.

The second, and more fundamental, point is that proposals for individual data ownership "double down" on the same atomistic vision of autonomy that animated twentieth-century informed consent requirements. Their underlying premise is that people, acting alone, can effectively protect their own interests—a questionable premise, as discussed below. Proponents of individual data ownership aspire to endow individuals with a bigger club with which to defend their own interests. The flaw is that individual self-defense—whether with a consent right or with an ownership right—may not suffice as a way to protect against the privacy risks that lurk in the twenty-first-century data environment.

As noted, the most valuable data resources for big-data research are deeply descriptive in the sense of linking, for each

---

HARV. J.L. & TECH. 69, 77–82 (2012) (explaining why individual data ownership would not afford protections superior to those patients already have under existing federal regulations).

31. Evans, *supra* note 3, at 16.

32. *Id.*

33. Edella Schlager & Elinor Ostrom, *Property-Rights Regimes and Natural Resources: A Conceptual Analysis*, 68 LAND ECON. 249, 250–51 (1992) (describing entitlements of shared ownership of fisheries and other natural resources, including: (1) "operational-level" entitlements (e.g., a right to gain access to the resource and to withdraw products, such as a right to catch fish) and (2) "collective-choice" rights (e.g., a right of management including the right to participate in decisions about resource uses; a right to improve or transform the resource; a right of exclusion, including the right to participate in decisions about who can access and use the resource and decisions about the appropriate process for approving and enforcing access and use; and a right of alienation that allows the above rights to be transferred to other people)).

34. 2 WILLIAM BLACKSTONE, COMMENTARIES *2, http://lonang.com/library/reference/blackstone-commentaries-law-england/bla-201/ [https://perma.cc/B5SP-JUSU] (where spelling conforms to modern conventions).

included individual, multiple streams of personal health data. Such data resources can potentially be re-identified by cross-correlating data elements with external datasets that link those same elements back to the person's name or other unique identifiers.[35] However, re-identification risk is not the only threat to individual privacy. An even more perplexing problem in modern, interconnected big-data environments is privacy interdependence: individuals' privacy is "affected by the decisions of others, and could be out of their own control."[36]

Privacy interdependence is familiar in online social networks: Person A chooses to share a group photo that displays an embarrassing image of Person B, which the latter would prefer to suppress.[37] Particularly with genomic data, which display similarities among related individuals, one family member's willingness to share data in identifiable form may reveal information about others who did not consent to data sharing. When people's privacy preferences are misaligned and some of the people reveal even a limited set of attributes, "it is almost impossible for a specific user to hide in the crowd."[38] Moving past petty traditional conceptions of clan and kinship, we are all one big human family, sharing genomic data that is 99.9% alike and even sharing weight gains within our social networks.[39] Even when familial interrelationships are not an issue, data scientists have demonstrated re-identification attacks that can infer—sometimes with surprisingly high probabilities—who a given genome belongs to, by applying algorithms that rule out identifiable individuals that the data could not possibly belong to.[40] Thus, if my

35. *See* FED. TRADE COMM'N, *supra* note 5, at 19–22 (warning that the distinction between personally identifiable information and non-identifiable information is increasingly irrelevant in light of the potential for data to be re-identified); Ohm, *supra* note 5, at 1706–07 (discussing the risks to individual privacy if de-identified data were to be re-identified); Rothstein, *supra* note 5, at 5 ("Despite using various measures to deidentify health records, it is possible to reidentify them in a surprisingly large number of cases . . . ."); Khaled El Emam, Elizabeth Jonker, Luk Arbuckle & Bradley Malin, *A Systematic Review of Re-Identification Attacks on Health Data*, PLOS ONE (Dec. 2, 2011), http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0028071 [https://perma.cc/2C8Z-FJHK].

36. GERGELY BICZÓK & PERN HUI CHIA, INTERDEPENDENT PRIVACY: LET ME SHARE YOUR DATA 1 (2013), http://fc13.ifca.ai/proc/10-1.pdf [https://perma.cc/WWP2-9VC8].

37. MATHIAS HUMBERT, WHEN OTHERS IMPINGE UPON YOUR PRIVACY: INTERDEPENDENT RISKS AND PROTECTION IN A CONNECTED WORLD 66 (2015), https://infoscience.epfl.ch/record/205089/files/EPFL_TH6515.pdf [https://perma.cc/4JBL-4XUS].

