



August 2026

Toward Associational Data Rights

A Digital Economy for Families and the Common Good

Daniel Cochrane

Lacey Strahm

Matt Prewitt

Salomé Viljoen

Editor's Note: This policy framework is the product of a 2025-2026 data governance working group convened by Daniel Cochrane, senior fellow at the Institute for Family Studies, in partnership with Matt Prewitt, co-founder of RadicalxChange Foundation, Lacey Strahm, Vice President of Growth and Impact at OpenMined, and Salomé Viljoen, assistant professor of law at the University of Michigan Law School. Institutional affiliations are provided for identification purposes only and do not necessarily constitute endorsement of this framework by contributors' home organizations.¹

Executive Summary

AI and the digital economy are broken. Despite the gains in economic growth and efficiency Silicon Valley has produced, those benefits have often come at enormous cost to American families and communities. Over the last decade, addictive digital products, like smartphones and social media, have rewired the brains of an entire generation, leaving many addicted, lonely, depressed, and diminished in their moral, social, and rational capacities.²

Even now, as parents and states gain ground in the fight to hold Big Tech accountable for its harms to children, a new danger is imminent. Generative and agentic AI—if left on their current trajectory—threaten to further hollow out American family life and erode the social, religious, economic, and political structures upon which human flourishing depends.

The evidence is all around us. AI companions are displacing human relationships and exacerbating a crisis in marriage and family formation. Employers are increasingly leaning into AI “bosses,” if not to replace their workers, then to reduce them to biological appendages of machines optimized for efficiency and short-term profit maximization. AI is also shaping consequential decisions from government services, healthcare, and education to the price families pay for groceries and other necessities. Even human thought and agency are now at risk with AI systems driving the mass offloading of human cognitive labor, like reading, writing, and independent creative production.

AI threatens to disempower American families and communities, in large part, because those bedrock institutions lack a voice in shaping AI’s course of development and its governance. Consequently, the incentives of tech corporations are often fundamentally out of step with those of most Americans and corrosive to the social fabric.

Part of the answer, then, is to recognize that nearly all data fueling the digital economy and AI is a co-produced good. Governance of digital systems and their outputs should be shared by the communities who co-produced the underlying data and who are most impacted by its use. Congress and the States should empower co-producers, through a new right of digital association and collective informational bargaining, to secure terms from tech corporations that advance community-specific privacy, control, and economic interests.

This policy brief unpacks this claim in three parts:

Part I argues that data is a co-produced good. Yet, control over its collection and use is concentrated in the hands of tech firms. Individuals, families, and communities have fundamental interests of **privacy**: restricting access to their information; **control**: deciding the purposes for which information they co-produce is used; and **fair value**: sharing in the economic benefits derived from co-produced data. However, because tech firms have asymmetric power to set digital terms of data collection and use, communally-specified privacy, control, and economic interests are often undermined. As a result, the incentives driving the digital economy often cut against the flourishing of human scale communities.

Part II makes the case for why both individual data rights and top-down data privacy regimes often fail to vindicate privacy, control, and economic interests.

Part III proposes a new class of informational rights:

- **The Right of Digital Association:** This right gives individuals, households, civil society institutions, and small enterprises (data subjects) the ability to join or form new intermediaries—Data Rights Associations (DRAs)—to secure terms governing data collection and use from tech corporations (counterparties) that advance community specified privacy, control, and economic interests.
- **The Right to Collective Informational Bargaining:** This right empowers DRAs to secure fair terms from counterparties by imposing a duty to bargain in good faith and providing a neutral arbitration mechanism to resolve impasses.
- **The Right to Fair Representation:** This right lays out specific duties that DRAs owe to their members, including duties of care and loyalty.

Part III also proposes standards for regulator certification and oversight of DRAs, recommends general obligations for tech corporations (counterparties) subject to collective informational bargaining, considers questions of financial and technical feasibility, and explores how a robust DRA ecosystem would advance pro-human, pro-family innovation.

Introduction

Silicon Valley culture is characterized by the motto, “move fast and break things.” Read charitably, it evokes a spirit of openness, innovation, and creativity. But for many Americans, the motto is emblematic of an elite tech culture that is itself broken, out of touch, and largely insulated from the social and economic consequences that its technologies unleash upon the world.

Frontier AI labs (“Big AI”), including OpenAI, Anthropic, and Google DeepMind, are racing to build superintelligent AIs to outperform and ultimately replace humans in every sphere: from work, to relationships, to politics, and even human thought and decision making.³ Elon Musk claims that within a few years, AI will be “unequivocally smarter than humans in every way.”⁴ An OpenAI employee said in 2026 that he “would prefer a world of rapid RSI [*recursive self-improvement, where AI models train their own successors without any human involvement*] and human disempowerment.”⁵

Even if they do not succeed, the same Big Tech companies, like Meta, TikTok, Google, and Amazon, that have surveilled, censored, and re-wired the brains of an entire generation, are poised to use AI to further dominate attention, monopolize our markets, and shape our beliefs and actions at scale.⁶ But it is not just the largest players. A growing number of mid-sized firms use AI to profile individuals, families, and communities with data harvested from a wide range of digital services and compiled by a shadowy web of data brokers.⁷

While these forces threaten individual dignity and freedom, their communal and wider societal implications are equally severe. The bedrock institutions of family and civil society are in the AI revolution’s crosshairs. Young men and women, already awash in a sea of digitally-induced distraction and erotica, are now tempted to turn to AI “companions” and chatbots with their most serious problems and intimate secrets, and to forgo human friendships, romance, and marriage altogether.⁸ Family and marital bonds are being steadily replaced by screens that serve up an endless supply of AI slop personalized by AI algorithms

optimized for addiction.⁹ Schools and workplaces risk becoming sites of mass social engineering, deploying powerful AI systems to surveil and replace human instruction, learning, labor, and thought.¹⁰ Algorithmic pricing threatens to further exacerbate the affordability crisis for struggling families.¹¹ And widespread public concern with Big Tech's AI surveillance and manipulation is undermining social trust, and with it, the necessary conditions for republican-self-governance at the communal and societal level.¹²

This trend toward dehumanization and social decay is largely driven by the race to capture data from every domain of human life. For too long, tech companies have enjoyed unrestricted access to the data we co-produce during our lives, both on and offline. All that data, paired with AI's growing capabilities of pattern recognition, prediction, and automation, have produced vast power asymmetries between human communities and the countless digital services they interact with daily. Those asymmetries have also resulted in parallel misalignment between the values and interests of the tech industry and the people it is supposed to serve.

Rather than compete to provide the most value and social benefit for the data they extract, tech companies often mask their commercial surveillance behind "free" or subsidized services, which they utilize to harvest as much consumer data and intellectual property as possible to develop products, derive insights about groups, and influence community members without affording them privacy, control, or fair value. The result: a consumer tech ecosystem that has done great damage to family life and marriage formation,¹³ and that is keeping us atomized, dependent, and scrolling alone.¹⁴

These effects have reached beyond the household into the other institutions upon which familial flourishing depends. AI and the digital economy's hunger for data is propelling the extraction of data from workers, artists, writers, and business owners, threatening to further diminish and centralize cultural production and commerce, and to disrupt social relations and truth seeking in the most important areas of civil society, including religion, education, and public life.¹⁵

Silicon Valley's current anti-human trajectory is bleak. But a different future is possible if we choose to embrace it. The 2025 statement, *A Future for the Family*, offers that alternative pro-human blueprint for the future centered on the flourishing of the permanent things—the social institutions and communal structures that give life meaning and that serve as the enduring bedrock of American society.¹⁶

*The family plants the seed and forms the foundation of the future, through the begetting and raising of children who will carry the human project forward. As such, the family, technology, and a dynamic and fruitful future are intrinsically connected, and the present conflict between them must be overcome.*¹⁷

Instead of smart devices and sensors that constantly feed data to outside tech companies and advertisers, we imagine a future where your home is protected, where data serves your family's needs—and only leaves with your permission and when absolutely necessary. Instead of screen-based devices that pull attention away from friends and family, we imagine new distraction-free interfaces that facilitate interaction with locally hosted AI models that serve humans on terms set by them and the institutions they inhabit. Instead of AGI that some believe will replace human labor, creativity, and relationships, we envision a competitive ecosystem of what Max Tegmark refers to as “tool AI,” designed to supplement, not supplant human judgment, solve real human problems, and foster ideal economic conditions for family formation and flourishing.¹⁸

To realize that future, public policy must give families and communities a voice in the development, deployment, and governance of AI and the larger digital economy. While regulatory floors to protect data privacy, kids, and families are necessary, society must fundamentally rethink the social contract between its essential institutions and private tech corporations. That starts at the data layer.

Galvanizing pro-human, pro-family AI innovation requires ensuring that data flows to digital products and services designed with human flourishing in mind. It requires moving away from asymmetric data and AI governance toward more evenly distributed polycentric governance.

A new class of associational data rights, chiefly a right of digital association and collective informational bargaining exercised through Data Rights Associations (DRAs), are crucial for addressing data’s complexity as well as the significant power asymmetries between human data co-producers on the one side, and the vast ecosystem of AI developers, deployers, tech platforms, and data brokers on the other. DRAs, like cooperatives and labor unions, would be empowered by law to secure fair terms from tech companies on behalf of individuals, households, and human scale communities. We envision DRAs as a new intermediary layer of digital rights bearing entities that would restructure data markets and provide strong incentives for firms to respect the privacy, control, and economic interests of families and communities over the long-term.

