The Right to Share: Affording Americans Meaningful Control Over Their Data

Kevin Frazier
AI Innovation and Law Fellow
The University of Texas School of Law

Submission to the MJLST

Every opportunity to share our data involves a trade-off: the benefits of disclosure versus the risks of misuse. The potential benefits of sharing data have never been higher. AI tools trained on the right mix of data can help solve myriad public policy problems, such as detecting diseases, as well as address mundane, yet consequential personal issues, like planning a carpool schedule. The popular perception of the risks of sharing data, on the other hand, is also spiking. People do not trust the companies claiming to use their data for good. An increasing number of laws are attempting to protect us by making it harder and harder for us to share our information and for data recipients to exercise their discretion in how best to use any data they receive. While such laws may serve the interests of some individuals, they should not interfere with the right of every American to share as much of *their* personal data for *whatever purpose* they see fit. Congress should enact a federal "right to share" that preserves every individual's ability to control the flow of their personal information.

Current norms and laws around data sharing are grounded in faulty assumptions and excessive paternalism. The theory behind many data sharing laws is that we all behave as rational actors in the aforementioned trade-off: expertly and neutrally weighing the pros and cons. The fact of the matter is that most of us are not rational. Extensive research makes clear that humans tend to disproportionately weigh the costs when asked to make such a trade-off. "Loss aversion" results in many of us forgoing beneficial exchanges. The mental barriers do not end there. We also tend to suffer from a "status quo bias." In short, we're more comfortable with an inferior status quo than a preferable, yet uncertain future. Then there's the "endowment effect," which describes our tendency to place extra value on something we own compared to the value we'd assign to that thing if we hadn't yet acquired it. Add all this together and it's somewhat obvious why our willingness to share our data is quite low in many contexts.

An inclination to be miserly in data exchanges also reflects our general unease with the current state of privacy laws and data security. The vast majority of Americans have become highly skeptical of sharing their information with both "Big Tech" and "Big Government." More than 80 percent of adults are "concerned" with how companies use collected data; seventy-one percent feel the same way about government use of collected data. A litany of headlines reporting on data leaks, misuse of data, and general exploitation of sensitive information has likely sustained a growing feeling that, all else equal, the best thing to do is to hoard your data.

This understandable reflex has carried over to the Age of AI. The public is bombarded by messages of AI laboratories treating data as just another input of production, with little regard for the dignity interests often implicated by data sharing. There's no shortage of news on AI labs "stealing" data from artists, using data for purposes the user has not agreed to, and buying up

datasets with little regard for whether other AI stakeholders could have made better use of that information. While labs forecast incredible revenue, the average American is left wondering if they will receive any compensation for their contribution to AI improvements. All of these "vibes" amount to a general public sentiment that the costs of sharing their data for AI development are quite high.

The benefits side of the ledger, in stark contrast, is perceived as being quite low--thanks again to a media landscape keen to share news about AI 'going wrong.' The public has no trouble finding stories about Theranos-like AI companies that allegedly have the mission and technology to save the world but instead flounder. They also hear quite frequently about efforts to use "advanced AI" leading to failed projects and a need to rehire the humans who AI was supposed to replace. A handful of entities are fastidiously trying to collect, verify, and share instances in which AI is improving daily life and collective well-being. The Center for Data Innovation has been at this task for years. Sample positive uses of AI documented by the Center include substance abuse treatment centers using VR to help individuals develop positive habits in simulated environments, researchers relying on AI tools to learn more about the origins of cancer development, and drone developers leaning on AI to build drones that can fly at night and, therefore, immediately assist with search and rescue missions at any time of day. Yet, these positive case studies have not shifted the public's perception of the general direction of AI development. Half of American adults are more concerned than excited by uptick in AI use across daily tasks. What's more, a plurality are skeptical that AI will be a net positive over the long term. Thirty-five percent of adults expect that AI will have a net negative effect on the U.S. over the next twenty years.

General public concern about data sharing may explain why privacy laws at the state level are increasing in number and expanding in scope. State legislators keen to show their constituents how attentive they are to the public's concerns (justified, unjustified, or somewhere in between) have caught on to the public's appreciation for new constraints on data sharing and data use. It is becoming harder and harder for individuals and entities to share information. Little suggests this trend will abate absent a shift in popular perception.

In ideal circumstances, empirical evidence of demonstrated AI capabilities to advance human flourishing would lead to a reevaluation of the data sharing trade-off in favor of sharing more data. For the aforementioned psychological, cultural, and legal reasons, however, this seems unlikely. The more probable future is an "AI Abyss." In this world, wealthy individuals have access to proprietary AI systems trained on troves of quality data. Well-off Americans have demonstrated an increasing willingness to share their most personal information to access tailored health, educational, and professional insights.