38. *Id.* at v.

39. Nicholas A. Christakis & James H. Fowler, *The Spread of Obesity in a Large Social Network Over 32 Years*, 2007 NEW ENG. J. MED. 357, 371 (2007).

40. Arvind Narayanan, Assistant Professor of Comput. Sci., Princeton Univ., New Genetic Re-Identification Methods and Implications for Privacy, Presentation at Big Data: Policy Meets Data Science (Oct. 15, 2015).

neighbor shares her genome in identifiable format, her decision to do so raises the odds that my genomic information can be linked to me.

Faced with privacy interdependence, the individual's autonomous right of consent no longer suffices to protect individual privacy. To protect one person's privacy, it might be necessary to constrain other people's rights to consent to sharing of their own data. In effect, respecting one person's autonomy would require limiting the autonomy of others. Atomistic, autonomous decision making breaks down as a way to advance individual interests.

This critique differs starkly from the oft-heard criticism that individual decisions fail to advance the *public* interest (for example, by making it impossible to assemble data resources that could be used to advance public health and the wellbeing of other patients). This latter critique—that atomistic autonomy undermines public interests—has never proved persuasive among strong proponents of individual data privacy, who may view autonomy as encompassing a right to make decisions harmful to others. In contrast, the critique grounded in privacy interdependence highlights an altogether different problem: individuals cannot, through their own autonomous decision making, protect *their own* interests anymore. No person is an island in the environment of big data. Insistence on atomistic autonomy disempowers individuals, if the problems they face require collective action.

III. EVOLVING CONCEPTS OF AUTONOMY

In the years since 1980, some bioethicists have explored alternative visions of what individual autonomy means, such as an interactive or relational[41] view where autonomy is "not merely an internal, psychological characteristic but also an external, or social" one.[42] By this view, individuals enhance their autonomy by working together rather than by acting alone.[43] A simple example is that an individual's desire to think boldly and independently may best be served by affiliating with a bureaucratic, conformist university that has excellent libraries and research facilities. The "self is understood as a confluence of relationships and social obligations that are constitutive of identity" and autonomy may, at times, "legitimately be subordinated to other moral principles that determine how the self is

41. *See, e.g.*, TAUBER, *supra* note 12, at 121.

42. *Id.* at 120 (citing GRACE CLEMENT, CARE, AUTONOMY, AND JUSTICE: FEMINISM AND THE ETHIC OF CARE 22 (1996)).

43. *Id.* at 122.

governed within a social context."[44] As individuals, people are autonomous yet they are simultaneously embedded in social relationships and shared institutions, and these are instrumental to the realization of individual autonomy. Individuals acting alone are weak; individuals acting together are stronger. Social institutions are soil out of which common purpose can emerge. These views were mere eddies and side currents in twentieth-century bioethics.

Insistence on atomistic autonomy, when discussing data access, has had the unintended consequence of keeping individuals disorganized and, therefore, weak. Those who assert a right of individuals to block access to their data in all circumstances—even when other people's health depends on data access—run a risk of blurring the line between individual autonomy and narcissism, "a pattern of traits and behaviors, which signify infatuation and obsession with one's self *to the exclusion of all others* and the egotistic and ruthless pursuit of one's gratification, dominance and ambition."[45] One sometimes hears that even if research has high social value and consent is difficult or impossible to obtain, and even if requiring consent may undercut the scientific validity of results, these problems "do not in themselves constitute valid ethical reasons for waiving a requirement of informed consent."[46] Such views consign individuals to the condition Thomas Hobbes referred to as "the confusion of a disunited multitude,"[47] unable to act together for the common purpose of promoting wellness and public health and also, in a time of privacy interdependence, unable to mount a unified response to shared threats.

In Hobbes's scheme, these confused, disunited people are empowered when they come together to form "commonwealths," institutions they create to advance common purposes. When forming a commonwealth, people agree "every one with every one" to create mechanisms for deliberating and making collective decisions that bind all of them: "every one, as well he that voted for it as he that voted against it" shall embrace decisions made by the "consent of the people assembled . . . in the same manner as if they were his own."[48]

Governance, "in the sense of binding collective decisions about public affairs[,]" is one of a basic set of universal concepts that

---

44. *Id.* at 85.