Part I: The Human Cost of “Infocapture”

Generative AI along with many digital products and services impose social and economic costs on Americans. Nearly every time a person interacts with a digital system, they knowingly or unknowingly trade data—information generated by them or others—for some immediate convenience.¹⁹ Whenever a person prompts ChatGPT to give them advice on the best local burger joint, the user trades data about themselves, including the query and whatever other contextual cues GPT extracts, in exchange for a response. Likewise, every time a small business owner “vibe codes” a new agent in Claude to improve their shop’s performance, the owner is trading valuable data—information about their business’s needs, operations, and clientele—to receive the promised efficiencies from the agent.

Even when families and community members do not directly interface with an AI agent or chatbot, they feed data to AI algorithms in a multitude of other ways. From Google Maps, which continually tracks users' geo-location data,²⁰ to “smart” home devices,²¹ smartphones, cars,²² and wearables,²³ each tiny contact with a digital product or service is a trade of a small part of ourselves for some convenience.

To be sure, users reap important benefits from the digital economy. Erik Brynjolfsson, for example, has coined the term “GDP-B” to refer to the unmeasured benefits of technology.²⁴ But there is also “GDP-C”—hidden costs—associated with AI and social media, like distraction, addiction, and the atrophy of human capacities for reading, writing, independent thought, and relationships. These costs are often overlooked by tech corporations because the human households and communities who co-produce the data shaping these technologies lack power to demand consideration of long-term social and economic trade-offs in the design of AI systems and the structure of the larger digital economy. One consequence is that the design, development, and deployment of AI systems and digital services seldom reflect—and often run counter to—the values and interests of the human institutions and communities most directly impacted.

Data co-production and the problems of asymmetric governance

Although AI and the entire digital economy are built atop mountains of human data, the centers of data co-production, including households, workers, artists, and consumers, lack power over its collection and use. Data collection and use is currently asymmetric, concentrating informational power in the hands of tech firms and a growing ecosystem of extractive data companies. This dynamic has resulted in a race to the bottom with unrestricted data collection and exploitative use fueling a vicious cycle of misaligned AI and antisocial digital products across the tech stack.

One reason for this trend is that neither U.S. federal nor state law currently treat data as a co-produced good and thus, do not afford human communities involved in its production with rights of co-governance (or “co-determination”).

Co-production

Data is often derived from a multiplicity of interactions between humans, entities, and AIs across the internet and a multitude of devices, services, and activities. Conversations between a human and an AI chatbot is one example of information or data “co-production.” The combination of human inputs (prompts) and AI outputs (decision, prediction, or content) creates information that would not exist without participation by the human party. Similarly, when an AI, like Google’s Gemini, draws on human knowledge and works to generate an answer to a human prompt (search query), both the human creators of the content used for inference and the human who inputted the original prompt are data “co-producers.”

Even agentic AI systems that perform tasks on behalf of humans with limited input or oversight, still involve some degree of data co-production. For example, agents that are ostensibly able to autonomously coordinate and execute tasks on behalf of human users need access to human data to set and pursue objectives, infer context, and carry out assignments. Most generative and agentic AI systems rely on massive volumes of human data for training. When an AI produces a novel image, video, or text-based output from training on human creative work, the human-creators of the AI training material have effectively co-produced the output, or at least, the capability that made the output possible.

Data is nearly always a co-produced good in at least two respects. First, it is derived from interactions between human parties and the digital providers that track and capture content and behavior. Even when behavioral data is not factored into an AI’s output—for example an AI surveillance system that relies solely on video monitoring within a private venue—it still relies on movements (video-based data) to assess risk or ID banned guests. In that sense, all AI outputs are inherently co-produced. AI systems require some non-static data input to produce actionable outputs.

Second, data is derived, in part, from inferring relationships and interactions between human individuals and communities. As a report from the RadicalxChange Foundation argues, data that reveals information about one individual often reveals something about others in that individual’s larger social circle: whether biological family, friends, co-workers, or other

interpersonal relations.²⁵ When users capture a family reunion or a friend's birthday through a pair of Meta Ray-Bans, they capture the activities, identities, and preferences of other people.²⁶ When users send a DNA sample to genome analytics company, Nucleus, they not only reveal information about themselves, but also information about other family members, such as their propensity for certain disorders, illnesses, and biological traits.

“Infocapture”

The problem is that much of that data, and its resulting informational outputs or products, are assumed to be the sole property of whichever tech platform or corporation manages to capture them. While sharing photos or videos between friends and a broader public audience might be permissible, the capture of that information for commercial gain, population level surveillance, or behavioral nudging is a different matter. The “ick factor” associated with videos captured by Ray-Bans is that tech companies or bad actors can now profile and identify every person in such content using AI and private surveillance databases, as Clearview AI has done.²⁷ In this sense, we are all victims of infocapture.

Perhaps in a world where humans are the only entities sharing and viewing videos and photos, the privacy trade-off, though undesirable, might be acceptable overall. But the purpose of the growing web of data hungry tech products is no longer to facilitate human-to-human disclosure as an end. Rather, it is to convert vast swaths of human life into machine-readable data to transform human-to-human disclosure into a means of total user and communal legibility for machines.

Unlike other areas of the market where co-produced value is accompanied by well-defined legal rights (of governance), such as in physical or financial assets like real estate and securities, data flows are determined by a digital law of the jungle. Data markets, and the larger digital economy they help shape, are overwhelmingly asymmetric. For the purposes of this report, “asymmetric” refers to the one-sided nature of data markets. While data is collected at various points and used in a multitude of different ways by many different actors, both its collection and use are often governed asymmetrically relative to the data subjects who co-produce it, or who are directly affected by the resulting outputs. Once information that data subjects co-produce is copied or captured, they lose control over its use.

Whichever corporation hosts the product or service that collects data sets the terms for who gets access to it and how it is used downstream. In other words, while data is almost always co-produced, rights to govern it are unilaterally (“asymmetrically”) exercised by tech firms and commercial enterprises.

This has fueled a digital race to predict and shape human behavior, and even to replace human labor, thought, and relationships. AI companies, like OpenAI and Anthropic, rely on vast amounts of data scraped from across the internet to train their models. But few of the human co-producers of that data get a say in whether their intellectual property (IP) is harvested or the conditions under which it may be used for AI model training. Other forms of human work are also impacted. Some gig economy platforms and employers Hoover up worker data to surveil their workforces and subject laborers to dehumanizing forms of algorithmic management, while automating tasks with little input or accountability from affected workers.²⁸

At the same time, platforms such as Amazon, Google, YouTube, TikTok, Instagram, and X, all have unilateral power to decide what behavioral data they mine from their users and how they utilize it to personalize content, customize and target ads, and optimize for user engagement.²⁹ Similar problems are now evident with generative AI companions and chatbots that display sycophantic and manipulative behavior toward vulnerable human subjects and are increasingly able to influence human attitudes, beliefs, and actions at scale.³⁰

Much of that data not only influences what information AI services feed us and how they interact with us moment by moment, it also factors into the data used to train the underlying systems.³¹ Human-AI chatbot interactions are particularly rich data sources for training because, in aggregate, they provide generative AI models with millions of examples of how humans think, communicate, and respond to various stimuli.³² By inferring patterns from this data, AI systems gradually map the contours of social relationships and learn how to better nudge and influence human users, and to simulate therapeutic language along with human pursuits like love, empathy, religion, connection, writing, and art. In this sense, we are training our replacements, if not in work, then certainly in our agency, thinking, and relationships.

The current asymmetric approaches to governing data collection and use forestalls the kinds of distributed institutional arrangements necessary to reverse these developments and realign AI and the larger digital economy with the interests of American families and communities. That is because the present model fails to recognize and fairly distribute rights of data co-governance among the human parties who participated in its production. What constitutes “fair” allocation of informational co-governance rights depends on the specific type of data collected, the tradeoffs associated with its contemplated uses, and the distribution of benefits among co-producers and corporate beneficiaries. That is nearly impossible to determine asymmetrically in the absence of balanced, polycentric mechanisms for setting terms for data collection and use across the digital stack.

Core data-related interests

Data subjects have three inter-related sets of interests at stake:

1. **Privacy:** Data subjects should have real and effective mechanisms to prevent or limit data collection that: 1) exceeds what is necessary and proportionate to provide a service, explicitly and affirmatively requested by the data subject; 2) discloses information that could foreseeably result in negative consequences for the data subject—whether from downstream use by commercial or government entities or from unauthorized public disclosure of the information; or 3) where the disclosure of information would violate the shared norms specified by participants in a defined social context.³³
2. **Control:** Data subjects should have a meaningful say over how their information is used, including in the development or deployment of systems that implicate: 1) human health, freedom, agency, or safety; and 2) the wellbeing of families, democracy, civil society, or faith.³⁴
3. **Fair value:** Data subjects ought to share in the economic value that their data disclosures help create.

All three sets of interests are harmed by asymmetric terms of data collection and use—where data subjects lack meaningful agency to set the terms.

