The University of Chicago

Whose Vote Counts in the Medicalized Data Democracy?: An American Political Philosophy of Privacy Protection

By Isabel Salvin

A project essay submitted for partial fulfillment of the requirements
for a Bachelor of Arts degree in Public Policy

Paper presented to:

Instructional Professor, Chad Broughton

Instructional Assistant, Saliem Shehadeh

Undergraduate Program in Public Policy

February 23, 2025

Casual proposals for data democracy abound in the bioethical literature on medicalized data privacy. However, experts construe this goal differently according to their personal priorities, political proclivities, and institutional experience, and systematic attempts to reconcile these visions and evaluate their feasibility are lacking. Starting from first principles of constitutional law and privacy ethics, this paper considers the origins and validity of four data democracy philosophies spanning the political spectrum: deregulation, regulation, intermediary advocacy, and collective organizing. It canvasses potential approaches to enacting this system and presents structural impediments to privacy preference aggregation and data governance. References are primarily medicalized privacy philosophy studies and literature reviews but also include technical big data studies, public opinion surveys, legal scholarship and forecasts, public legislative records, and an interview with Dr. Peter Angelos at the UChicago Maclean Center for Clinical Medical Ethics. I argue based on this investigation that data democracy as commonly conceived of is – perhaps unsurprisingly – a worthy aim and a powerful tool to safeguard privacy. The intermediary approach to governance presents an especially compelling and realistic case. But before enacting systematic change, American society might do well to return to first principles, drumming up more grassroots participation, fortifying our institutions, and elevating democratic values besides privacy in our pursuit of an egalitarian regime.

Keywords: Data democracy, biomedical data privacy, privacy ethics, commodity societies, liberal democracy, data rights

Do you feel confident that your data is secure? It's what the parties violating your privacy labor to ensure. Healthcare organizations, academic research institutions, and corporations (among many others)[1] know more about us than we realize, yet they fight tooth and nail for their own privacy (Lanier 2013, Terry 2017). Traditional privacy policy assumes we are informed enough to decide on permissions for ourselves instead of putting in place substantive protections that much of the rest of the Western world enjoys (Smith 2011, 1000-1001). Still, our information travels. We consent to studies in university, corporate, hospital, and government settings that spirit it away to proprietary and open source archives and exchange it between institutions. Nobly expanding knowledge for the greater good, we risk sacrificing autonomy. But this tradeoff also happens needlessly: wittingly or unwittingly, in the most mundane exchanges and even via passive surveillance, we sign over our data to corporations who prioritize profits over privacy.

There is a broad consensus in America that data collection, use, and sharing should be more accountable to the people (American Medical Association 2022). Data privacy – most often defined as control over one's personal information – is in jeopardy at each of these points (IBM 2023). More digitized information has been produced in the last year and a half than in the rest of human history (Rivery 2024). Accompanying this "data explosion" is the emergence of "big data," prodigious datasets which when analyzed computationally "reveal human behavior and interactions" (Hoffman and Podgurski 2013, 499). Risk is everywhere, and recent breaches and violations have been widely publicized. In the Internet age, a doctor might open their e-notes to a catalog of your visit summaries stretching back years or even decades. What qualifies as

[1] These are the three sectors covered by US medical privacy law, whose interactions I will consider throughout this essay. For lack of space, I had to select representative examples from each. I will not be able to discuss pharmaceutical and biotech companies, pharmacies, insurance agencies, government departments conducting research (ex. public health, FDA), law enforcement, or employers using biometric data among others because additional laws or provisions apply to each.

medicalized data has also expanded exponentially beyond such traditional examples. New technologies have enabled everything from genetic sequencing to Facebook studies on the predictors of suicide among users. Biometric data (identifiable features including fingerprints, facial profiles, and iris scans), biomedical data (everything from diagnostic imaging to genetic analysis to heart rate graphs from your FitBit), and non-medical information (like an abortion-seeker's iPhone location or a teenager's shopping habits, which Target's marketing analytics used to predict her pregnancy before she was even aware of it) all feed into medical studies although each boasts different legal protections, which leave swaths of vulnerability in their wake (The World Bank Identification for Development 2025, DriveResearch 2023, Hallinan and De Hert 2016).

In a data democracy, "research participants are cast as a community that has interests and entitlements in controlling its data" (Blasimme and Vallena 2017). There are four models in the literature: self-regulatory, regulatory, intermediary, and collective (Schwartz 2000, 816, Prewitt and Siddarth 2021). The justifications that their supporters provide understandably focus on big-picture principles: they are idealistic, oftentimes literal works of philosophy, and motivated by heady privacy concerns. They include structural and operational recommendations only insofar as these illustrate the specific model put forth. A democracy is characterized by its accountability to the people, stable and balanced power structures, and avenues for citizen participation (Prewitt and Siddarth 2021). I argue that given privacy is such a nebulous concept to begin with, the proponents of data democracy ought to develop more concrete plans to ensure these cornerstones are in place. In order to collect privacy preferences, we need to assess the public's views, ensure that there are effective methods of preference aggregation available, and determine whether institutions can work together to compile and respond to these "votes" on

privacy (Shepsle 2010). Few of the data democracy proposals I have read address these issues, and none consider all of them across the three key domains where American privacy regulations apply.

Americans' privacy stances – along with doctors', researchers', and medical entrepreneurs' – depend on our ethical, legal, political, technological, and practical perspectives on the balance between individual rights and the common good. Priorities and incentives differ somewhat between individuals and our spokespeople in institutions, so we need to question whether we favor a representative or direct democracy or even something collectivist or anarchic. Can we reconcile these disagreements and tensions between Americans' economically and socially liberal viewpoints, or is there too much polarization for us to realistically settle on one of the four models? The passionate ideas behind these visions threaten anti-democratic consequences if we do not attend to and strengthen the relationships between individuals and the institutions processing their medicalized data. I believe that workable mechanisms are in place to enable a data democracy, itself an auspicious project since democracy and privacy are interlinked, but their many current faults pose a significant unaddressed challenge to all four proposals. What is the most promising way to improve America's medicalized data protection? The intermediary model in particular offers an actionable compromise. Still, before revamping data governance institutions, we should inform and empower the people, which would require reevaluating transparency, equity, and the overlooked nuts and bolts of these very institutions.

Why do reformers champion data democracy as an instrument for medicalized data privacy protection?

A healthy democracy has an interest in privacy. Without the opportunity to withdraw from public life, citizens would suffer decreased autonomy, and their legally protected freedoms of association and expression would be compromised. If they could not candidly offer their views, democratic participation would become coercive and lose its meaning. Democracies – echoing their constituents' stance – see privacy as essential to dignity and well-being and promise to preserve it. It is easy to argue that democracy needs privacy just as privacy needs democracy and that allowing these principles to mutually reinforce kills two birds with one stone.