45. *See Narcissistic Personality Disorder (NPD) Definition,* HEALTHY PLACE, http://www.healthyplace.com/personality-disorders/malignant-self-love/narcissistic-personality-disorder-npd-definition [https://perma.cc/3PBV-YCXZ] (last visited Dec. 29, 2016).

46. Franklin G. Miller, *Research on Medical Records Without Informed Consent,* 36 J.L. MED. & ETHICS 560, 560 (2008) (discussing but not necessarily espousing this view).

47. THOMAS HOBBES, LEVIATHAN 101 (1651).

48. *Id.*

anthropologists observe in both primitive and advanced cultures; other such concepts include giving, lending, reciprocating, and forming coalitions.[49] This core concept was poorly developed in twentieth-century bioethics.

In 2015, the White House Precision Medicine Initiative (PMI) finalized a set of Privacy and Trust Principles[50] addressing governance of the one-million-person PMI cohort, which aims to assemble genomic, clinical, and other sources of data on individuals who volunteer as research participants. These state, as the first principle: "Governance should include substantive participant representation at all levels of program oversight, design, implementation, and evaluation."[51] The second principle is that governance "should create and maintain active collaborations among participants, researchers, healthcare providers, the Federal Government, and other stakeholders."[52]

These principles reflect movement toward a new norm of treating people whose data are used in research as active participants whose engagement extends beyond the moment they sign an informed consent document. Kelty et al., in their recent meta-analysis[53] of what participation means in modern informational research and design practice, describe a tendency to treat participation as unidimensional and to "cherry pick one aspect of participation and substitute it for the whole."[54] In regulations like the Common Rule and HIPAA Privacy Rule, the right of informed consent was the lone "cherry" for patients and research subjects.

Meaningful participation, according to Kelty and his colleagues, engages people along seven distinct dimensions:

(1) Participants receive an educative dividend—they learn something or somehow gain skills or become better people by participating.

---

49. Stuart P. Green, *The Universal Grammar of Criminal Law: Basic Concepts of Criminal Law by George P. Fletcher*, 98 MICH. L. REV. 2104, 2112 (2000) (citing DONALD E. BROWN, HUMAN UNIVERSALS (1991)); *see also* Robin Bradley Kar, *The Deep Structure of Law and Morality*, 84 TEX. L. REV. 877, 885 (2006) (citing DONALD E. BROWN, HUMAN UNIVERSALS (1991)).

50. THE WHITE HOUSE, PRECISION MEDICINE INITIATIVE: PRIVACY AND TRUST PRINCIPLES 1 (2015), https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf [https://perma.cc/UVZ7-MUSU].

51. *Id.*

52. *Id.*

53. Christopher Kelty et al., *Seven Dimensions of Contemporary Participation Disentangled*, 66 J. ASS'N INFO. SCI. & TECH. 474, 476–77 (2015).

54. *Id.* at 475.

(2) They are involved in decision-making and goal-setting and are not merely instrumental to completion of a task by others.

(3) They have "control or ownership of the resources *produced* by participation."[55] The italics have been added to emphasize that this statement relates to the outputs rather than the inputs of participation. Simply owning the data one contributes as an input to research would not satisfy this requirement.

(4) Participation is voluntary and participants have the capacity to exit.

(5) They have an effective voice.

(6) The effectiveness of participation is evaluated using metrics.

(7) There is a "collective, affective"[56] experience of participating—people feel they are part of something greater than themselves.

If this is what it means for individuals to "participate" in research that uses their data, then twentieth-century regulations like the Common Rule and the HIPAA Privacy Rule fall short of it. The regulations give people a rebuttable right of informed consent and a limited right to withdraw their data from research after they consent, consistent with Item 4 in the above list. As for the other dimensions of research participation, a telling example is the immense efforts over the past twenty-five years by Internal Review Boards (IRBs) operating under the Common Rule, regulators, and bioethicists to restrict people's access to their own individual research findings, lest research participants should suffer psycho-social or other harms from learning through their participation in research.[57] So much for the "educative dividend" of Item 1. There is concern that research subjects are too unsophisticated, vulnerable, and susceptible to fear to benefit from education.

---

55. *Id.* (emphasis added).

56. *Id.* at 483–84.

57. *See* Barbara J. Evans, *The First Amendment Right to Speak About the Human Genome*, 16 PENN. J. CONST. L. 549, 577–83 (2014) (summarizing bioethical literature that recommends against allowing research participants to have access to data about themselves generated in research settings).