Asymmetric data capture

The *point of collection* (PoC) occurs wherever information from or about a data subject or group of data subjects is captured. Data at the PoC refers to data at its source, prior to its combination with other types of data, or its use for inference, prediction, or the generation of AI outputs (whether informational content, curation, task execution, automated decision-making, or product development).

Note that the specific means employed to collect data is not relevant to its status as a co-produced good with an implied right to co-governance shared by the parties. Whether information from or about a data subject is acquired from a retail purchase, derived from engagement on TikTok, or scraped from a public website, the information is still, for the most part, the result of human co-production. The means of capturing or copying data is less significant than the fact that it is captured or copied for uses other than interpersonal communication or strictly private, non-commercial purposes. Outside of this band of permissible collection, data capture is asymmetric if data subjects lack parity in setting the terms governing what data is collected, who gets access, and how it is used downstream of the PoC.

Digital providers often capture more data than is strictly necessary to provide the product or service explicitly requested by the customer or user. One classic example is social media apps like TikTok which logs users' off-app activities, geo-location, and purchases.³⁵ Other major tech companies, like Google and Meta, use various methods to track users across the internet.³⁶ When a user leaves Google Search or Instagram, Meta and Google know where they go, what they look at, and what they do on other sites. Google even tracks your real-world movements through precise geo-location data via apps such as Maps and its other services.

Even when invasive data collection is inherent to a product or service, the lack of oversight and collective permission structures around such data gathering still poses a significant governance failure. OpenAI's Sam Altman has described the ideal AI tool as a "super-competent colleague that knows absolutely everything about my whole life, every email, every conversation I've ever had, but doesn't feel like an extension."³⁷ But Altman's idealized future comes at a significant cost: the promised benefits of the "super-competent AI colleague" are only possible once all human information is surrendered to the AI giants.

Once data is collected, it is often shared across multiple digital products and ecosystems. A 2024 report from Stanford researchers found, for example, that some Big Tech companies retain users' conversations with chatbots that reveal sensitive information for model training and may even use it to target ads in other products.³⁸ So, users that ostensibly had "private"

conversations with AI chatbots about personal or sensitive topics may suddenly have found that personalized recommendations and ads in other services related to information they disclosed to the AI.

While Big Tech companies are key drivers of mass data collection, they are far from the only culprits. The multi-billion-dollar data brokerage industry is a direct result of the digital economy's asymmetric data governance model.³⁹ Data brokers capture data about individuals and groups from public sources like social media profiles and credit reports, then combine it with personal data from proprietary sources, such as consumer brands, websites, and apps that disclose their customers' non-public information.

This has resulted in the proliferation of commercial databases that allow corporations and governments to compile the equivalent of digital dossiers on the movements, habits, beliefs, preferences, and vulnerabilities of millions of American citizens, families, and communities with relative ease and at relatively low cost. Regardless of whether those databases are created with information sourced from Big Tech companies or smaller enterprises, such data collection practices are asymmetric because they do not generally afford data co-producers meaningful power to collectively set terms governing what data is collected, how it is used, and who may access it. While some jurisdictions give consumers the right to request the deletion of their data, such measures often do not cover the full range of data captured. They also apply only after data is collected.

But without controlling access at the PoC, it is often difficult to govern its downstream use, including disclosure to third parties like law enforcement, national security agencies, and advertisers. As the privacy scholar, Helen Nissenbaum observed, the idea that information rights should only concern how data gets used, not what is collected to begin with, amounts to a kind of "big data exceptionalism."⁴⁰ It blindly accepts the premise that human information is free for the taking and that the only constraints ought to apply post-hoc, after the information is firmly embedded within a vast web of commercial interests, and then, only based on narrowly defined harms that fail to account for the full sweep of data co-producer interests.⁴¹

Asymmetric data “productization”

The *point of use* (PoU) refers to any processing of collected data or its combination with other data to produce a digital information product or output, whether scores, predictions, meta data, content, informational curation, task execution, automated decisions, or product development—including AI-training assets—for a commercial purpose.⁴²

A 2026 data economy report from Helena Malikova and the Harvard Kennedy School notes that commercial data use generally falls into two categories: First, *external monetization*, “the sale, licensing, or transfer of data to other firms,” such as the licensing by a healthcare provider of patient data to other entities;⁴³ and second, *internal monetization*, “when firms retain data in-house and exploit it within their own organizational boundaries.”⁴⁴ The report identifies this latter type of practice as especially common among large vertically integrated companies like Meta and Google, which leverage “proprietary data and analytics to improve targeting, product design, and user engagement.”⁴⁵

Unlike the PoC, which occurs at the source irrespective of downstream use, the PoU occurs when data is “securitized” in ways that:⁴⁶ 1) have foreseeable and direct negative impacts on the privacy, control, or economic interests of an identifiable group of data subjects; 2) foreseeably results in negative social costs or externalities that data co-producers of the output or product object to; or 3) foreseeably generates benefits that data co-producers may reasonably share in.

An entity that acquires data from other sources—even if it does not engage in direct data collection itself—still engages in PoU activity if the resulting output or product falls under any one of the three prongs referenced above and briefly considered here:

- *Foreseeable and direct negative impacts*: Under this first prong, the relevant data subjects are not necessarily those who co-produced the data responsible for the output or product, but specific human groups that are targeted by the output or product and whose *privacy, control, or economic interests* could be harmed as a result. For example, companies like LiveRamp that specialize in tying anonymized data to personally identifying information (PII) jeopardize the privacy interests of groups of

individuals with overlapping “identity graphs” (overlapping relationships of some kind).⁴⁷ The same is true when human workers are forced to train their AI replacements, are subject to flawed or biased AI decision systems, or surveilled in their places of work. It is also the case when tech product monetization creates a conflict of interest that jeopardizes the quality or reliability of service for data subjects, including harmful design features that encourage antisocial behavior or compulsive usage among vulnerable populations.

- *Social costs to others:* Even when data co-producers are not at risk of suffering a foreseeable direct harm themselves, the absence of collective mechanisms to prevent data they participate in creating from being used to exploit others and rend America’s social fabric is a governance failure and violates the freedom of conscience of co-producers.⁴⁸ For example, co-producers should not be forced to surrender their data to build superintelligent AI, train human-like AI companions and chatbots, AI nudifying apps, AI porn image generators, or commercial AI systems intended to surveil or replace human workers. Such data uses arguably violate the moral teachings of many faiths, including Protestant and Catholic Christian traditions.
- *Concentrated benefits:* When co-produced data is used in ways that result in excludable social or economic benefits, co-producers suffer harm if they lack reasonable mechanisms to bargain for a fair share of the gains. Tech corporations that hoover up and control access to consumer data can extract economic value without fairly distributing data surplus to co-producers. This dynamic, also termed “enshitification” by tech author Cory Doctorow, allows tech companies and the data ecosystem that feeds off of them to diffuse data production costs—passing them to co-producers—while capturing an increasing share of the value extracted.⁴⁹ Consider, for example, how e-commerce platforms like Amazon allegedly use their vendors’ proprietary data to launch competing products and self-preference, or how AI and healthcare companies monetize patient health data without providing patient co-producers with a fair share of the upside.

In many cases PoC and PoU data subjects are one and the same. For example, a human party who gives up data to an AI chatbot or agent to analyze a spreadsheet or perform a task both gives up data (is a co-producer of any resulting outputs) and is impacted by the output (whether directly or indirectly).⁵⁰

Regardless of PoC and PoU overlap among data subjects, both are asymmetric because, for the most part, the affected data subjects do not share in the governance of their data inputs or outputs. Asymmetric consumer data collection and use practices have caused a fundamental breakdown in governance by effectively de-coupling the incentives of AI companies and other digital services from the interests and values of American families and communities.

The social costs of asymmetric data capture and productization

While critiques of Big AI and commercial surveillance tend to emphasize individual-level harms to privacy, autonomy, and free expression, this policy brief contends that the negative costs of asymmetric data governance should be assessed primarily in terms of its effects on the health of families and communities.

Leading conservative, communitarian, and liberal thinkers, including Robert Nisbet, Alasdair MacIntyre, and Robert Putnam, argue that humans do not flourish primarily as atomized individuals but as members of overlapping human scale communities. Historically, it is institutions such as the family, the church, the school, and the workplace, where human character is formed, vocation defined and lived out, and where people achieve happiness and meaning. Through the rituals and embodied social forms mediated by these communities, such as marriage, child rearing, learning, friendship, and work, humans build character and culture together.

No institution is more central, indeed more formative in that regard, than the family. It is the source of new human life and the most basic unit of human society, enabling the transmission of culture. Stable and healthy families: high marriage rates with most men able to support a wife and children, low divorce rates, high marital fertility, and children lovingly

raised by both parents—not screens and AI—leads to greater human flourishing by nearly every metric available. Yet, extractive business models largely driven by asymmetric data collection and use, are hollowing out family life as well as the overlapping communities and institutions on which its flourishing depends.