Political freedoms and civil rights are preconditions of democracy, but democratic laws also limit these entitlements. Democracy and these liberties themselves depend on restrictions. For example, permitting individuals to keep one hundred percent of their medicalized data private would cause medical care, research, and the democratic marketplace of ideas to grind to a halt. This flagrant error in the law would render all other privacy rights – no matter how well-conceived – null and void.

As a liberal democracy, the US applies an atomistic political philosophy to our collectively organized system. Liberalism prioritizes individual rights. Ideally, it and democracy work as counterparts: while democracy without liberalism verges on a dictatorship of the majority, liberalism without democracy can mutate into a tyranny of "propertied elites." Liberalism shares democracy's affinity for privacy. Its most extreme variations suggest that individuals owe nothing whatsoever to society; the state exists to protect their self-interest.

Where it differs on the question of data autonomy is in its insistence on individual liberties (Hornet 2021).

Americans do not have a right to privacy. Yet a 2022 survey by the American Medical Association found that 92% of us believe that privacy is a right (American Medical Association 2022). 20 US states from red to blue have enacted comprehensive privacy laws (White & Case 2025). Our polarization manifests in the fine points of privacy debate and in ethical attitudes regarding the calibration of collective and individual entitlements. The rift between progressive and conservative liberalism highlights this philosophy's social and economic divergences from the democratic perspective. But when all is said and done, a right to privacy evidently squares with democratic principles.

Do Americans have measurable privacy preferences in the first place?

Why wouldn't data privacy activists target this neglected basic freedom as a first step towards data democracy? Instead of producing an abundance of proposals to restructure the data governance system wholesale, why not address such a pivotal misalignment at the federal level?

A key barrier to enshrining data privacy rights is the very individual perspective paramount in a democracy. If the people do not want this protection, to impose it on them would be more tyrannical than egalitarian. That Americans are uninformed and fail to coordinate and mobilize politically on the issue cannot be the full explanation for their inaction. On a more micro level, we often readily share our personal information although aware of substantial privacy concerns (in what literature labels "the privacy paradox") (Smith 2011, 993). Our actions may speak louder than our words. Studies find privacy preferences to be subjective and

culturally conditioned, dependent on individual disposition, demographic background, and community membership (Smith 2011, 1000-1003).[2]

Most philosophers do not recognize privacy as an intrinsic right or human good. The privacy entitlement to them represents not one unified interest but rather a collection of disparate principles: "The right to privacy can always be analytically reduced to other, more basic rights" (Goodman 2016, 152). Theorists tend to foreground autonomy (control over and license to access) as the basis for privacy's importance. While a handful take it as grounds for a privacy right, the majority question this relationship and argue instead that shielding autonomy is imperative so that rational individuals may pursue their interest in privacy (Smith 2010, 993), sounding much like economically liberal corporate actors. It is possible that Americans are making a conscious choice not to devote their energy to legal privacy right protections because from their perspective, the existing near-consensus ethical view renders this unnecessary. We may feel that the balance between privacy and these other rights settles differently depending on the situation, in which case securing a privacy right before any of the others could generate skewed results. Throughout decades of data ethics discourse, privacy has held a privileged position; it dominates discussions – and that may be costly (Lobel 2022).

[2] Those who are less concerned tend to be male, young, African-American, poorer, and less educated. One's family background/ethnicity may hold sway as well, as differences in institutional trust from country to country steer attitudes.

The legal privacy baseline is also influential. Study participants from countries with omnibus privacy legislation desire more regulation than those accustomed to sectoral regulation, who support more than subjects from countries with no privacy law. Thus, Americans' thinking is a product of our system thanks to a feedback loop which short-circuits critical thought and action.

The porous quality of our privacy opinions implicates interactions with the parties responsible for protecting our data. "Patients with higher trust in provider confidentiality have significantly lower likelihood of reporting having ever withheld important health information and lower likelihood of thinking it is important to find out who has looked at their medical records." Although this representative sample of patients had a limited understanding of confidentiality, they accepted one characteristic of a singular provider as a proxy for their data's ongoing security. Studies conclude that personalization benefits are another impetus to relax one's standards, which raises alarm bells given the ubiquity of this corporate gimmick in the algorithmic age.

Economic liberal ideology strikes one more blow to these rights: even if they are real, it claims to trump them. Privacy rights fall apart at the individual level not only as individuals brook competing ethical priorities and operate according to diverse psychologies but also as they assess material tradeoffs. Within a capitalist system, citizens are proficient in utilitarian cost-benefit calculations. The personal payoff for sacrificing data privacy need only outweigh the cost for abandoning rights to align with one's self-interest. Some in this school of thought actively criticize privacy for obscuring information, which diminishes market efficiency (Posner 1977, 404).

Countries like Australia, Canada, and New Zealand have long maintained omnibus privacy bills which cover all instances of data gathering, use, and transfer and define privacy as a human right (Smith 2011, 1000). The EU enacted a trailblazing General Data Protection Regulation (GDPR) in 2018 which extended this definition to all its member states; even US-based corporations have felt ripple effects (University of Michigan IT Services Safe Computing 2025). America and other commodity societies avoid such sweeping laws on principle, instead implementing a "patchwork" of sector- and data type-specific regulations (Smith 2011, 1001). Many of those in power operate according to an economic logic which regards additional legislation as inefficient and ineffective.

A more widespread and less controversial attitude than support for a privacy right is concern for privacy – however diverse and subjective its interpretations. Privacy preferences do exist – even if questions around their origins, morality, and assessment (via actions or attitudes?) intervene. While the contested realm of rights fails to provide a clear path forward, if our institutions are sound, the conditions are rife for more democratic representation.

How do Americans' representatives across the three regulated privacy sectors think?

The data democracy literature frequently analyzes the conflict between organizational actors' individualist and collectivist privacy thinking. In so doing, it overlooks a broader pattern: the custodians of medicalized data across regulated agencies skew more economically liberal on privacy issues than the public claims to be. In recent years, practitioners' prevailing economic, legal, and ethical ideologies have aligned along this axis. Companies handling medicalized data – data brokers, third parties, biobanks, social media platforms, personalized medicine and device providers, medical software brokers, et cetera – exemplify the liberal economic trend most plainly. To succeed in our capitalist system, they portray privacy decisions as a pure cost-benefit calculation, an individual choice that the free market leaves us at liberty to make. In the past couple of decades, a transition from torts to the subcategory of property law has swept the medical privacy landscape (Bambauer 2024). This development is in companies' interest: the economic rational choice theory of law takes the combination of free exchange and property law as the efficiency-maximizing model. In other words, corporations see individual privacy choices as optimizing efficiency and markets as optimizing freedom, the ability to make these individual decisions. The Coase Theorem suggests that given privacy is effectively a property right, when an individual agrees to disclose their medicalized data to a company, the right to privacy will drift towards whichever party values the data more (Professor David Lebow, Introduction to Law, Letters, and Society lecture notes). Under economic logic, this efficient outcome is admirable.