The PMI Privacy and Trust Principles seem to offer a new approach. Yet much depends on what the word "substantive" means in the first principle ("Governance should include substantive participant representation . . ."). Does this merely mean more-than-token representation—that is, more than the lone community representative that the Common Rule requires on an IRB? Alternatively, does it mean that the people whose data are used in research will be given a genuine voice in deciding which uses of their data are worthwhile and what the privacy, data security protections, and terms of use should be? The mention of "substantive representation" calls to mind the contrast between descriptive representation and substantive representation in Hanna Pitkin's work on meaningful representation.[58] For example, descriptive representation of women would involve having women serve in Congress, and thus it has a potential for tokenism. Substantive representation, on the other hand, would involve having representatives—of whatever gender—focus on issues of concern to women. A key question with the PMI Privacy and Trust Principles is whether they will go beyond token or symbolic involvement of research participants in governance bodies and focus governance on the issues that concern people when their data are used in informational research.

The preamble to the Privacy and Trust Principles is not altogether encouraging on this score. It recounts that the principles were developed "by an interagency working group that was co-led by the White House Office of Science Technology Policy, the Department of Health and Human Services Office for Civil Rights, and the National Institutes of Health."[59] The principles were "informed by a series of expert roundtables, review of the bioethics literature, an analysis of privacy policies and frameworks used by existing biobanks and large cohorts"[60]—seemingly a top-down, expert- and scholar-led pursuit of bioethical orthodoxy. Where were the people as the issues were defined? They were allowed to give "comments from the public," but only after the main contours of the principles already had been drafted. The people need to be engaged in data-system governance from the beginning, not just at the end.

Moreover, some of the Privacy and Trust Principles amplify these concerns. For example, the Principles state: "Communications

58. *See generally* Karen Celis & Sarah Childs, *Introduction: The Descriptive and Substantive Representation of Women: New Directions*, 61 PARLIAMENTARY AFF. 419 (2008) (citing Hanna Pitkin and discussing the concept of substantive representation).

59. *See* THE WHITE HOUSE, *supra* note 50, at 1.

60. *Id.*

with participants should be overseen centrally in order to ensure consistent and responsible engagement."[61] The notion that responsible public engagement requires central controls over the free flow of information is somewhat disquieting if this means that unelected IRBs will continue to block participants' access to information about themselves for the participants' own good. There is hope, but it remains far from clear, that the Privacy and Trust Principles mark a real departure from the top-down bioethics of the past.

IV. THE BEGINNINGS OF COMMON PURPOSE

It is difficult to imagine a scenario in which self-serving individuals, endowed with the right to make autonomous decisions that serve their own perceived best interests, would willingly surrender that right in favor of a norm of common purpose. One possible scenario is that self-serving people may be willing to eschew go-it-alone individualism if it ceases to promote their own personal aims. This section argues that, in big data environments, traditional norms of individual informed consent are not capable of serving the principal aim for which they were designed: that is, empowering individuals to protect themselves against research-related risks.

These traditional informed consent norms of the Common Rule and HIPAA Privacy Rule were designed several decades ago for clinical research and for small-data studies of the past.[62] In those contexts, individual informed consent is a rather effective instrument for protecting people from research-related risks. A person can effectively avoid the physical risks of clinical research by refusing to consent to the research. Such refusals are strongly respected in our legal system, which treats unconsented touching of a person's body as a battery. Only in rare circumstances, such as emergency clinical research where participants are not able to consent, can their right of consent be waived, and then only under the oversight of an IRB.

In informational research that uses a person's data, the principal risks individuals face are privacy and dignitary risks associated with data disclosure. At least in the past, a right of informed consent gave individuals considerable power to manage their privacy risks. The degree of privacy risk people faced, it was thought, was proportional to how widely they chose to share their data. The Common Rule and HIPAA Privacy Rule do allow some unconsented uses of data in research, but only subject to constraints: for example,

61. *Id.* at 2.

62. *See* Evans, *supra* note 3, at 8–9 (discussing history of these regulations).

requiring data to be de-identified (which was thought to neutralize privacy risks), or requiring a consent waiver (which requires an IRB or Privacy Board to assess the privacy risks and judge them to be minimal).[63] In twentieth-century data environments, the consent norms embodied in current regulations plausibly advanced individuals' desire to be protected from privacy risks.