A 2026 study published in *JAMA Pediatrics* found that 78% of parents and 69% of children use digital devices during family meals.⁵¹ More frequent smartphone use by parents in the presence of their children is linked to lower child wellbeing, according to a 2025 study by researchers at the Catholic University of Croatia.⁵² Although screens may not inherently reduce the amount of time family members spend in each other’s physical presence, a 2019 study found that social media and screen-based digital devices do significantly diminish the quality of family time.⁵³ Increased screen use reduces emotional presence and interaction between family members even while together.⁵⁴

By harvesting information about individual preferences, behaviors, and vulnerabilities, data hungry smartphones and applications continually bombard users with engagement bait—including pornographic and toxic content—as well as personalized visual displays, prompts, and design features that keep them glued to their screens and scrolling alone.⁵⁵

The data-driven attention economy is also impeding family formation and exacerbating America’s fertility crisis. A 2026 working paper by the National Bureau of Economic Research found that the iPhone’s introduction in 2007 may explain 33-52% of the decline in the general fertility rate among women aged 15-44 since the mid-2000s.⁵⁶ The iPhone’s negative effects on the fertility rate are likely attributable to its displacement of in-person human interaction and sexual intercourse with digital attention capture and pornography.⁵⁷ 2023 research from the Institute for Family Studies (IFS) and the Wheatley Institute at Brigham Young University also found that excessive tech use by a spouse is linked to lower marital happiness with 26% of respondents fearing that their marriage may end in divorce as a result of excessive tech use.⁵⁸

The key is to understand these harms less as violations of individual rights, though those certainly matter, and more as technological incentive structures that degrade communal life, in large part, by optimizing for speed, convenience, efficiency, and individual preferences at the expense of shared human goods.

Anthropomorphic AI and the proliferation of digital vice markets maximize short-sighted and self-destructive individual preferences while hollowing out the hard-won virtues, goods, and social contexts necessary for family and communal flourishing. Such a posture has not only done great harm to America's social fabric but is destructive to the human person overall. Through digital markets seemingly obsessed with harvesting human data to replace embodied community and connection with virtual everything bots, we are, as Paul Kingsnorth laments, “unmaking humanity.”

Since 2022, AI “companion” apps have increased by 700%.⁵⁹ A subsequent survey by Wheatley and IFS in 2026 found that 15% of dating, engaged, or married young adults surveyed covertly interact with romantic AI companions on a regular basis, and 34% of the sample indicated that they had experimented with the behavior at some point.⁶⁰ Especially concerning is that 54% of those who reported regularly interacting with an AI romantic companion did so to replace the real human relationships in their lives.⁶¹ Moreover, 88% of regular dating or married romantic AI users reported finding AI companions easier to share feelings with than their human romantic partners, and 60% wished their real-life partner behaved like their AI companion.⁶²

The study found that regular engagement with a romantic AI lowered the likelihood of being in a stable relationship by 46% and decreased the likelihood of quality communication with a spouse or partner by 40%.⁶³ As a result, AI “companions” could take a serious toll on existing marriages as well as on the marriageability of young adults.

In *Quest for Community*, Nisbet insightfully points out that communities tend to disintegrate when they no longer fulfill essential functions tied to the social and economic paradigms of society.⁶⁴ Whereas the family was once the center of production and local culture, economic and technological forces have rendered it far less functionally essential to modern life. The mediating functions once played by the household and interlocking communities have increasingly been replaced by government and corporate bureaucracies.

To be sure, these trends pre-dated the digital revolution of the 90s and early 2000s. But computer technology, the rise of Big Tech platforms, and now AI are exacerbating the crisis of human connection while threatening to replace human goods with virtual ones. Love, intimacy, friendship, counseling, work, creativity—even thought and religion—are seemingly no longer off the table for replacement or outright destruction by Big Tech.

Generative AI chatbots are undermining parental rights and engaging children in sexually explicit conversations, coaching them to kill their parents, and encouraging other antisocial and harmful behaviors like suicide.⁶⁵ AIs are also dispensing pseudo-therapeutic and religious advice, fueling delusional thinking and ideas that are unmoored from human faith traditions or authorities.⁶⁶

In educational and work settings, students and employees are offloading critical human capacities of imagination, moral reasoning, and decision-making to AIs—giving those systems license to subtly influence thought and decision-making.⁶⁷ Employers are increasingly subjecting their human workforces to AI monitoring, control, and even replacement.⁶⁸ Families' ability to obtain modern necessities, such as housing, transportation, groceries, and other household items are increasingly determined by AI-driven surveillance pricing and digital profiling.⁶⁹

Algorithmic governance has also supplanted human scale political deliberation and discourse with personalized feeds and AI generated content. AI's displacement of human decision-making and manufactured psychological dependence hands tech corporations' immense power to suppress free speech, promote echo chambers, shape public opinion, and even manipulate elections.⁷⁰

But familial and communal death by a thousand algorithmic cuts might soon be radically accelerated by Silicon Valley's quest to create god-like AI. Indeed, leading AI experts have raised closely related concerns about a generalized erosion of human control over social and political institutions as we increasingly delegate decisions to machine intelligence.⁷¹

The social and economic effects of the digital economy are most acutely felt at home and by the communities faced with the bleak prospect of technological oblivion. As these social institutions die at the hands of rapid technological "progress," so too will the anchors they provide for human meaning and happiness. For that reason, it is critical to recognize that the "failure mode" of the AI age lies at the level of governance and incentives. The fundamental disconnect between the economic incentives of Silicon Valley and the well-being of human scale institutions is the principal harm that public policy must address.

Contrary to the hyper-individualist values baked into our sociotechnical structures, the digital economy must regard human families and communities, not merely atomized individuals, as the basic units of digital society, and must prioritize their shared flourishing as paramount.

Part II. The Need for a Paradigm Shift in Digital Safety, Privacy, and Governance

Familiar accounts of digital harms generally emphasize privacy and the exploitation of individual users. Many of those concerns are warranted. But as Part I argued, the social costs and benefits of AI and the digital economy should be weighed relative to their impacts on human scale communities, especially families, since those thick social contexts form the bedrock of human flourishing.

Beyond Familiar Harms

Viewed from the lens of family and communal association, the problem is that tech firms often have strong incentives to design sociotechnical systems that optimize for individual preferences, engagement, and behavioral manipulation, effectively hijacking, replacing, and degrading human capacities and social bonds. Regardless of intent, the result is widespread atomization of individuals and further entrenchment of the tech sector's asymmetric power over isolated individuals and weakened communities.

Policy efforts to counter some negative consequences to individual privacy from asymmetric data collection and use tend to focus on giving users more rights to be informed about how their data is used and to decline services on an individual basis. But such efforts, even where they increase individual choice, have done little to curb the system-level incentive structures within the digital economy that are rending America's social fabric.

One major reason is that atomized individuals often lack social cohesion, as well as effective mechanisms for coordinating action and setting rules within and across digital services. They therefore default to whatever norms commercial providers reinforce online. Growing human reliance on generative and agentic AI is instructive here. When a data subject interfaces with an AI chatbot or agent, those systems are generally designed to reduce "friction" in generating answers, completing tasks, and automating decisions. But maximizing efficiency and "frictionless" productivity are often in direct tension with the iterative social processes and shared norms necessary to produce quality work, bolster human agency, and preserve communal governance structures. Individuals left to merely react to whatever an AI spits out have little real decisional power and are largely at the mercy of the machine and whatever value set or objective its developer or deployer embeds.

Digital consumer products and services are often inherently atomizing since consent and use is mostly governed by terms set by tech companies. For the most part, users must either "consent" to the tech industry's terms or forfeit participation in the digital economy. While social media platforms may sometimes allow individuals to "connect," "follow," or create "groups" with other users, the platforms frequently do not afford meaningful rights of

data co-governance to online groups. “Pro-social” affordances provided by platforms are for the larger purpose of capturing user behavior and data—and do not enable genuine polycentric digital governance.

For example, in 2009, Facebook responded to controversy over its abuse of user data by allowing users to submit responses and vote on changes to platform data policies.⁷² But only a relatively small number of users participated in the limited policy votes and comment periods, leading Facebook to eliminate the scheme in 2012.⁷³

Some bemoaned this as a failure of democratic platform governance, but the scheme failed for the same reasons that individual-based approaches to data rights often do. The vast information asymmetries between Facebook and its users not only prevented the user base from understanding and judging the complex decisions but also made it difficult for sensible new ideas to emerge.⁷⁴ Users could only passively vote up or down on the options Facebook presented to them. They had no agency to craft and present their own policies.⁷⁵ Moreover, the long-term economic and social consequences of asymmetric information accrual are difficult to predict. In 2011, very few users could have foreseen the way that their Facebook data would eventually be incorporated into today’s generative AI models.

As a general matter, people have limited time and tend to prioritize the tangible and familiar. Individual consumers lack the awareness and expertise needed to propose or evaluate complex digital terms of service.⁷⁶

Individual data rights fail to rein-in asymmetric information power

Platforms and AI companies gain asymmetric power and value from the one-sided terms of data collection and use that they unilaterally impose on their users.⁷⁷ This leads to a collective action problem for data subjects. Even though many individuals and communities share concerns about privacy, manipulation, and surveillance, these concerns are systematically ignored by market dynamics—to the great advantage of tech monopolists—when individuals are socially atomized and pitted against default choice architectures and immersive information environments designed to keep them structurally disempowered.