Neoliberalism nestles between economic and social liberalism. It stops short of blocking state interventions in the market and instead redirects state power to favor market interests. This

doctrine – operating since Reagan – has installed technocratic public regulators trained in cost-benefit analysis. It shifts governmental power away from the democratically accountable Congress (where countless privacy bills are currently stalled or slow-moving) to more centralized presidential offices (Professor David Lebow, Introduction to Law, Letters, and Society lectures). I notice its fingerprints in 1999's pioneering appointment of chief privacy officers and counselors, new executive committees like 2009's Presidential Commission for the Study of Bioethical Issues, and FTC-mandated privacy officers across presidential agencies (University of Michigan IT Services Safe Computing 2025). In 2012, President Obama announced the "Big Data Research and Development Initiative," a government effort to collect and publicize massive quantities of data so as to open up avenues for research and knowledge sharing (Hoffman and Podgurski 2013, 503). By maximizing data transparency, the state cedes its monopoly on formerly classified data. It seeks to level the competitive playing field so that companies' success reflects on the value they add to data through their analysis, not just their ease of access via lack of transparency (Davies 2010, 2).

As far as ethics, healthcare and research institutions have witnessed an encouraging internal shift away from paternalism. This doctrine had emboldened professionals to direct patients'/subjects' treatment according to their charges' best interest – even if it compromised their autonomy – when patients/subjects did not completely understand the choice at hand and its implications (Lamont et. al. 2013). Data custodians today typically report a practice of respecting individual wishes when privacy dilemmas arise. Ethical principlism urges them to make decisions based on "respect for autonomy, beneficence, justice, non-maleficence," and above all, their charges' input (European Bioinformatics Institute 2025). Nonetheless, organizational administrators operate at a remove and – beyond IRBs' and hospital ethics boards' purview – are

much more disposed to take on the privacy as commodity economic and legal perspectives (Interview with Dr. Peter Angelos 2025).

There is still merit in examining individual practitioners' perspectives. Data custodians at different rungs on the institutional ladder rely on varying professional norms, economic incentives, laws and levels of policy awareness, and answerability to internal governing bodies. They may consult different regulations (working group vs. organization vs. professional vs. state vs. federal) and norms/codes of conduct when deciding to what extent to factor in the public's perspective. Can they still reliably evaluate their clients' opinions on data privacy? How much discretion should we afford the people making and implementing data privacy decisions? Should a data democracy correct for some of this inconsistency? How representative should it be given this setup? The four governance models address these concerns.

I will assess where the strongest ideological inconsistencies appear in each and how these endanger the individual perspective. Existing analysis on the corporate, research, and medical actors strikes me as siloed between them: a reflection of the sectoral legal regime. The result is several unanswered questions about their interactions. Applying any given proposal to all three of them demonstrates that certain groups will struggle more to adapt, complications multiply across several organizations, and some entities will reclaim various attempts to rein them in to antidemocratic ends. Thus, I will illustrate my critiques through industry examples that try to present a broader point of view.

Organizational and corporate self-regulation

How does an outlook focused on economic self-interest, corporate privacy rights (but not individual ones), and internal procedures purport to serve the common good? While this model offers convincing democratic arguments for contextual adaptation and self-regulatory incentives, I believe that healthcare organizations' struggle to reconcile top-down and bottom-up reforms in their internal governance threatens to tilt the balance away from individual interests. Meanwhile, the corporate transparency case for self-regulation is questionable and potentially undemocratic, and the individual economic logic underpinning this viewpoint is unpalatable given the obstacles to an informed decision.

Self-regulation addresses fears of government inefficiency and stifling innovation. Even those in favor of regulation can appreciate this alternative's ability to take on issues the government does not have authority over. Institutions can lean on technology to support privacy as well; this approach is adaptable all around. It is in medical professionals' interest to protect privacy as they see fit. For instance, doctors operate according to an ethical framework (principlism, the product of that shift away from paternalism) that prioritizes adaptability to patient wishes. This ground-level investment lends the model credence.

Companies have an especially well-defined incentive to self-regulate. When it comes to privacy, partaking in unpopular data practices could harm their reputation, bringing costs that outweigh potential short-term profit optimization and incurring new governmental restrictions. Operating out of similar caution, corporations predicting stricter data laws will pass can minimize downstream compliance costs by instituting ethical data guidelines now. Such action may invite a competitive advantage (McCoy et. al. 2023, 8-9). If companies disregard the

public's privacy concerns, they may undermine trust in the industry at large (The Hastings Center 2014). Many conglomerates have recently adopted oversight bodies to address gaps in the privacy legislation, but these moves have been regarded as possible "ethics washing," which is the downside to corporations' ulterior profit motive (Agata et. al. 2021, 3). Companies are less regulated than academic institutions and healthcare, and the public anxiety surrounding them is at a fever pitch: 80% of surveyed Americans report the risks of companies' collecting their data outweigh the benefits (Pew Research Center 2019).

Clinical ethics boards' internal governance raises red flags around bottom-up approaches. Their patient/research subject-centered ethical outlook and encouragement of practitioners to think for themselves risk a disconnect with regulations. The quality and procedures of these boards vary wildly from institution to institution (Ferretti et. al. 2021, Hoffman and Tarzian 2007), and doctors' familiarity and concern with the law ranges depending on specialty, experience, personal ethical attitudes, and the recency of the law (Koskenvuori 2018, Singh 2016, and Pais 2020). In such a setting, enabling too much discretion may be hazardous. Studies show that organizational and professional ethical competence need to improve (Fouad et. al. 2022, 1399) – whether self-regulation on its own will eventually usher in these reforms is uncertain.

The data collected through university Internal Review Board (IRB) studies contributes to large quantities of scientific knowledge, and improvements in IRB regulation have led the public to trust academia more than either healthcare providers or companies. Still, like medical ethics bodies, IRBs are viewed unfavorably. They are insufficiently bottom-up by contrast (given poor lay representation), tend to get lost in procedural details (which burden would only increase

under self-regulation), and often opt not to publish their internal codes of conduct, which results in a lack of democratic accountability (Ferretti et. al. 2020, 19).

A key argument for bottom-up governance in both of these sectors is that professional medical and research ethics and norms may be more pressing than the law. Their boards' reliance on ethical guidelines rather than just legal rules might generate more nuanced decisions than are possible at state level (Dara et. al. 2017, 339). This strategy also may appeal more to practitioners, who tend to worry most about their day-to-day decisions and consider liability only insofar as it affects research certification, which happens through institutions like IRBs anyways (interview with Dr. Dr. Peter Angelos 2025). All the same, over the decades, patient/subject protection laws have accelerated the transition to decision-making grounded in individual autonomy. Perhaps internal governance can afford to be more top-down given these protections and the valuable expert perspective institutions are especially well-prepared to provide. The implementation of bottom-up and top-down approaches in medical and academic settings respectively have left much to be desired. How critically the sectors are currently evaluating these self-governance options is unclear, and neither option is more evidently democratic in practice. These conditions will complicate future efforts to design democratic data privacy self-governance plans.