These assumptions grow weak in the modern big data environment, where cross-correlation among multiple datasets allows re-identification and where individuals' privacy risks are interdependent. This environment thus offers two incentives for people to band together to pursue common purposes. The first incentive is the one that Professors Faden, Kass, and their collaborators highlight: sharing individual health data offers a prospect of public health benefits, and it may improve the health of other people, such that the balance of individual and public interests justifies a moral obligation to share one's own data.[64] The second incentive is more self-serving: individuals, acting alone, may no longer be able to protect the privacy of their own health data. Collective action of many individuals will be required, even to serve one's own selfish aims. This latter point may turn out to be the more compelling rationale for collective action in the age of big data. It is possible that some people value their individual autonomy so greatly that they would be willing to let other people die to protect their own data privacy. Such people, while unwilling to work with other people to pursue public health objectives, may nevertheless be willing to cooperate with other people if that is the only way to protect individual privacy. In the age of big data, public health and privacy *both* are collective enterprises.

Common purpose requires civic solidarity. Richard Rorty has reflected on the long struggle, dating back at least as far as the Greek philosophers, to reconcile individual autonomy with membership in a community.[65] There is an obvious potential for autonomy to undermine solidarity. Some thinkers view solidarity as flowing from metaphysical principles—religious or ethical—that link the interests of individuals to the good of the community; others portray solidarity as more accidental, a product of socialization and historical circumstances.[66] The ultimate origins of solidarity and common purpose are fortunately not essential to this discussion. It is essential,

63. *See id.* at 7 (summarizing nonconsensual access under the Privacy Rule and Common Rule).

64. Faden et al., *supra* note 11, at 24.

65. RICHARD RORTY, CONTINGENCY, IRONY, AND SOLIDARITY xiii (1989).

66. *Id.*

however, to admit that people are deeply divided about the privacy, ethical, and moral issues in bioethics,[67] making solidarity difficult, if not impossible, to achieve.

Some people desire near-absolute control over their health data, while others would like to see everybody's data openly accessible for research and other projects perceived to advance the public good. These differences are deep and intractable and cannot be resolved through persuasion, because the disputants lack a shared set of principles—and sometimes even a common set of perceived facts—by which to judge whose view is correct. They are "moral strangers" to one another, to use Engelhardt's phrase about the perils of bioethical discourse.[68] Deliberation is circular: my religion is correct because its scriptures say so. Disputants must either agree to disagree or else impose their views by force, by lobbying Congress, or otherwise maneuvering to control the direction of policy.[69] Solidarity cannot be achieved by sitting down and talking about it.

In the absence of common purpose, will it be possible to assemble the vast data resources that twenty-first-century science requires? Under existing regulations, future access to data looks highly problematic. A detailed analysis elsewhere[70] reached the following conclusions: de-identification, which has been a major pathway for research data access in the past, draws increasing skepticism; re-identification risks are real. Even if de-identification worked, de-identified data have limited scientific utility because they cannot be linked together to form the deeply descriptive individual health records most useful to science. Waivers of consent and privacy authorization have been another important way to free data for research but they, too, are increasingly problematic. How can IRB members, in good conscience, deem the privacy risks of big, deeply descriptive, general-purpose data resources to be minimal, as waiver criteria require? Individual consent may be the only remaining regulatory pathway for obtaining access to data resources. Yet, even today, individuals do not consent to share their data in the numbers that would be required in order to assemble the very large-scale, inclusive data resources that twenty-first-century science needs. They may grow even more reluctant to consent in coming years amid growing public awareness of re-identification risks and privacy interdependencies.

---

67. *See* H. TRISTRAM ENGELHARDT, THE FOUNDATIONS OF BIOETHICS 3–7 (2d ed. 1996).

68. *Id.* at 7.

69. RORTY, *supra* note 65, at 73.

70. *See* Evans, *supra* note 3, at 17–24 (evaluating various pathways for assembling large-scale data resources under existing federal regulations).

Two approaches have been proposed (and, in various contexts, implemented) to address future data access problems. These two approaches are worth highlighting because they mark opposite ends of a spectrum that, at one end, maximizes the power of autonomous individual decision-makers and, at the other end, imposes compulsory data sharing to promote public good.