Take, for example, Fountain Life. Every quarter Fountain's members undergo a barrage of tests--body scans, blood tests, and other assessments of more than 100 biomarkers. They then receive access to a series of tools to help them live a healthier life. An AI tool helps them interpret the results of their tests. Doctors prescribe treatments not only to correct for deficiencies but to improve the patient's performance across those biomarkers. Finally, they will

also receive access to “the latest regenerative therapies under FDA trials.” All of this for $21,000 a year. Meanwhile, more than 100 million Americans lack a primary care physician and all Americans face extensive barriers to controlling their own health information thanks to privacy laws enacted well before this Age of AI. This gulf will be replicated and is already taking place in other domains, such as education and career services.

This is not an endorsement of these AI use cases but rather an illustration of the fact that with more data sharing comes more opportunity, more freedom, and more liberty. When people can control when, how, and whether to share their information, they can contribute to collective efforts to improve AI tools intended to improve their lives and those of their loved ones. No American should be denied the opportunity to leverage their data toward such ends. All Americans should have the right to share their information with any other party for any purpose. Recognition of this right will drastically increase the odds of AI tools being developed that can reliably serve the needs of communities that stand to benefit most from advances in AI. Additionally, this right would legally entrench a sense among the people that they are capable of stewarding their own data. Nearly 80 percent of Americans trust themselves to make the right decision about their own personal information. Current privacy laws and norms, however, do not reflect that.

Imagine a rural community with few local health providers. The vast majority of residents live in poverty. Hardly anyone in the community regularly receives preventative care such as frequent screenings and timely health advice. Thankfully, there’s a clinic in town that does its best to meet local health needs. A doctor at the clinic learns about new AI tools that can be fine-tuned on a community’s health data to develop more tailored mental and physical health regimes based on that area’s environmental and economic factors. The doctor shares this information at a town hall meeting. She proposes to aggregate the clinic’s information, combine it with the health data people track on various wearables, and then work with the AI tool developers on discovering timely health insights. The public is, for the most part, thrilled. They see the potential to drastically cut down on emergency health costs and to improve their day to day experience.

The town lawyer, crouched in the back, then speaks up. He reminds them that state law mandates that regulated parties obtain handwritten authorization from a patient prior to sharing medical information with another party. This includes wearable app developers, he reports. What's more, such authorization is contingent on the intended use of that data being explicitly outlined. He concludes with a warning that each violation of the law may result in a fine of $2,500. A resident stands up and challenges whether this small town lawyer has a strong grasp of privacy law. Others chime in about his lack of experience in this field. The lawyer admits his limited knowledge but emphasizes that if even one resident or one state regulator has questions about the legality of this effort, then there may be months, if not years, of delays.

The vibe in the room quickly shifts. The understaffed clinic realizes that their plan is unlikely to come about. They lack the staff to go door to door and ask community members for their signature--a task made all the more difficult given that many residents do not speak English and

work non-traditional hours. The doctor is also unsure of how to work with the various wearable companies to get them involved.

Meanwhile, the next town over reports a surge in health metrics--they flag that many of their families have joined “Health Data Clubs” and swear by the AI-driven health recommendations they receive on a frequent basis.

So long as people lack control over their own information, stories like this will become all the more common. AI will never realize its potential to improve the lives of many Americans--especially those lacking access to some of the core components of a good life--under the current legal paradigm.

A few quick facts illustrate this point. Let’s start with mental health. Just 15 percent of children in need of mental health support who live in poverty receive care. We should not expect a reliable AI therapy tool until the law allows parents to share as much information as they see fit with AI developers. Current trends among state legislatures suggest this will remain the case. Until recently, Illinois law required that individuals seeking to disclose qualifying mental health information not only affirmatively consent but also have a witness testify to that consent. Washington recently enacted the My Health, My Data Act, which imposes numerous barriers on the exchange of protected information, such as separately receiving consent for both collecting and sharing data.

Next, let’s turn to education. During the pandemic, about 20 percent of wealthy parents hired personal tutors for their students. Only eight percent of low-income parents were able to do the same. In a future, similar scenario, under a right to share, AI tutors trained on each student’s learning style, grades, and skill level were available while schools were closed could have been made available to those kids. That’s unlikely to happen in any future marked by laws in which numerous boxes must be checked before a student’s data is shared. Compliance with the Federal Education Rights and Privacy Act, for example, mandates that schools go through several hurdles before sharing data with third parties and, even when permitted to do so, they must de-identify the data in ways that may limit the utility of that data for training personalized AI tutors.

The paradox at the heart of this problem is that the use cases of AI that have the greatest potential to benefit Americans are those that require the most sensitive and, oftentimes, legally protected information. Iterative processes to amend the disparate federal and state laws that form that protective shield to allow for more data exchange will take too long to prevent the formation of the aforementioned AI abyss. A federal right to share is the best approach given the stakes at hand.