A final concern with self-regulation is its potential for corporate obfuscation. Ironically, this danger is cloaked in promises of transparency (Price II and Cohen 2020, 10). The legal third party doctrine maintains that when our information is shared with a third party, we have no privacy rights over it, which puts consumers in a compromising position to begin with (Kaminski 2018). Companies toy with transparency in their marketing. Also with privacy: keeping our data "secure" is in their proprietary interest and reduces transparency. Sometimes, companies

successfully argue that these practices constitute protected speech ("Recent Proposed Legislation" 2023). Internal data retention policies allow extended storage, and there is no economic incentive to delete our data, which again might be forbidden anyways under deletion and disclosure rights (McCoy 2023, 7). Many companies have exclusive rights over enormous health datasets, and their operational procedures are masked by NDAs. Similarly, data brokers claim to "bring transparency to technology and democratize data access" so as to hide their "unpopular, nonconsensual business and data sharing practices" (Allen 2016, *Scientific American* 2023). They can use access to such data as an "anticompetitive cudgel," which goes against the fundamental free market principles motivating self-regulation to begin with (Cyphers and Gebhart 2019, 33). A lack of public accountability and laws may leave their power unchecked, kneecapping democratic checks and balances.

To conclude on the individual perspective, we are sitting ducks when it comes to the economic logic and economically liberal, privacy as a commodity nature of this framework. That is, advocates for self-regulation argue that it preserves our autonomy and enables us to make essential personal cost-benefit calculations, but our personal opinions mean little if the institutions meant to survey and convey them cannot get their act together.[3] Neither bottom-up nor top-down internal governance has so far managed to address these issues, and an uneven regulatory regime gives the corporate sector yet another leg up. At an individual level, a vicious cycle emerges: how can a public lied to and denied a seat at the table formulate any sort of meaningful privacy opinions?

[3] They may also mean little on their own given the privacy paradox and companies' tendency to consider consumer behavior to the exclusion of reported attitudes. See the later section on problems with institutional vote collection for more details on organizational failures.

Government support for self-regulation: the neoliberal middle ground

The regulatory approach suffers from a striking internal divide between socially and economically liberal logics. Bridging these economic schools of thought, the neoliberalism our government has embraced fosters slow-moving debate over how much political intervention is appropriate; state action raises suspicion over transparency while market protection threatens equity. In this inefficient context, agitating for individuals to have more say makes it harder for them to get a vote in – yet another example of antidemocratic fallout.

The case of big data makes plain how tenuous neoliberalism's compromise position is. How much transparency is too much? Once again, an excess can tip over into the invasion of privacy. Skeptics of neoliberalism's use of state power and/or government intervention overall fret that making information free "incentivizes the government to spy as the people relinquish their power of the purse" (Cyphers and Gebhart 2019). Government surveillance is a real threat especially given that recent Court cases like *Cruzan* and *Lawrence* have relaxed the conditions for states to discount citizens' privacy (Exploring Constitutional Conflicts n.d.). Individuals and actors from all three sectors may object to the government obtaining their information – regarding for example members of marginalized groups, women seeking abortions, or corporate medical products. Those who wonder why neoliberalism lets the market run free may interrogate the assumption that competitive advantage becomes more meaningful when data is fully transparent. The entity with more computing power still benefits far more from open data than others; for some, this newly available information may not even be legible or usable without costly technology (Davies 2010, 35). Equity is at stake, and the open data project also risks siphoning away resources from other possible data protection measures, which is a potentially

bipartisan argument (alternatives could be more or less market favorable) (Kingman and Martinez 2024).

The regulations that are in place around open data will result in "lower profit margins for firms and higher prices for customers." Consumers feel that companies can build on this data more effectively than the government, so for the government to position itself at a potential advantage over them is fishy (Smith 2011, 1001). An alternative data pricing scheme would be an option under a more market interventionist order. If individuals received compensation when organizations used their data, grand data schemes like open data (and even more so proprietary corporate datasets) would need to earn money by adding value (as open data hoped to prompt) rather than "using people's information against them" (Brino 2013). Perhaps such a view is not antithetical to free market thinking either once the government regulates it into existence: tagging information with a commercial value could allow for an efficient market resolution of the privacy dilemma. It would be more equitable as well. Currently, a significant barrier to personal privacy is access to and knowledge of technology, but if we could price our data according to how much we personally value our information, we might have more agency. On the other hand, enshrining this market logic into law could serve to reinforce its incentives to surrender data for material rewards.

The state has the power through the law to alter societal norms. It can revise maladaptive beliefs, introduce policy interventions and incentives to change groups' behavior, and even construct "positive bandwagon effects" which stimulate peer pressure (Schwartz 2000, 856). Its potential to advance privacy interests is notable, but its pervasive slowness warrants examination. Gridlock – if relevant at all here – cannot be the whole answer: all one has to do is consult public opinion polls and the bipartisan sign-on to bills across red and blue states. I

believe innovative privacy laws struggle to pass because of the very economic logic that the neoliberal system upholds among its bureaucrats and the American people. It has perverted its extension of state control and stepped away from the wheel on market regulation instead of critically striving for genuine transparency. In order to justify its power, the state should not delegate the data revolution to the corporate sector. If its economic logic is relevant anywhere, it may be internally given longstanding bureaucratic inefficiencies. That the argument for private right of action (the ability to sue companies for privacy violations) has stalled many medicalized data privacy bills (Klosowski 2021) is emblematic of the government's misaligned priorities; it represents just one of many undemocratic legal side effects alongside similar consequences for transparency and equity.

Government regulation of institutions

The current scene, as in self-governance, is less than ideal. Laws are durable and especially in a rapidly changing technological environment, not so adaptable. Whereas institutions can foreground researchers' and doctors' ethical patient focus, whoever has the data owns it according to federal laws' hot potato game.

Granted, an artillery of precedent backs privacy warriors, who can craftily and effectively defend this right even without precise legal backing. The consummately liberal Bill of Rights overflows with privacy implications – from 1st Amendment privacy of beliefs and 3rd Amendment privacy of the home to 4th Amendment privacy of the person and possessions against wrongful searches as well as 5th Amendment defense against self-incrimination. The "Silent" 9th Amendment lends room for interpretation, and several justices have used it to justify

privacy protections beyond what the four previous amendments furnish. Originalist Supreme Court Justices are reluctant to recognize any Constitutional privacy shields beyond the amendments, but from 1923 through the present, Court decisions have interpreted the 14th Amendment's promise of "liberty" to encompass a breadth of privacy issues (Exploring Constitutional Conflicts n.d.).