The first approach facilitates creation of personally controlled health records, to be shared according to individual consent.[71] Individuals or their designated agents, such as a commercial data management company, would obtain copies of their own health information—for example, by exercising the individuals' access rights under Section 164.524 of the HIPAA Privacy Rule[72]—and assemble these data into comprehensive individual health records. Individuals could then specify, in granular detail, the particular data uses acceptable to each individual. By accessing individuals' data in accordance with their declared privacy and consent preferences, multi-person data resources could be assembled on the basis of informed consent.

The opposite extreme is to enact legislation requiring compulsory data access to create large-scale data resources in the public domain[73]—for example, by requiring entities that hold data to supply it for specific public health, scientific, or regulatory uses. These data resources would be openly available for use by a designated group of qualified entities, such as public health officials or biomedical researchers, that are legally authorized to use data on the public's behalf.

---

71. *See* Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 JAMA 1282, 1283–84 (2009) (discussing advantages of patient-controlled longitudinal health records and suggesting that one way to foster the development of such records would be to "give patients the rights to sell access to their records, rights that are superior to the property rights held by [entities that currently hold patients' data]"); *see also* Kelly Caine & Rima Hanania, *Patients Want Granular Control over Health Information in Electronic Medical Records*, J. AM. MED. INFORMATICS ASSOC. 0, 1–9 (2012); Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 651 (2010) ("[I]f patients were given ownership of their complete medical treatment and health histories, they could license to compilers their rights to that information in a propertized form that could be more fully developed and commercialized."); Eric M. Meslin & Peter H. Schwartz, *How Bioethics Principles Can Aid Design of Electronic Health Records to Accommodate Patient Granular Control*, 30 J. GEN. INTERNAL MED. S3, S3–S6 (2015) (discussing granular consent).

72. *See Individuals' Right Under HIPAA to Access their Health Information 45 CFR § 164.524*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/ [https://perma.cc/S2JU-U9SY] (last visited Jan. 3, 2017); *Questions and Answers About HIPAA's Access Right*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs [https://perma.cc/5ZJF-9YKZ] (last visited Jan. 3, 2017).

73. *See, e.g.*, Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 593 (2010).

Both approaches have limitations. The first can create useful data resources, yet its reliance on individual consent limits its potential to produce highly inclusive datasets that capture rare events (for example, rare genetic variants or unusual responses to specific therapies). Rare events are of great scientific interest in some contexts, including precision medicine, which by definition focuses on individual rather than average group characteristics. Studying rare events often requires vast datasets reflecting large samples of the population, and it sometimes requires datasets free of consent bias (selection bias).[74] At the opposite extreme, compulsory data access solves these problems but is ethically repugnant to many people. Moreover, it is fraught with practical and legal complexities that cause legislatures to reject this approach except in narrow situations where data are necessary to serve a compelling public health need (such as tracking epidemics and reporting child abuse).[75] Compulsory data access has never been—and probably never will be—embraced as a general solution to the problem of making data available for research.

Neither of the two extremes discussed fully resolves the problem of data access. Intermediate options are needed—options in the middle ground between individual, granular consent and compulsory data access. The Common Rule and HIPAA Privacy Rule implement intermediate options by allowing institutional data holders (such as hospitals, insurers, and research organizations) to override individual consent in specific circumstances—for example, if data are de-identified or released pursuant to an IRB-approved waiver. These intermediate solutions have always been controversial and, as noted, they seem doomed to fail completely in the near future. New intermediate options are needed at this time. The question is how to develop them.

V. CREATING LABORATORIES TO SEARCH FOR COMMON PURPOSE

One of the most questionable aspects of twentieth-century bioethics was its presumption that ethical and privacy standards governing research data access should be developed "top down"—by National Commissions, a Privacy Protection Study Commission, expert advisory bodies, or federal agency officials—rather than

74. Evans, *supra* note 30, at 95–96; *see also* IOM, PRIVACY REPORT, *supra* note 19, at 209–14 (surveying studies of consent and selection bias); Brian Buckley et al., *Selection Bias Resulting from the Requirement for Prior Consent in Observational Research: A Community Cohort of People with Ischaemic Heart Disease*, 93 HEART 1116, 1116 (2007).

75. *See* Evans, *supra* note 30, at 102–03 (discussing practical and legal problems); Evans, *supra* note 3, at 22–23 (same).