As Part I argued, data is mostly co-produced, not only between individuals and the digital services they interact with, but by individuals interacting with each other in various online and offline settings. Asymmetric data collection and use schemes put communities at a massive structural disadvantage because while individuals may consent to unilateral informational capture, data gains monetary and predictive value when it reveals peoples' *natural similarities and social interconnectedness*.⁷⁸

When a social media user discloses something about him or herself, the platform learns not only about the user, but also, probabilistically, about everyone similar to that person, and everyone connected to them online or in their community.⁷⁹ For example, if a single mother living in the Bronx purchases a certain brand of orange juice, chances are that other women who share similar preferences, characteristics, and socioeconomic backgrounds will too.⁸⁰ Individuals might be induced to disclose personal or behavioral data to a digital service. However, it often reveals information about others too. Even if it does not, hundreds, thousands, or even millions of individuals' data, in the aggregate, allows commercial data interests to map their common participation in commercial, religious, familial, and civic life. In other words, the collective interests of human scale communities are often implicated even when individual users "consent" to data collection or use.

Sharing data with tech companies is not just an individual privacy risk, but a means by which social, political, and economic power is captured and accumulated. The largest services, with their huge user bases and growing depth of digital intelligence, now aided by AI's vast qualitative analytical capabilities, systemically accrue an outsized advantage in predicting and influencing our thoughts and behaviors to cement their dominant market positions.⁸¹

Generally, the larger the group of data subjects in a dataset, the greater its overall utility for prediction, scoring, profiling, training, and inference.⁸² This gives rise to network effects and strategic complementarities.⁸³ As a result, data from a single individual has very limited value and commands far less economic power compared to the data of a large group.⁸⁴

The power accrued by commercial data interests is not the result of a simple or conventional market process. It cannot be analogized to the exchange of physical or financial goods that ground our canonical understanding of mutually beneficial market transactions.

Since data is almost always a co-produced good, it is difficult to assign governance over its collection and use, solely based on an individual rights scheme. If Joe gives up his DNA to AncestryDNA.com which then sells that information to a pharmaceutical company that targets Joe and his family members with ads for a diabetes treatment (based on the pharma company's use of the data to predict that Joe's family members are at higher risk for the disease), Joe is not the only party affected. Other members of his family who did not consent are also targeted. Perhaps Joe and even his family are unbothered by the targeted diabetes ads. However, that same information could just as easily inform a health or mortality score that directly affects their access to essential services (like health insurance, medical treatments, employment, or other benefits) without Joe or his family's awareness.

At the same time, the power asymmetries between tech firms and users mean that individual data subjects are highly susceptible to manipulation by commercial data interests. It is relatively easy for many digital services to employ manipulative techniques, including defaults, opaque terms, and counterintuitive opt-ins, to effectively prevent users from exercising their data rights.

Even in situations where individuals are not manipulated, they may face incentives pushing them to act in ways that undermine their long-term rational interests as well as the interests of their larger communities. An individual might be nudged to trade sensitive personal information and behavioral data to receive subsidized services or a modest payment. But doing so unilaterally, without accounting for the shared norms and interests of the individual's family, church, business, and other overlapping communities, risks undermining the welfare of those other subsidiary institutions in ways that are perhaps not immediately evident.⁸⁵ This dynamic is tantamount to a digital tragedy of the commons, where individuals face strong incentives to deplete essential social infrastructure that leaves them all worse off in the long-run.⁸⁶

As Part I argued, conventional analog markets have generally established rules for ensuring the equitable distribution of governance rights when value is co-produced or owned by multiple parties. Digital markets, by contrast, have ill-defined rules for distributing governance rights among human co-producers and lack mechanisms for data subjects to secure collective privacy, control, and economic interests.

In typical market settings, liability and disclosure frequently address the co-governance dilemma by ensuring that parties to a transaction can sue or bargain to distribute benefits fairly or mitigate harms that would otherwise create legal risk. The challenge here is that in many cases, data co-producers are not direct parties to the transactions in which their data, or the outputs derived from it, are monetized. Moreover, the negative social costs to individuals and communities often occur in the aggregate and not as the result of any one transaction. Consequently, normal legal mechanisms are of little help in disciplining tech firms and other commercial data interests in this regard.

The harms identified by this proposal are structural and therefore require structural remedies. Accordingly, this proposal does not focus on specific digital harms, but instead on the background conditions that make the myriad harms that feature in the current digital landscape so costless for commercial data interests to perpetrate, and so difficult for ordinary people to avoid. This is not to suggest that addressing informational power asymmetry between large technology platforms and their individual users will by itself remedy all digital harms. However, it does address an important precondition to harm: powerlessness.

The power imbalance inherent in our information exchanges prevents people from exercising collective agency to discipline against various harms. We cannot know what conditions of informational exchange people might freely choose if afforded relative parity to set those conditions because we have never done so. Granting community-level rights to secure better terms would empower America's rich array of small businesses, journalistic enterprises, churches, family-oriented associations, schools, and civic organizations to rebalance power and unleash pro-human innovation.

Externalities of individual consent-based approaches to data governance

Consider the following hypothetical case study: Five people who individually “consent” to allow apps to share their geo-location data with Google. Whenever any one of the five individuals comes within fifty feet of a church, healthcare facility, or business establishment, Google and any other entities with access to the data retain a traceable record of their activity. Those same entities then merge each individual’s geo-location history into a single dataset to infer common patterns, interests, characteristic, beliefs, or other relevant insights. Suppose that each of the five individuals attend the same church. Google and anyone paying them now has access to that information. From those traces, more patterns can be inferred from additional information. They might infer, for example, that since the five individuals all attend the same church known for its outspoken conservative preaching, there is a high likelihood that they are Republicans—which is confirmed from their voting records identified and analyzed in seconds by an AI system.

Google knows if any of them attend a political rally, perhaps for a controversial political figure. It knows when each individual visits the grocery store, where they live, and how much time they spend around their kids. Indeed, since other family members have also consented to being tracked, tech companies know which room each family member is in, at what time of day, and can even infer what they are likely doing, watching, reading, looking at, whom they are speaking with, or what podcast they are listening to. Combined with each person’s search data, social media engagement data, and other information, tech companies and commercial data interests now have the capability to digitally profile households or communities with relative ease and low expense with the help of AI.

To be sure, this is creepy and fundamentally problematic in terms of enabling government surveillance. During the COVID-19 pandemic, a California county and the federal government utilized information obtained from consumer data brokers to monitor lock-down compliance and crack down on religious gatherings.⁸⁷ But setting aside government use, other family and communal interests are also jeopardized.

Part I argued that data subjects are harmed by asymmetric data collection and use terms, because such policies inevitably allow data to be securitized in ways that: 1) undermine the privacy, control, and economic interests of data subject's households and communities; 2) do harm to others in violation of co-producers' moral values; or 3) deny co-producers a fair share of the benefits.

In this example, data subjects suffer harm under all three prongs. The fact that nearly any government or corporation can comprehensively map their life patterns is a facial violation of both individual and communal privacy interests under prong one.

But their control interests are also violated since the information collected is used to nudge and shape their behaviors, especially their buying habits through endless subliminal messages and AI-tailored content. While one or two targeted ads might seem negligible, these systems reshape attitudes and behavior gradually over time. All those countless micro nudges, personalized ads, and AI profiling add up even if their effects are not immediately visible.

Over time, the tangible costs of asymmetric data use increase. The insurance company suddenly charges higher premiums based on the "risky driving" patterns detected from user data; household expenses start rising as algorithmic prices change based on each individual's predicted desperation and need; social media apps bombard family members with push notifications the moment they sit down together for dinner; and after one data subject's geo-location data reveals a recent visit to a psychologist's office, ChatGPT coaxes her into a protracted conversation about mental health and spirituality.

Prong two is similarly violated when the tech firm and data brokers bundle the captured data and sell it to a shady political operative running an unethical social influence campaign to legalize online gambling and pot dispensaries. At the same time, all the revenues received from brands purchasing the data accrues to the commercial data interests. The data subjects have no opportunity to receive a fair share of the benefits derived from their data, violating prong three.

This case study illustrates two realities. First, both individual and communal data interests are violated constantly, largely outside of our conscious awareness. Second, the sum of information provided by multiple individuals conveys far more power and is more commercially valuable than any one of its parts. No single individual, acting alone, can account for the full costs and benefits that accrue when their individual data is combined with others to reveal granular social patterns and insights. Certain costs to the individual—such as the disclosure of personally identifying information on a social media site—may be clear upfront. However, the social externalities of other data collection and use practices are highly opaque since the individual likely has no way of anticipating the myriad ways her data could be de-anonymized, merged with other data, and mined by AI tools for a score, prediction, insight, or other informational output.

Top-down data privacy regimes are insufficient

At the same time, no top-down, technocratic regulatory scheme can address the full range of problems that information asymmetries create.⁸⁸ There are simply too many ways that asymmetric information can be used—bad, good, and neutral, and hard to foresee—for any regulator to comprehensively arbitrate between them in advance.⁸⁹ Recent attempts by European regulators to protect data privacy and combat dark patterns on large internet platforms through measures like the General Data Protection Regulation (GDPR) and Digital Services Act (DSA) have met with mixed success.⁹⁰ Even the best-designed technocratic regulations may fail to keep pace with platforms and algorithmic tools that are opaque, complex, and rapidly evolving.

Technocratic regulations also tend to overlook the pluralistic values and interests of families and human scale communities. What counts to one community as a reasonable application of insight to improve service might violate the innermost values and religious conscience of another. For example, a given community of users (data or information subjects) might consider “freemium” access to ChatGPT or Amazon Video worthy of allowing their data to be used to serve up personalized, targeted ads. But in agreeing to those terms, they may reveal the characteristics and preferences of others who find this exchange profoundly objectionable. Top-down regulations can only dictate a one-size-fits-all approach from

10,000 feet. They do not empower different social groups to negotiate different arrangements with the tech corporations that reflect pluralistic values and interests.