For centuries, the legal system has proffered torts as a recourse for privacy violations. When a party oversteps their "implied contract," the resulting "breach of confidence" constitutes a wrongful infringement on the plaintiff's implicit rights. Privacy regulations range from the local to the international; sub- and super-national law may supersede federal standards. The UN has stood up for privacy since its 1948 Universal Declaration of Human Rights, which guarantees "a right to the protection of the law against… arbitrary interference with their privacy" (University of Michigan IT Services Safe Computing 2025). Three states, California, Colorado, and Virginia, have piloted comprehensive consumer privacy laws. California's is especially robust and parallels the GDPR's data protection model; it illustrates "a growing transatlantic consensus emerging on privacy in the digital age" (Klosowski 2021, Kaminski 2018). As corporate operations and digitalized medical data extend across state and national borders, the big actors in medicalized data are compelled to consider various legal regimes. The most streamlined approach may sometimes be to accommodate themselves to the most stringent guidelines across the board (Klosowski 2021).

There *are* still plenty of potent federal regulations in play. The Privacy Act of 1974 and 1973 Fair Information Practice (FIP) Framework segued into the Privacy Protection Act of 1984 (spurred by new computer, network, and database capabilities). The '90s saw the rise of the Internet, the 1991 Common Rule on Human Research Privacy, and the first iteration of the

Health Insurance Portability and Accountability Act (HIPAA) in 1996. From the late ‘90s onwards, the executive branch has appointed an increasing number of privacy officers across internal agencies (University of Michigan IT Services Safe Computing 2025). Task forces and committees on fresh data concerns crop up regularly. The enforcement agencies (OCR and HHS for HIPAA, OHRP, HHS, and DoD Assistant Research Secretary for the Common Rule, etc.) for each law proliferate (Health.mil 2023). Most relevantly, a pile of medicalized data privacy legislation is on the docket. Its sponsors across the aisle call for a right to privacy (IAPP 2025).

On a less encouraging note, inconsistent state laws may be confusing to companies and consumers and as goes without saying, disadvantage local providers (Klosowski 2021). It is difficult for data engineers and IT crews to comply with laws that do not specify technical details. For instance, agencies use the Fair Information Practice Principles (FIPPS) to evaluate information systems with privacy implications, and these have received loud criticism from either end as weak, failing to require a privacy agency (a potential future government contribution widely called for), and behind on tech as well as “unworkable, expensive, [and] inconsistent with… freedom of speech.” New technologies adjust the relationship between privacy and disclosure, but it can be slow for the bureaucracy to adapt (Gellman 2024, 46). Techno-optimism is a potentially problematic orthodoxy in our neoliberal order: current big data laws for instance are extremely lax and assume that researchers somehow have consistent and developed ethical big data standards to follow. Laws constitute limited, rigid, and market-biased interventions.

Institutional vote collection: consent, representation, and consensus

Until we trust that the public is sufficiently well informed about the state of their medical data, reliably defining consent will be an uphill battle. Neoliberalism is built on negative rights, which preserve state power by foreclosing stronger entitlements to active control over our data (Professor David Lebow, Introduction to Law, Letters, and Society lecture notes). Unlike the European Union, we don't opt in to data collection: we opt out from the default order, exercising our right against the state (Smith 2011, 1001). Like the private right of action, consent is a sticking point in state privacy bills (Klosowski 2021). 75% of Americans would like an opt-in setup, but as economics measures our opinions by our actions, skipping that cookie approval pop-up keeps the system running (American Medical Association 2022). As we have all experienced, opting out is tiring, and the dials to click when you choose to specify your preferences can be overwhelming and time-consuming. In yet another way, our preferences lose their meaning. Like transparency, consent offers a competitive advantage (Kushmaro 2021); companies can tout their detailed cookie menus. But this pursuit only makes the thing itself hollow.

The three sectors operate according to different legal definitions of consent – HIPAA's broad consent and the Common Rule's informed consent engender debates in healthcare. Informed consent is a stronger protection, but it can be time-wasting and bias experiments so that only people willing and able to read the fine print participate (European Bioinformatics Institute 2025, McGraw et. al. 2015). No matter what, the third party doctrine promotes corporate interests, and our data's many afterlives are a complete mystery. Data portability rights are another proposed mechanism to increase consumer control over data (The White House 2016).

They would allow us to request to see our data after consenting to its release. I worry these may get lost in the hubbub of transparency and privacy rights discourse.

I ran into many calls for more research on consent (and general privacy) attitudes (e.g. Stone et. al. 2005), but what we do know is that people prefer sharing their information with academics, then the government, and last of all companies (Kaufman et. al. 2009). Public opinion suggests industry control and governmental regulation might not be the most trusted routes to democracy at baseline – and for another thing, consent documents should ask with whom patients want their data shared.

We need to decide whose vote counts in the data democracy. Issues like bottom-up vs. top-down governance and individual rights vs. group rights vs. the common good may be perennial and vary case by case. Strict economic liberals believe that increasing the quality of demand is the best way to calibrate our barometer. But overall, do we aim to preserve individual decision-making or shift to a more collective mode? Maybe rather than the people driving outcomes, their representatives from relevant sectors – be they practitioners or administrators – should step in. Whether we want a democracy or a republic leads into the question of whether industry groups should represent protected interests. In states like California, data protection laws have passed by ballot, but elsewhere, the legislature's vote decides. In my opinion, clinical and organizational ethics may struggle for dominance on internal regulatory boards; perhaps directly soliciting practitioners' opinions via a federal/state vote would yield more representative preferences.

If we want a more direct than representative democracy, bioethics' consensus procedure seems quite top-down for a democracy. Rigid consensus-based decision making is somewhat unaccountable and presents citizens with a falsely decisive expert opinion. In a society that

prides itself on its diverse value systems, why respect a consensus or even regard it as possible? Small groups within institutions may further distort the decision. Consensus is political: "bioethics [is] a consensus-oriented social reform movement," and consensus serves as a useful – attention-grabbing, forceful – tool (Moreno 1995). Still, a social consensus does not imply a moral certainty.

Preference exchange and sharing

Institutions advocate for themselves at the federal level. The government tries to arrange interactions between them. These exchanges can also be involved in mutual regulation. Because different standards apply to them, these groups might worry about becoming subject to additional liability if they share privacy-related information and thus are reluctant. The diverse professional standards between doctors and researchers also drive them to consult with different institutional boards, which means that assessing both groups' opinions is a struggle to coordinate. Given the dearth of existing research on such viewpoints and the relative emptiness of public privacy discourse, soliciting industry representatives' takes appears to be more of an obstacle than allowing them to speak for themselves and reconciling privacy regimes based on the government's response thus far.

Medical interest groups and data companies lobby on privacy to advance their professional and/or constituent priorities. There is a fear that companies may take on a "quasi-legislative power through undue influence on policy making" especially when conflicts come up between industry and government bodies; the political and the corporate coincide so often in the US that politics can easily be swayed to permit self-regulation (Ferretti et. al. 2020,

24). Federal laws are also full of loopholes across the sectors. IRB approval is waived for research without human subjects – which is so much of data analysis. Identifiable information can get through to corporations if it originates from the government (Health.mil 2023). A strength of the government regulation proposal is its prospective ability to harmonize these standards and to sync them with industry and institutional guidelines.