"bottom up" through collective decisions of the people whose data researchers wish to use. In normative ethics (the study of what constitutes an ethical course of action), experts "disagree so much and so radically that we hesitate to say that they are experts."[76] Courts consider normative ethics so standardless and nonreproduceable that there is ongoing controversy whether normative ethics testimony even meets the threshold for admissibility as legal evidence.[77] Government-appointed expert advisory bodies add value in fields—such as setting consumer product safety standards and water quality standards—where recognizable bodies of expert knowledge exist. But when answering the question, "What is an ethical use of an individual's personal health data?" meaningful public engagement offers expertise as credible as that of self-declared ethics experts. The "top-down" approach to setting ethical standards for data access may, however, reflect a pragmatic assessment that the people, if asked, would never be able to agree what the standards should be. Policymakers may simply have deemed civic solidarity to be impossible.

A mistake we may all be making is to assume that public engagement is fruitful only if there is a prospect that a broad public consensus will emerge. Too often, we assume that the public will never agree on appropriate ethics and privacy standards to govern data access, and the perceived intractability of their disagreement becomes an excuse to cut them out of the debate. The real mistake here lies in presuming that everyone needs to agree on a single set of uniform access and privacy standards, applicable to all, in order for data access to work. The reality may be that a vibrant framework of research data access can exist in the presence of multiple, competing visions of what ethical data access requires. If big data is as big as it purports to be, perhaps it is big enough to accommodate a "marketplace" of ethics and privacy standards.

Top-down ethical and privacy standards, such as those reflected in the Common Rule and HIPAA Privacy Rule, have not persuaded enough people to contribute their data to enable development of the vast data resources that twenty-first-century science ultimately will need. Those standards were, after all, *minimal* regulatory standards, not designed for the purpose of pleasing the

76. Bethany Spielman, *The Future of Bioethics Testimony: Guidelines for Determining Qualifications, Reliability, and Helpfulness*, 36 SAN DIEGO L. REV. 1044, 1056 (1999) (citing J.R. Bambrough, *Plato's Political Analogies*, *in* PLATO, POPPER AND POLITICS 152, 158 (R. Bambrough ed., 1967)).

77. Edward J. Imwinkelried, *Expert Testimony by Ethicists*, 76 TEMPLE L. REV. 91, 96–99, 105–06 (2003).

public, and they have not done so.[78] Why not engage the public in the challenge of designing a better set of standards that can satisfy concerns of data contributors, while still making data available for socially valuable research uses?

Other recent work[79] proposed the formation of consumer-driven data commons, which would be self-governing communities of individuals, empowered by access to their own data, who work together to assemble large-scale data resources for research. These commons are conceptually similar to the "data cooperatives[] that enable meaningful and continuous roles of the individuals whose data are at stake" that Effy Vayena and Urs Gasser have proposed for genomic research,[80] to "people-powered" science that aims to construct communities to widen participation in science,[81] and to the "patient-mediated data sharing" described in a recent report on FDA's proposed medical device safety surveillance system.[82]

Consumer-driven data commons would, in effect, be self-governing data commonwealths, formed by consent of the members—people self-selected because they share at least some degree of common purpose. These commons could be organized and operated by the members themselves, by disease advocacy groups, or by commercial data management companies acting as trustees to manage members' collective data resources according to rules the members themselves would set.[83]

Each commons-forming group would establish its own rules of access to—and use of—its members' shared data resources. Group members would deliberate and have a voice in setting their privacy practices as well as the duties and rights of membership in the group, their policies on entry and exit from the group, and how to operate their collective decision-making processes. This would not necessarily lead to adoption of ethical and privacy norms that differ starkly from today's Common Rule and HIPAA Privacy Rule. A commons-forming group might decide, after considering alternatives, to embrace norms

78. Evans, *supra* note 3, at 31.

79. *Id.* at 29–32.

80. Effy Vayena & Urs Gasser, *Between Openness and Privacy in Genomics*, 13 PLOS MED. 1, 1 (2016).

81. Berris Charnley, *People Powered Science*, CONSTRUCTING SCI. COMMUNITIES (May 14, 2015), https://conscicom.org/2015/05/14/people-powered-science/ [https://perma.cc/6GGW-FSAB].

82. NAT'L EVALUATION SYS. FOR HEALTH TECH. PLANNING BD., THE NATIONAL EVALUATION SYSTEM FOR HEALTH TECHNOLOGY (NEST): PRIORITIES FOR EFFECTIVE EARLY IMPLEMENTATION 27 (2016), https://healthpolicy.duke.edu/sites/default/files/atoms/files/NEST%20Priorities%20for%20Effective%20Early%20Implementation%20September%202016_0.pdf [https://perma.cc/6QQD-FB7T].