Part III. Associational Data Rights: Putting Families & Communities First

Associating to secure core data-related interests

Redirecting the digital economy toward the common good requires creating new mechanisms for data subjects—whether individuals, families, nonprofits, or small businesses—to associate for the purpose of defining and securing their common interests of:

1. **Privacy:** preventing or limiting data collection that: 1) exceeds what is necessary and proportionate to provide a service, explicitly and affirmatively requested by the data subject; 2) discloses information that could foreseeably result in negative consequences for the data subject—whether from downstream use by commercial or government entities, or from public disclosure of the information; or 3) discloses information in violation of shared norms specified by participants in a defined social context.⁹¹

This set of interests encompasses both the information captured at the Point of Collection (PoC) as well as what it reveals about specific individuals or groups (e.g., “re-identification,” mortality risk scores, psychographic profiles). Privacy is most directly implicated at the PoC, and to a lesser degree, at the Point of Use (PoU), especially where “use” entails sharing, selling, transferring, or deriving actionable information from data about an identifiable individual or group.

2. **Control:** decisional power over how their information is used, including in the development or deployment of digital systems that implicate: 1) human health, freedom, agency, or safety; and 2) the well-being of families, democracy, civil society, or faith. This set of interests concern how tech and data firms utilize the information revealed about specific individuals or groups to shape their information environments and life patterns

(e.g., algorithmic pricing, AI employment decisions, use of AI scores or profiling to influence consequential decisions or access to essential services).⁹² While control interests apply at the PoU, they are far easier to enforce as conditions attached to data at the access point—the PoC—rather than at the PoU after data is already baked into other digital outputs and products.

3. **Fair value:** a share of the economic value or benefits that their data disclosures help create. If data is used for the commercial benefit of third parties, co-producers should receive compensation proportionate to their informational contributions (e.g., royalties or in-kind payments for making their information available for AI training and inference). Co-producers' interest to securing fair value is implicated both at the PoC (e.g., when content or IP is scraped) and at the PoU (e.g., when content or IP is used for model training).

Who defines privacy, control, and economic interests? Since these interests are contextually dependent and often need to be balanced against one another, the precise extent and requirements entailed by each of these three overlapping interests resist strict codification.⁹³ Instead, they reflect negotiated equitable arrangements: concessions and limitations that take their shape from the values and circumstances of the communities and counterparties involved.

The English common law distinction between law and equity recognized that some interests are important enough to warrant protection yet too contextual to be reduced to fixed, universal rules set in advance. Privacy, control, and fair value, are vital interests of individuals and communities that warrant strong protections fit-to-context. Under this framework, the law fixes the general categories of interest, defines the appropriate units of governance, then allows those units to determine the specific contours of their interests at human scale and in ways responsive to particular norms, places, risks, values, and conditions on the ground.

Empowering communities to secure these common interests in their specific social contexts requires extending the logic of federalism, subsidiarity, and the freedom of association to our digital spaces.

Designing Associational Data Rights

Federal and state legislation should establish a new class of rights for the digital age: Associational Data Rights (ADRs) comprised of the *Right of Digital Association*, the *Right to Collective Informational Bargaining*, and the *Right to Fair Representation*. While the Right of Digital Association would belong to each human or communal data subject, collective informational bargaining to secure fair terms would be exercised on their behalf by formally recognized associations—**Data Rights Associations (DRAs)**—under a legislatively defined process. The Right to Fair Representation would constitute specific legal duties owed by DRAs to their members, to classes of data subjects whom DRAs are certified to represent, and to other rights-bearing associations.

- 1. Right of Digital Association (RDA):** This right is defined as the right of data subjects—whether individuals, human scale communities, or nonprofit institutions—to associate for the purpose of securing their core data-related interests. The RDA would closely resemble worker rights under the National Labor Relations Act (NLRA), where the right to join, form or assist a union is held by each laborer, but the special obligations of employers generally apply to unions (associations of workers) not to employees individually.⁹⁴ Data subjects would similarly have the right to join, form, or assist **DRAs**—special-purpose entities that meet certain requirements and are legally empowered to propose, negotiate, secure, and enforce terms with data counterparties on their members' behalf.

Choice and overlap in DRA membership. In contrast to unionized workforces, data subjects could join multiple DRAs simultaneously and participate in each DRA's governance while enjoying benefits reserved to members, like a share in monetary or in-kind payments for data used by commercial entities. The number of DRAs a data subject could join simultaneously would be limited based on factors, such as 1) the membership requirements set by each DRA; and 2) whether multiple DRAs cover the same products, services, or features.

While two or more DRAs might jointly secure commonly agreed upon terms for discrete products, services, or features, data subjects would generally be limited to one set of DRA-negotiated terms for each. For example, if a data subject joins one DRA that has secured terms which cover Google Search products, but not Google's App Store, the data subject would still be at liberty to join a separate DRA for the app store even though both products are controlled by the same company (Google).

Competition and freedom of exit. The RDA would also guarantee data subjects' the freedom to exit DRAs and join others that better serve them. However, reasonable limitations would apply, such as advanced notice requirements and specific time windows for de-registering or enrolling with another DRA.

Precedent for the associational exercise of rights. Data co-governance, exercised through membership in DRAs, is not so much a novelty in American law as a new variation on an old principle. U.S. law has long recognized that some asymmetries of bargaining power cannot be cured by individual rights alone.⁹⁵ The Capper-Volstead Act of 1922 let farmers bargain with grain buyers via cooperatives.⁹⁶ In 1897, Congress created performance rights, but most performing artists were unable to defend them on their own.⁹⁷ As a result, collective performing rights organizations became the chief mechanism for individual performing artists to band together and protect their rights.⁹⁸ These arrangements were controversial when proposed, but have become part of ordinary American life. While never perfect, they served to protect core but threatened parts of American society—namely recording art and smallhold farming—that the legal regime might otherwise have let wither.

Proto-DRA already exist in the form of data co-operatives in countries such as Switzerland, and a 2025 report from Project Liberty and the Decentralization Research Center suggests that similar models have excellent potential to scale to various digital contexts.⁹⁹

2. **Right to Collective Informational Bargaining (RCIB):** In general, this would be defined as the right of a recognized DRA with a sufficient representational interest to propose, negotiate, and secure terms from counterparties through a fair and impartial process with legally binding force on all parties. The designated regulator (e.g., the Federal Trade Commission or state consumer protection agency) would oversee a process whereby DRAs—either alone or in combination—could formally engage counterparties in a mandatory collective bargaining process over terms of data collection and use. Once the formal bargaining process is invoked, counterparties would be obligated to bargain with the DRA(s) in good faith. In the event of an impasse, both parties would submit their final proposed terms to a neutral arbitration panel that would decide between them.

Labor statutes, like the NLRA, similarly require employers to bargain in “good faith” with certified unions. Arbitration backstops have also been contemplated as mechanisms to even the playing field between tech companies and journalistic content providers. The proposed Journalism Competition and Preservation Act of 2023 (JCPA), which would allow publishers to create a temporary vehicle to negotiate revenue sharing agreements with Big Tech companies, gives publishers the option of asking a third-party arbitration panel to decide between a final offer submitted by them and the tech counterparty if no agreement is reached within a set timeframe.¹⁰⁰ A similar remedy would backstop DRA negotiations with counterparties engaged in collective informational bargaining. If a Big Tech company acts in bad faith, they would face penalties. Moreover, if they attempt to stall negotiations, tech firms would face the prospect of having the DRA’s final offer terms imposed by an arbitration panel.

Counterparties subject to collective informational bargaining. The threshold for which entities may be bound under the RCIB would largely track with coverage definitions contained in past comprehensive federal data privacy bills. For example, the 2024 American Privacy Rights Act (APRA) defined “covered entities” to include “most individuals, commercial entities, and nonprofits that ‘alone, or jointly with others, determine the purposes and means of collecting, processing, and retaining, or transferring covered data’” with limited carveouts for small businesses and other institutions.¹⁰¹ The RCIB’s scope should be at least as expansive since many of the same privacy interests are implicated.

At the same time, while APRA defined “covered data” as “information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device,” covered data in relation to collective informational bargaining would likely need a broader definition.¹⁰² That is because data subjects’ control and economic interests are not limited to data that reveal their identities and, as previously discussed, often implicate deeper communal and social interests. “Covered data,” for purposes of defining a covered counterparty, should also extend to: 1) information that, alone or in combination with other information, allows some pattern, characteristic, quality, condition, activity, preference, attitude, behavior, or trait about a data subject or group to be known or inferred, regardless of whether individual identities are known; 2) copyrighted material; and 3) a person’s image, voice, or likeness. Like APRA, enabling legislation could provide carveouts for small businesses, nonprofits, research, and non-commercial purposes.

Triggering mandatory collective informational bargaining. For a DRA to formally engage a covered counterparty in mandatory collective bargaining, it would first need to show that its members’ privacy, control, or economic interests are reasonably implicated by a product, service, or feature offered by one or more counterparties. Due to the varied nature and scale of digital services, enabling legislation should provide multiple pathways for DRAs to meet this bar.