Data sharing between doctors and researchers is a sticking point. Doctors hesitate to share proprietary data, which incurs liability and can put a strain on the organization to transfer. Researchers and doctors alike worry that they do not understand each other's federal law and its data sharing requirements (US Institute of Medicine Roundtable 2010, Stone et. al. 2005). IRBs and ethics committees serve a distinct clientele (UChicago's ethics board, like many, sees mostly doctors). These bodies do not seem to interact much, and data administration and legal teams higher up in the institution may also sidestep any discussion (Interview with Dr. Peter Angelos 2025).

The neoliberal order makes it so that industry procedures reflect too much on societal decision making and generates inconsistent sectoral regulations. Against this backdrop, trusting the proposed representatives of our data democracy is difficult. Given these practical obstacles and the isolated nature of preference collection, it is unclear that current decision-making preserves individual voices. It may be more achievable to begin by improving public awareness and thereby strengthening consent's meaning rather than working to reconcile the inherently opposed big picture frameworks of self- and government regulation in a polarized state battling to maintain both.

The intermediary governance model

This plan sets itself up as distinct from the previous two because it is socially liberal. It asserts that data is not private property, nor something that the people must independently manage: We can collectively address collective problems. Under this branch of collectivism (model #4), the public entrusts a new kind of legal entity with the rights and fiduciary obligation to represent their interests (Prewitt and Siddarth 2021). Such organizations include Personal Information Management Systems (PIMS), data cooperatives, data trusts, data unions, data marketplaces and data sharing pools, many of which are already in place (EU Science Hub 2023). Data coalitions modeled on member-governed open source movements (which usually convene via location-spanning technology like blockchain) guide the organizations to negotiate with platforms and other companies on their behalf. Academics have also circulated checklists for these go-betweens to use in their enforcement tasks. The government regulates intermediaries and presides over complex arguments between coalition members and companies (Prewitt and Siddarth 2021).

The philosophy behind such groups is democratic but devoted to preserving individual freedoms; it strives for an exact 50/50 balance between its collective decision-making and duties to the collective (Prewitt and Siddarth 2021). It defines the common good as equivalent to individual freedom.

As this is my favorite framework, I will save its pros for the conclusion. It is a bit out there and deviates from many regulators' and Americans' economic logic, which may present problems in arbitration. Technology poses a barrier to entry, and the movement's special invitation to tech hobbyists could discourage other participation. The intermediary structure is

appealing, but who exactly will staff the intermediary organizations, and how can we ensure a balance of representation? How can organizers ensure that experts align with the movement's somewhat neutral constitutional values on privacy and left-leaning economic stance? A broader definition might account for existing academics, think tanks, watchdogs, norms-generating organizations, etc. who try to involve the general public in reform according to the guidelines they have formulated and negotiate agreements from companies to follow suit – this would be my uninformed suggestion.

Although the intention may be to maintain a balance between the common good and individual interests, a given intermediary will have to be a very authoritative structure in order to keep the outside actors it works with from continually directing results. It will need to secure a certain legal status for institutions with internal judicial boards to want to work with it and might have to reel in corporations with an economic logic it doesn't espouse – especially since it promises to secure benefits from them for its trustees. An intermediary similarly relies on sweet-talking the government to secure its interest: who in the movement has these skills and the necessary access to get the project off the ground? Finally, intermediaries commit to fulfilling a corrective function rather than directly calling for change; why not attempt something more?

Collective governance

Like the first two models, this one suffers from inequity and a vulnerability to economic and regulatory logics. The collective view redefines data democracy and science in ways that I find responsive to the current system's flaws. It points out the elitism of neoliberal technocracy even as it preserves its focus on technical knowledge and calls direct democracy into question as

overly deliberative and slow. By instead pushing for collaborative efforts, collectivism devotes itself to outcomes – once again, a neoliberal remnant. It pursues transparency so that nobody gets an unfair advantage but does not require "procedurally uniform dialogue" if it is not effective (Davies 2010, 16). A common critique of the government is that it overlooks data use and focuses only on collection. This alternative can compensate somewhat for the lack of distribution end regulation by taking into account the entire data pipeline. Although it is still vulnerable to breaches, it claims to prioritize confidentiality by keeping users linked to their information through the deliberation process (Vayena and Blasimme 2017). Its other strength is its reevaluation of science. It introduces an ethical "right to science and culture" and expands science by collecting data in unconventional settings and formats and via non-scientists, which introduces a more egalitarian perspective on research (Ienca and Vayena 2020).

Still, using biased, nonscientific data can set undemocratic outcomes in motion. Collectivism's lack of oversight and regulation creates vulnerability, and without the filter of publishing, there is the potential for misinformation to spread (Ferretti et. al. 2020, 9). More privileged and scientifically literate members might skew representation, as may people with certain diseases or unusually strong privacy convictions. The reliance on data from wearables, platforms, and data aggregators may perpetuate faulty consent models' ethical infringements (Wiggins and Wilbanks 2019).

"Pay-to-play services" like 23andMe are not citizen science: they are "for self-discovery, not scientific knowledge." Still, they illustrate what can happen down the line in this and either of the economically liberal models discussed so far: as personalized medicine gains currency, data mutates from a commodity into a luxury good. Profit-motivated actors can manipulate participants' hope to partner in research to their own ends. Pricey goods add another layer of

exclusivity while affordable resources attractive to citizen scientists may be booby-trapped: companies can resell mass collections of data or leave them unprotected on the labor market when they go out of business (Wiggins and Wilbanks 2019).

Collective governance sets up the public to collaborate with government bureaucrats (non-democratically elected for the most part) on database analysis and production. I feel that one more of its flaws is the reliance on open government databases, which provide ample opportunities to build data echo-chambers without any guidance on unbiased scientific methods (Collins and Varmus 2015). This ideology could easily become fully neoliberal or economically liberal in time, and its operations reinforce the standing corporate-government order.
Self-tracking may contribute to the democratization of science, but it also allows Big Data to reproduce itself. At this point, questioning why we view mass data so uncritically in the first place may be the more basic and necessary paradigm shift.

For all of human history before our age of information overload, the medical system managed just fine to deliver genuinely personalized care and come to research results humanely. Revolting against information sounds ignorant and luddite, and Pandora's box is already open; much of our data is out of our hands. We may benefit instead from using the information available to educate ourselves so that our privacy preferences mean something and we do not accept the current wide-eyed trust in data and its institutional stewards as an inevitability.

Next steps

Just to be sure, do we even want a data democracy? Given that privacy preferences vary so widely and the privacy paradox complicates assessment, maybe we shouldn't rely on majority

decisions. What if practitioners sometimes know better? It seems plausible in the current atmosphere of diminished transparency and public awareness. Institutional obstacles and faulty consent and consensus practices provide practical hindrances to the public's opinion making its way up the chain. The different elements of democracy we want to strive for all at once may conflict with one another (the private right to action stalls legislation). Individual protections can make for more biased research outcomes (ex. informed consent and participatory governance). Who says consent of the majority is more important than fairness? This puts a priority on autonomy rather than equity. Anyways, bolstering democracy cannot reverse the "protected interference of corporate interests in our democratic system" (Kennedy 2017).