83. Evans, *supra* note 3, at 29–30.

similar to those reflected in current regulations. They might, however, tweak them slightly, for example, by electing members of the IRB that can grant consent waivers on behalf of their group, and making these members fireable at the group's discretion. Presumably, however, if people had been happy with the norms reflected in current regulations, they already would have contributed their data for scientific use, which most people have not done. The real value of consumer-driven data commons is that they offer a laboratory for modernizing ethical and privacy norms to function in big data environments. Commons-forming groups would enunciate their privacy and ethical standards "bottom up"—that is, for themselves—rather than having standards imposed "top down" by regulators, external ethics advisory bodies, and IRBs.

Some commons-forming groups might reject traditional regulatory norms altogether, replacing them with collectively agreed norms that are more (or less) favorable to research uses of data. Groups would enunciate their own visions of what constitutes an ethical use of their members' data. Some groups, to enhance the value of their collective data resources, might agree to abolish individual consent and instead make collective decisions about how their entire data resource—including the data of all members—can be used. The more inclusive a data resource, the greater its value to science.

No individual would be required to join a commons-forming group. Individuals wishing to participate would first obtain their own health data by exercising their HIPAA Section 164.524 access rights, which allow individuals to obtain a copy of their data held by HIPAA-regulated healthcare entities. Access to data held by non-HIPAA entities, such as wearable device manufacturers, is not subject to uniform national policies and varies depending on the manufacturers' policies, making it important for commons groups to encourage their members to do business with pro-access companies.[84] Having obtained their data, individuals could choose to deposit their data in one or more consumer-driven data commons. Once in, individuals would give up their right of traditional, granular informed consent to specific data uses and would instead agree to be governed by whatever norms the group had agreed. The individual right of consent thus would be conceived as a right to enter or not enter a specific commons group—to remain in or exit it in accordance with its rules—and to participate in the group's collective decision-making processes.

An advantage of consumer-driven data commons is that the Common Rule and HIPAA Privacy Rule do not restrict individuals'

84. *See id.* at 23–25 (discussing difficulties in accessing data from mobile and wearable fitness devices and other non-traditional sources of health data).

ability to sell their own data. In contrast, institutional data holders such as hospitals face restrictions, like the Health Information Technology for Economic and Clinical Health (HITECH) Act's restrictions on sale of data that make it hard to finance the development of large-scale data resources and to sustain them for long-term use. Consumer-driven data commons could make collective decisions about the revenue model they wish to adopt, using proceeds to retain legal and other consultants to help manage their data assets and to convert their data resources into consistent formats that enhance their value and scientific utility. However, the members of consumer-driven data commons would be free to decide that commodification of their data is ethically objectionable and instead donate their data resources for scientific uses chosen through their collective decision-making processes.

As groups enunciate their respective visions of ethical data access, there would be a marketplace of ethical and privacy policies. Individuals could compare these as they make decisions about which consumer-driven data commons best satisfy their own vision for ethical use of their data and their own goals concerning how their data should be used. A successful consumer-driven commons would be one that attracts members (by enunciating ethical and privacy standards that satisfy concerns of data contributors) yet is able to supply data for useful lines of research on terms satisfactory to those members (by threading the needle of ethically acceptable research data access). As successful consumer-driven data commons expand, their expansion would supply empirical data on what works and what does not work in engaging people in the excitement of twenty-first-century research and incentivizing them to contribute their data.

VI. CONCLUSION

The transition from twentieth-century small-data bioethics to twenty-first-century big-data bioethics, in many respects, resembles a shift from self consciousness to social consciousness. We are now officially interdependent, and collective action will be required both to overcome the scientific challenges that lie ahead and to protect our privacy as we do so. Regulatory frameworks of the past have served us well and will continue to deliver good service in the contexts for which they were designed—clinical research and traditional informational studies. They are not, however, adequate in the context of modern big data science. In developing new frameworks, "top-down" approaches of the past should be avoided. The people whose data are used in research possess expertise of what is ethical that is as valid as what regulators and ethics "experts" can offer.

Consumer-driven data commons offer a laboratory in which groups of consenting individuals can discover the common purposes that they share and can enunciate ethical and privacy standards that, at last after six decades of bioethical debate, will be of the people, by the people, and for the people.