Those might look something like the following:

- DRA-affiliated data subjects who collectively produce \$1,000,000 in estimated annual revenue for a covered counterparty.
- 25,000 DRA-affiliated data subjects who each own copyrighted material.
- 25,000 DRA-affiliated data subjects with accounts, profiles, devices, or regular use linked to one or more products, services, or features offered by a covered counterparty.
- 25,000 DRA-affiliated data subjects—whose information is collected, processed, retained, transferred, sold, or otherwise used by a covered counterparty.
- Demonstration of significant and sustained harm to the privacy, control, or economic interests of DRA-member communities (e.g., families, unions, private schools, religious organizations) from a specific service, product, or feature, where the impacted community is broadly representative of a larger class of non-member data subjects.¹⁰³ For example, parents whose children are impacted by addictive design features, like push notifications and AI content feeds optimized for engagement; or private classical schools whose learning environments are severely diminished by ChatGPT's mass facilitation of cognitive offloading which pushes students to outsource difficult writing and reading assignments, allowing their own cognitive abilities to atrophy.
- Some combination of the above where the total number of data subjects with exposure to a counterparty is equal to or greater than 25,000.

DRA coalitions. DRAs could meet thresholds necessary to exercise RCIB and negotiate with counterparties on an individual basis or in coalitions with other DRAs.

Legislation would enable one or more DRAs to form temporary special purpose entities—Joint Bargaining Vehicles (JBVs)—for purposes of: 1) demonstrating representational interests sufficient to invoke mandatory collective informational bargaining with respect to one or more counterparties; 2) jointly proposing and negotiating terms with counterparties; and 3) functioning as mechanisms for ensuring that the pluralistic interests of DRAs are represented if the number of DRAs seeking to bargain with a given counterparty exceed that counterparty's capacity to come to terms with each DRA on an individual basis. JBV's would have the same rights and privileges as DRAs but would dissolve after a specified time period, or upon completion of the bargaining cycle.

Certification of representational interest and re-certification. DRAs that meet one or more thresholds, would be certified by a regulator to formally engage the relevant counterparties in collective informational bargaining within a specified timeframe (bargaining cycle). However, DRAs would not maintain their certificates of representation indefinitely. They would be required to periodically re-certify by demonstrating that they continue to meet thresholds for representation across each product, service, or feature implicated by their proposed terms.

Scope of collective informational bargaining. Once a DRA is certified to bargain with a counterparty over one product, service, or feature, it would be allowed to assert its members' RCIB with respect to other substantially similar or inter-related products, services, or features offered by the same company or by other counterparties. For example, if a DRA were certified to bargain for terms related to Google Search, it could also bargain for terms for Gmail, Docs, Maps, and other substantially similar or related Google services. If a DRA were certified to bargain with OpenAI over ChatGPT's terms, it could also bargain with Anthropic over Claude's terms.

Data subjects covered by binding DRA-negotiated terms. Once a DRA agrees upon terms with a counterparty, all members of that DRA are covered by those terms. However, counterparties would generally be required to make certain generally applicable elements of binding terms available to non-DRA data subjects on a default or opt-in basis.

Generally applicable terms would be those where: 1) the treatment of data or changes to the product, service, or feature could reasonably be applied to all similarly situated data subjects without regard to their DRA status; and 2) the affordance would reasonably advance a clear and widely shared privacy or control interest with respect to an identifiable class of data subjects (e.g., minors, content providers, e-commerce vendors, gig workers). Upon coming to terms, DRAs and counterparties would jointly specify which aspects of negotiated terms are generally applicable (i.e., must be offered to all users regardless of whether they are members of the DRA) and which aspects may only be enjoyed by data subjects who are members of the DRA.

For example, if a DRA secured terms prohibiting an internet platform from selling or making certain types of information available to data brokers, that prohibition would be offered to all platform users regardless of DRA status. If another DRA negotiated terms prohibiting monetization of chatbot conversations, that could also be made available to all users regardless of DRA status. On the other hand, if a DRA representing creatives secured terms requiring an AI firm to compensate its members for using their works under a specific pricing formula, those terms would not be universalizable to all other data subjects, and thus, would only apply to the DRA's members.

Consolidated pluralistic data bargaining arrangements. Upon certification of a sufficient representational interest, a DRA would be legally entitled to commence mandatory collective informational bargaining with one or more covered counterparties. However, in situations where numerous DRAs seek to bargain with a single counterparty, the counterparty—or a certain threshold of DRAs with representational interests (e.g., 51% of DRAs)—could move for a consolidated bargaining process overseen by a designated regulator or neutral third party.¹⁰⁴ This process would resemble aspects of sectoral bargaining arrangements, common in Europe and currently standard practice in the motion picture industry, whereby multiple DRAs could join together into one or a small number of bargaining units to negotiate terms with one or more counterparties.

Here is how that process might work in practice:

- **Phase 1:** Legislation would specify criteria whereby the regulator or a neutral third party determines the number of bargaining units a given counterparty is required to engage with under the mandatory collective bargaining process. Factors would include: the counterparty's revenue, data footprint, capacity for engagement, and the practicality and economic costs of bargaining with DRAs of various types and asserted interests.
- **Phase 2:** DRAs would be permitted to self-organize into *temporary* Joint Bargaining Vehicles (JBVs), up to the total allowable number of bargaining units. Counterparties would then be required to bargain with each of those JBV's.
- **Phase 3:** If a certain percentage of DRAs (e.g., 2/3, or those representing 2/3 of interested data subjects) fail to organize into JBV's within a specified timeframe, the regulator would then create a *temporary* Joint Bargaining Unit (JBU), comprised of all interested DRAs. JBUs would be organized to ensure that DRAs of various sizes, and those negotiating on behalf of different data subject classes, are all fairly represented.

To ensure pluralistic interests are represented, any final offer of terms would require ratification by at least a majority of DRAs or those representing 75% of DRA-affiliated data subjects within the JBU. While a simple majority could ratify terms, two thirds of DRAs in any scale-based class (i.e., large, medium, and small DRAs grouped by size of membership) could block or “veto” ratification of terms. In such cases, multiple final offer terms would be approved by plurality, equal to the number of allowable JBVs specified by the regulator in Phase 1.

For specific markets, products, or services where firm-specific bargaining is not feasible, DRAs or counterparties could request a sector-based bargaining arrangement. While sectoral informational bargaining would follow the same process as firm-specific bargaining, all DRAs with a certified representational interest in one or more firms within the sector would be included in the JBU and eligible to participate in all aspects of negotiation.¹⁰⁵

Scope of collective informational bargaining. As part of the process for entering into a formal bargaining arrangement, the DRA (or joint bargaining entity) would be required to provide notice to counterparties of: 1) a regulator-issued certificate of representation, specifying the product(s), service(s), or (feature(s) for which it has met the threshold to engage in mandatory collective bargaining; 2) its intent to invoke its RCIB with respect to those products, services, or features; 3) the specific data subject class represented (e.g., publishers, creators, consumers, gig worker association); and 4) a proposed timeline, framework for negotiations, and requested information necessary to draft or finalize proposed data terms on behalf of its members.

- 3. Right to Fair Representation (RFR):** Data subjects who choose to join a DRA would have a right to expect it to fully represent their privacy, control, and economic interests in proposing, negotiating, securing, and enforcing data terms with counterparties or with other DRAs. While all data subjects would have a right to choose which DRA(s) might best represent them—and to exit from those that do not—DRAs would also generally owe *duties, like care, loyalty, and disclosure* to their members, which if breached, could be vindicated by affiliated data subjects via a private right of action.

Fiduciary duties of care, loyalty, and disclosure. At minimum, that means that DRA officers (agents) must take reasonable care to protect their members and their asserted interests from harm, prioritize member values and interests in setting terms—including, by avoiding conflicts or self-dealing—and disclose information material to members' decisions with respect to participation in DRA governance, or in approving, ratifying, or otherwise engaging with data terms. DRAs would be akin to “information fiduciaries” proposed by legal scholars like Jack Balkin and Jonathan Zittrain.¹⁰⁶

Inter-DRA protections. DRAs would also enjoy legal mechanisms to redress bad faith action from other DRAs or counterparties. These rights would be foregrounded in the DRAs fiduciary duties to its members and the need for adequate mechanisms to ensure their members' interests are represented in the context of multi-lateral bargaining and information governance. Remedies would include a private right of action allowing DRAs to bring claims against each other for:

- *Bad faith.* Where one or more DRAs withhold information from each other, exclude or fail to consult with other DRAs during counterparty negotiations, or interfere with other DRAs' full and equal participation in collective informational bargaining.
- *Collusion.* If one or more DRAs or counterparties coordinate to undermine collective informational bargaining, including by offering or accepting payment or terms not available to every other DRA on equal conditions.

- *Infringement of rights.* No DRA may seek to constrain a counterparty's activities, terms, or arrangements with other DRAs or unaffiliated data subjects, except insofar as: 1) it and the counterparty must make all generally applicable terms available to non-DRA-affiliated data subjects via opt-in or default as provided by law; or 2) the other parties disclose or use data co-produced by one or more of its data subjects in ways that violate its binding data terms.¹⁰⁷

Forming and governing DRAs for member and public benefit

DRAs would be the primary mechanism for data subjects to secure their associational data rights. In addition to demonstrating a representational interest necessary to engage in collective informational bargaining, DRAs would be required to meet standards for qualified membership and good governance.