Maybe before constructing a data democracy, we should reform American democracy. We might bridge the gap between economic and social liberalism by other means, scale back the economic logic driving so many decisions, etc. Some would argue that our democracy is perfectly fine, in which case we should just keep in mind moving forward that data doesn't need just any democracy: it needs a functional one.

Before trying to carry out one of the four governance models, I believe we should focus on three democratic first principles: representation, transparency, and equity. People already devoted to privacy organizing might target more efforts at getting a higher percent of the public involved in advocating for whatever system they favor. They might draw on the civic participation methods that self-regulation, regulation, *and* collective governance put forth. They can build networks to recruit more of the public and generate flows of information. Reform-minded companies can relax their marketing claims to transparency and simply be more open about their data processing procedures and the tools open to individuals to protect their privacy when interacting with less secure institutions. The government might fund a public

education campaign and grease the wheels so that institutions can more seamlessly work together to compile preferences and work towards data protection. The issue of equity emerged in my research as more pervasive, overlooked, and potentially amenable to consensus than privacy. Using equity to re-evaluate our thinking on privacy might therefore provide some clarity as a secondary benefit, but it seems to me that any and all of these three principles may be more pressing issues in the medicalized data governance space than privacy itself.

The collective movement's right to science and culture also strikes me as an eloquent way to protect the common good. If it could secure formal protections, it might moderate court disputes. Reigning in surveillance capitalist companies is my favored stance, but that may be due to personal political beliefs.

When we reach the point of striving for a new governance model, I predict that the intermediary option will garner the most support. Given the instability and inconsistency of the other three options, this one stands out as designed to broker compromise. Potentially more efficient than government and more accountable to the common good and rights than self-regulation, it avoids both of their easily manipulable economic logic and aims at equity and a balanced ethical perspective. I appreciate that it allows for a diversity of approaches (including some more grassroots agencies) but also recognizes and adapts to the fact that people higher up in administration tend to be more informed and influential and care more about this issue.

For the moment, I do not think we need to painstakingly revise our legal and ethical principles or question our fundamental political orientations. Simply by getting involved and fighting against the apathy our overwhelming data ecosystem and divided democracy can provoke, we will set in motion the push for a future we all basically agree on. As we urge change in whichever venues we personally find most effective, we will discover and continually revise

the democratic outcomes. The beauty of the existing system will hopefully extend far into the future.

Works Cited

Allen, Anita L. 2016. "Protecting One's Own Privacy in a Big Data Economy." *Harvard Law Review* 130 (2): 71-78. https://harvardlawreview.org/forum/vol-130/protecting-ones-own-privacy-in-a-big-data-economy/.

American Medical Association. 2022. "Patient Perspectives Around Data Privacy." *AMA*. PDF. https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf.

Bambauer, Jane R. 2024. "How to Get the Property Out of Privacy Law." *The Yale Law Journal.* https://www.yalelawjournal.org/forum/how-to-get-the-property-out-of-privacy-law.

Brino, Anthony. Healthcare IT News. 2013. "Q&A: Privacy Activism in the Age of Big Data." https://www.healthcareitnews.com/news/privacy-activism-age-big-data.

Collins, Francis S., and Harold Varmus. 2015. "A New Initiative on Precision Medicine." *N Engl J Med* 372: 793-795. https://doi.org/10.1056/NEJMp1500523.

Cyphers, Bennett, and Gennie Gebhart. 2019. "Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance." *Electronic Frontier Foundation*. PDF. https://www.eff.org/document/behind-one-way-mirror-deep-dive-technology-corporate-surveillance.

Davies, Tim. 2010. “Open Data, Democracy and Public Sector Reform.” PDF. 1-47. https://www.academia.edu/988533/Open_Data_Democracy_and_Public_Sector_Reform.

DriveResearch. 2023. “How Target Used Data Analytics to Predict Pregnancies.” Last modified January 8, 2023. https://www.driveresearch.com/market-research-company-blog/how-target-used-data-analytics-to-predict-pregnancies/.

Economist. Kaminski, Margot. 2018. “Toward Defining Privacy Expectations in an Age of Oversharing.” Published August 16, 2018. https://www.economist.com/open-future/2018/08/16/toward-defining-privacy-expectations-in-an-age-of-oversharing.

European Bioinformatics Institute. 2025. “Ethical Principles in Biomedical Data Collection.” Accessed February 12, 2025. https://www.ebi.ac.uk/training/online/courses/biomedical-data/data-collection/ethical-principles/.

EU Science Hub. 2023. “Data Intermediaries for More Inclusive Data Governance: How Do They Work?” Published October 4, 2023. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/data-intermediaries-more-inclusive-data-governance-how-do-they-work-2023-10-04_en.

Exploring Constitutional Conflicts. N.d. “The Right of Privacy.” Accessed 2025. http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

Ferretti, Agata, et. al. 2020. “Big Data, Biomedical Research, and Ethics Review: New Challenges for IRBs” *Ethics Hum Res* 42 (5): 17-28. https://doi.org/10.1002/eahr.500065.

Ferretti, Agata, et. al. 2021. “Ethics Review of Big Data Research: What Should Stay and What Should Be Reformed?” *BMC Medical Ethics* 22, 51. https://doi.org/10.1186/s12910-021-00616-4.

Forbes. Kushmaro, Philip. 2021. “Why Data Privacy Is A Human Right (And What Businesses Should Do About It).” Published June 7, 2021. https://www.forbes.com/councils/forbescommunicationscouncil/2021/06/07/why-data-privacy-is-a-human-right-and-what-businesses-should-do-about-it/.

Gellman, Robert. 2024. “Fair Information Practices: A Basic History.” *Creative Commons*. PDF. https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

Goodman, B. 2016. “What’s Wrong with the Right to Genetic Privacy: Beyond Exceptionalism, Parochialism and Adventitious Ethics.” In: Mittelstadt, B.D. *The Ethics of Biomedical Big Data*. Law, Governance and Technology Series, (29): 139-167. https://doi.org/10.1007/978-3-319-33525-4_7

Hallinan, Dara, and Paul De Hert. 2016. “Many Have It Wrong – Samples Do Contain Personal Data: The Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research.” *Ethics of Biomedical Big Data* 29: 119-137. https://doi.org/10.1007/978-3-319-33525-4_6.

Health.mil. 2023. “HIPAA Privacy Rule vs. Common Rule.” Last updated July 11, 2021. https://www.health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Board/HIPAA-Privacy-Rule-vs-Common-Rule.

Hoffman, Diane E., and Anita J. Tarzian. 2007. The Role and Legal Status of Health Care Ethics Committees in the United States. *Routledge*. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203799352-9/role-legal-status-health-care-ethics-committees-united-states-diane-hoffman-anita-tarzian.