Congress has clear constitutional authority to preempt state privacy laws that undermine the ability of individuals to share their data. Transfer, license, or sale of data via the Internet is clearly a matter of interstate commerce. Whole industries exist based on these exchanges. The Commerce Clause, even under today’s tortured and flawed interpretation of the Clause, permits

Congress to govern such exchanges. Though it is hard to exactly state which test a majority of justices on today's Court would endorse, the current framework looks into whether the activity in question qualifies as a commercial and whether the intervention falls into one of three buckets: regulating the channels of commerce, regulating instrumentalities (persons/things), and regulating activities with a substantial effect on interstate commerce. Data exchange satisfies these conditions. Transfer, license, or sale of data is clearly commercial given that whole markets exist around those activities and that some exchange of value or provision of goods or services is afforded to participants in such exchanges. The Court has also repeatedly interpreted telecommunications networks, such as the Internet, as channels of commerce. Laws impacting how, when, and under what conditions an individual may engage in a data exchange may also tick off the "substantial effect" box.

How the right to share would work in practice is fairly straightforward. The federal preemption would simply give Americans a right to opt out of any state privacy laws that would inhibit their ability to absolutely control the flow of their own information. For individuals disinterested in sharing their information to aid in the development of AI tools that align with their own well-being--life would not change. For Americans keen to see such tools come about, however, a whole new world could open up. This right to share would ease the creation of data cooperatives, for instance, through which individuals pool their information and make it available for various purposes. Parent Teacher Associations might form a coop of student data and use it to help create AI tools responsive to their unique community needs. Communities of individuals suffering from a common physical health ailment might do the same. You get the point. If and when a state or entity fails to recognize an individual's right to share, the Federal Trade Commission (FTC) may serve as the enforcement backstop. The Commission has taken an active role in enforcing company's terms of service and privacy policies. This experience will come in handy when assessing complaints raised under the right to share.

The technical aspects of a right to share are a bit more complicated. Rather than punt this question to others, I will attempt to roughly sketch some considerations to get the conversation started. I welcome feedback and suggestions! Key questions involve what form and mechanism of consent would be required. To start, consent via online means is a must. Barriers such as wet signatures on physical forms are the sort of paternalistic, process driven hurdles that run contrary to the assertion that people trust themselves to look out for their own data. People must also have a reasonable opportunity to revoke their right to share; this right, however, must be balanced against the needs of the data recipient to process any data they've received. An annual opportunity to opt back into state laws might be sufficient. There's also the matter of how granular the right to share would be -- is it an all or nothing arrangement that wholly exempts an individual from applicable state privacy laws or can it be asserted on a day-to-day, exchange-by-exchange basis. This latter question rests on technical considerations that are beyond my expertise. That said, again out of recognition of the agency and autonomy of Americans, I would err on the side of greater control, to the extent technically possible and administerable.

Of course, the practical design of a right to share must rest on a principled foundation—clear boundaries that respect other liberties and prevent abuse. No right is absolute, and the right to share should be no exception. This right must coexist with other core liberties and legitimate state interests. For example, a person's right to share cannot extend to information that directly implicates another individual's privacy, such as a family member's genetic data or a patient's mental health records that contain third-party identifiers. Nor should the right be used to facilitate fraud, coercion, or other illicit activities. Congress could therefore establish narrow, content-neutral limits modeled on existing exceptions to free expression—focused not on suppressing the choice to share but on ensuring that such sharing respects the autonomy and safety of others. These boundaries could be defined through FTC rulemaking, giving the agency flexibility to update them as new technologies emerge. In sum, properly bounded, the right to share would enhance liberty rather than erode it.

At its core, the right to share affirms a simple, deeply American idea: that individuals—not corporations, nor bureaucracies—should decide how their information moves through the world. This is the principle of informational self-determination. It does not call for reckless transparency or forced openness; it calls for agency. Just as the First Amendment protects our right to speak or remain silent, informational self-determination protects our right to disclose or withhold. Both rest on the same constitutional value: personal autonomy as a safeguard of democratic life. In this sense, the right to share is less a novel entitlement than a modern expression of the liberty our legal system has long prized.

For decades, our privacy framework has tilted toward distrust—assuming that individuals cannot be trusted to make responsible choices about their own data. A federal right to share would restore balance to that framework. It would give individuals a way to act on their judgment, their values, and their aspirations. It would also align the law with public sentiment: most Americans already believe they are best suited to decide how their personal information should be used. By grounding this right in the same respect for autonomy that animates property, contract, and speech law, Congress can move beyond paternalism toward a system that dignifies choice rather than restricting it.

Ultimately, informational self-determination is about participation—the liberty to take part in the digital and AI-driven future on one's own terms. The right to share would ensure that participation is voluntary, meaningful, and empowering. It would let every American decide whether to contribute their data to collective efforts that expand knowledge, cure disease, and improve daily life. In doing so, it would affirm a broader constitutional promise: that liberty is not merely the freedom from interference, but the freedom to engage, to innovate, and to build a better common life. In the age of AI, that freedom begins with the right to share.