Hoffman, Sharona, and Andy Podgurski. 2013. “The Use and Misuse of Biomedical Data: Is Bigger Really Better?” *Case Western Research University School of Law Scholarly Commons* 39 (4): 497-538. https://doi.org/10.1177/009885881303900401.

Hornet, Jan. 2021. “The Complicated Relationship Between Liberalism and Democracy.” Last modified May 13, 2021. https://www.orfonline.org/expert-speak/complicated-relationship-liberalism-democracy.

IBM. 2023. “What is Data Privacy?” Last modified December 19, 2023. https://www.ibm.com/think/topics/data-privacy.

IAPP. Kingman, Andrew, and Willy Martinez. 2024. “Data Privacy and Protection in the US: A Sign of Bipartisan Progress.” Last modified October 22, 2024. https://iapp.org/news/a/data-privacy-and-protection-in-the-us-a-sign-of-bipartisan-progress.

IAPP. 2025. “US State Privacy Legislation Tracker.” Last updated February 19, 2025. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Ienca, Marcello, and Effy Vayena. 2020. “‘Hunting Down My Son’s Killer’: New Roles of Patients in Treatment Discovery and Ethical Uncertainty.” *Journal of Bioethical Inquiry*. https://doi.org/10.1007/s11673-020-09963-0.

Kaufman, David J., et. al. 2009. “Public Opinion About the Importance of Privacy in Biobank Research.” *AJHG* 85 (5): 643-654. https://doi.org/10.1016/j.ajhg.2009.10.002.

Kennedy, Liz. American Progress. 2017. “Corporate Capture Threatens Democratic Government.” Published March 29, 2017. https://www.americanprogress.org/article/corporate-capture-threatens-democratic-government/.

Koskenvuori, Janika, et. al. 2018. “Healthcare Professionals’ Ethical Competence: A Scoping Review.” *Nursing Open* 6 (1): 5-17. https://doi.org/10.1002/nop2.173.

Klosowski, Thorin. 2021. “The State of Consumer Data Privacy Laws in the US (And Why It Matters).” *New York Times*. Published September 6, 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

Lanier, Jaron. 2013. “How to Think about Privacy.” *Scientific American*, November 1. https://www.scientificamerican.com/article/how-to-think-about-privacy/.

Lamont, Scott, et. al. 2013. “Health-Care Professionals’ Knowledge, Attitudes and Behaviours Relating to Patient Capacity to Consent to Treatment: An Integrative Review.” *Sage* 20 (6). https://doi.org/10.1177/0969733012473011.

Lobel, Orly. *Time*. 2022. “The Problem With Too Much Data Privacy.” Published October 27, 2022. https://time.com/6224484/data-privacy-problem/.

McCoy, Matthew S., et. al. 2023. “Ethical Responsibilities for Companies That Process Personal Data.” *American Journal of Bioethics* 23 (11): 2-10. https://doi.org/10.1080/15265161.2023.2209535/.

McGraw, Deven, et. al. 2015. “Privacy and Confidentiality in Pragmatic Clinical Trials.” *Clin Trials 12* (5): 520-529. https://doi.org/10.1177/1740774515597677.

Moreno, Jonathan D. 1995. Deciding Together: Bioethics and Moral Consensus. *Oxford University Press.* https://hss.sas.upenn.edu/content/deciding-together-bioethics-and-moral-consensus.

Pais, Veena, et. al. 2020. "To Evaluate the Knowledge, Attitude and Practice of Healthcare Ethics Among Medical, Dental and Physiotherapy Postgraduate Students—a Pilot Study." *International Journal of Ethics Education* 6: 97-107. https://doi.org/10.20529/IJME.2014.025.

Pew Research Center. 2019. "Americans Concerned, Feel Lack of Control Over Personal Data Collected by Both Companies and the Government." Last modified November 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/.

Posner, Richard A. 1977. "The Right of Privacy." *Georgia Law Review* 12: 393-422.

Price II, W. Nicholson, and Glenn Cohen. 2020. "Privacy in the Age of Medical Big Data." *Nat Med 25* (1): 1-16. https://doi.org/10.1038/s41591-018-0272-7.

Rasoal, Dara, et. al. 2017. "Clinical Ethics Support for Healthcare Personnel: An Integrative Literature Review." *HEC Forum* 29 (4): 313-346. https://doi.org/10.1007/s10730-017-9325-4.

Rivery. 2024. “Big Data Statistics: How Much Data is There in the World?” Last modified December 11, 2024. https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/.

Schwartz, Paul M. 2000. “Internet Privacy and the State.” *Connecticut Law Review* 32: 815-859. https://doi.org/10.2139/ssrn.229011.

Shepsle, Kenneth. 2010. Analyzing Politics. *Norton*. Chapter 7.

Singh, Surjit, et. al. 2016. “Knowledge, Awareness and Practice of Ethics Among Doctors in Tertiary Hospital.” *Indian Journal of Pharmacology* 48 (1): 589-593. https://doi.org/10.4103/0253-7613.193320.

Smith, H. Jeff, et. al. 2011. “Information Privacy Research: An Interdisciplinary Review.” *MIS Quarterly* 35 (4): 989-1008. https://doi.org/10.2307/41409970.

Stone, Margaret A., et. al. 2005. “Sharing Patient Data: Competing Demands of Privacy, Trust and Research in Primary Care.” *BJGP* 55 (519): 783-789. https://pubmed.ncbi.nlm.nih.gov/16212854/.

Terry, Nicolas. 2017. “Existential Challenges for Healthcare Data Protection in the United States.” *Ethics, Medicine and Public Health* 3. https://doi.org/10.1016/j.jemep.2017.02.007.

The Hastings Center. 2014. “Facebook’s Emotion Experiment: Implications for Research Ethics.” Last modified July 21, 2014. https://www.thehastingscenter.org/facebooks-emotion-experiment-implications-for-research-ethics/.

The White House. 2016. “Exploring Data Portability.” Published September 30, 2016. https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability.

The World Bank Identification for Development. 2025. “Biometric Data.” https://id4d.worldbank.org/guide/biometric-data.

US Institute of Medicine Roundtable on Value & Science-Driven Health Care. 2010. “Clinical Data as the Basic Staple of Health Learning: Creating and Protecting a Public Good: Workshop Summary.” *National Academies Press*. https://doi.org/10.17226/12212.

Vayena, Effy, and Alessandro Blasimme. 2017. “Biomedical Big Data: New Models of Control Over Access, Use and Governance.” *Symposium: Ethics and Epistemology of Big Data* 14: 501-513. https://doi.org/10.1007/s11673-017-9809-6.

Wiggins, Andrea, and John Wilbanks. 2019. “The Rise of Citizen Science in Health and Biomedical Research.” *The American Journal of Bioethics*. https://doi.org/10.1080/15265161.2019.1619859.

White & Case. 2025. “US Data Privacy Guide.” Last modified February 4, 2025. https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide#:~:text=Currently%2C%20a%20total%20of%20twenty,%2C%20Nebraska%2C%20and%20Rhode%20Island.