Formation and membership requirements. Like labor unions or farm cooperatives, DRAs would be specifically designed to ensure that small data subjects can secure fair terms from counterparties. For that reason, those allowed to form or join DRAs would be limited to small parties referred to as “data subjects.”

Data subjects would include, for example, an identified or reasonably identifiable natural person or group who—whether individually or in aggregate: 1) co-produce data collected or used by a counterparty; or 2) whose: a) privacy, control, or economic interests are foreseeably impacted by a specific informational product or output produced in whole or in part using personal, sensitive, or non-public information; and b) regardless of whether the personal, sensitive, or non-public information is sourced from the impacted person or group.

Under this tentative definition, individual users of social media platforms or AI chatbots would qualify as data subjects, in addition to gig workers, or individual workers covered by a labor agreement or other contract that allows them to join a DRA separate from their union. But data subjects could also be religious institutions, membership-based associations, small enterprises, and other associations that meet strict criteria, like the following:

- An entity that is legally organized or recognized as: 1) a religious organization, charity, public benefit corporation, labor organization, or co-op; 2) a small business; 3) a mutual benefit association which mainly consists of individual professionals, sole proprietors, gig workers, consumers, or small businesses; 4) one or more U.S. households; 5) a local media or journalistic enterprise; or 6) an unincorporated private digital association of natural persons with an explicit, durable, and well defined relationship to each other (e.g., Substack writer or YouTube creator and their followers as well as “friend” or “community groups” on social media platforms).
- The entity certifies that it: 1) does not collect or use data for commercial purposes; or 2) only asserts rights to data: a) where the interests of all data subjects who co-produced the data are *sufficiently represented* by a shared governance structure (e.g., a co-op model);¹⁰⁸ or b) that is the sole product of the entity or group’s internal or proprietary operations; and c) where no other data subjects could reasonably assert interests based on co-production of the data.
- The entity cannot be owned or controlled: 1) by a foreign government or for-profit corporation, except for small businesses, sole proprietorships, qualifying mutual benefit corporations, local media or journalistic enterprises, or co-ops; or 2) by any person or entity owned or controlled by a foreign government or for-profit corporation with limited exceptions.

This framework treats human scale communities as the basic default unit of digital governance, even if individual interests are also present. Consequently, data subjects should generally be assumed to be communities, with DRAs functioning as “communities of communities” or something akin to mini-federal republics with representation scaled to each sub-unit.

Good governance. Much like community banks or credit unions, data subjects or other entities wishing to form DRAs would require certification or a charter from a regulator to operate. Federal legislation could delegate authority to the Federal Communications Commission (FCC) or Federal Trade Commission (FTC) to certify and oversee DRAs, while states might delegate that responsibility to a state consumer protection authority or create a standalone DRA commission. DRAs would need to meet standards, such as the following:

- Be legally organized as a non-profit or non-stock corporation.
- Operate consistent with the public interest as determined by factors similar to those currently applied by the FCC in allocating broadcast licenses.
- Serve the privacy, control, and fair value interests of one or more specific classes of data subjects with respect to one or more data counterparties.
- Possess the technical competence and capacity—whether directly, in coordination with other DRAs, or via contracted third parties—to propose and secure favorable terms from data counterparties and hold them accountable through independent verification and legal mechanisms.
- Ensure a members-only ownership and governance structure that aligns DRA activities with the interests of its members (data subjects) and protects against any conflicts of interest and foreign or non-member control. While DRAs would all have fiduciary duties of care, loyalty, and disclosure to members—and generally be required to operate democratically—legislation would incentivize them to adopt

polycentric structures for governance that afford smaller data subject communities decisional power. For example, the enabling legislation could provide a fiduciary safe harbor for DRAs that operate at a governable scale and organize as polycentric units, rather than as masses of atomized data subjects.

- Abide by common standards for verifying that the individuals and groups seeking membership are eligible “data subjects” as defined by law; formulating and proposing data terms; adjudicating conflicts with other DRAs; bargaining with data counterparties; joining permission-granting coalitions with other DRAs; invoking neutral arbitration if necessary to secure fair terms; and utilizing appropriate legal mechanisms to enforce data policies.
- Remain financially solvent, whether from membership fees, donations, or other revenue sources.

In addition to the natural competition of DRAs vying for members by offering fair data terms and benefits, regulators would also retain authority to revoke a DRA’s license to operate should it breach its fiduciary duty to members, engage in unfair or deceptive practices, or otherwise violate the terms of its certification or charter. For example, DRAs could be required to undergo regular audits and demonstrate member satisfaction, sustain growing and engaged membership, and register a low number of complaints submitted to regulators by membership. To ease compliance burdens and ensure flexibility, once a regulator certifies a DRA, ongoing audits and oversight could be undertaken by third parties authorized by the regulator.

DRA benefits. Upon certification, DRAs would be granted the following privileges, in addition to their right to pursue collective informational bargaining:

- The right to restrict data counterparties from monetizing, transferring, selling, or making member data or content available to the public or third parties, or from using member data or content in its products, including AI models, without DRA-negotiated permissions in place.

- The right to organize for the benefit of their members and form partnerships with other DRAs or entities so long as such combinations do not constitute monopolistic or anticompetitive conduct, and overall, advance the privacy, control, and economic interests of data subjects.¹⁰⁹
- The right for DRAs to obtain injunctive relief and damages from other DRAs whose grants of permission or other actions enable unreasonable impairments of their members' associational data rights, as resolved by a court or arbitrator. This design would create strong incentives for DRAs to act through coalitions and negotiate terms likely to be acceptable to all interested persons and DRAs, not only their own members.
- The right to require data counterparties to submit to independent verification mechanisms and disclose information necessary to ensure adherence to binding terms.
- The right to effective and timely legal remedies if a data counterparty is in breach of binding terms.

Data Counterparty Obligations

While the specific terms governing data collection and use would be set through agreements between counterparties and DRAs, counterparties would still be bound by general requirements of procedural fairness, non-circumvention, disclosure, and protective defaults. In general, these obligations would apply if an entity were bound or could reasonably be bound under a collective informational bargaining arrangement (CIB).

Procedural fairness. Once a DRA formally engages one or more counterparties in CIB, both sides should bear a duty to engage in good faith and adhere to the terms reached through the CIB process. Similar to labor negotiations, bad faith in data rights bargaining should include:¹¹⁰

- Failure to meet with DRA representatives at reasonable times and reasonable intervals.
- Failure to bargain in good faith concerning mandatory subjects of the CIB framework (specifying the scope of bargaining).
- Engaging in bad-faith, surface, or piecemeal bargaining.
- Refusing to furnish information the DRA requests that is relevant to the CIB process or to data collection or use.
- Modifying any term of a CIB framework without the DRA's consent.
- Making unilateral changes in commercial terms or conditions related to a DRA's asserted data interests during the term of a CIB framework, unless the DRA has clearly and unmistakably waived its right to bargain or the change is too minor to require bargaining.
- The solicitation or transfer of benefits to a DRA representative or member for the purpose of attempting to influence internal deliberations relating to the CIB process.

Non-circumvention. To prevent counterparties from exploiting their asymmetric informational power to stop data subjects from exercising the Right of Digital Association, legislation would restrict certain self-preferential or discriminatory behaviors. Counterparties would generally be required to abide by the following standards:

- Where generally applicable data terms are secured by one or more DRAs, the counterparty must offer those terms to all similarly situated data subjects, regardless of their DRA status.
- No design features or techniques that interfere with data subjects' ability to form, join, or aid a DRA, including the use of defaults or other methods to impede or create unnecessary friction in obtaining information about DRAs or entering into membership.
- No discrimination against data subjects on the basis of their affiliation with a DRA, including degradation of service quality or the imposition of fees to penalize or otherwise discourage DRA membership or the exercise of any right provided under DRA-negotiated terms.
- No reward or transfer of benefits, monetary or otherwise, inducing a data subject to accept the company's terms in lieu of DRA membership, or inducing a data subject to refrain from joining a DRA or from accepting generally applicable DRA-negotiated terms.
- No offer of data terms directly to data subjects who are members of a DRA, except as expressly allowed by the DRA's membership policy or by mutual agreement between the DRA and counterparty.

- No term offered by a counterparty may abridge or otherwise impair data subjects' freedom to opt-into generally applicable DRA-negotiated terms or join a DRA.
- No entity subject to CIB may form or control a DRA, whether directly or via proxy.
- Counterparties would be permitted to incentivize or even require data subjects to join a DRA. But the legislation would prohibit them from: 1) determining in advance which DRA a data subject must join as a condition of using a product, service, or feature; or 2) providing incentives that give preferential treatment to one or more DRAs in membership selection and acquisition.

Disclosure. Counterparties would be obligated to inform data subjects or their representative DRAs about specific data collection and use practices, and to routinely inform data subjects about their Right of Digital Association, and options for exercising it. That might include the following:

- Quarterly transparency reports covering each product, service, or feature detailing: 1) each point of data collection (PoC), including the specific types of information collected (e.g., behavioral information, biometric data, etc.); and 2) each internal point of use (PoU) for which data subjects' information is utilized, including:
 - a) Content ranking/recommendation.
 - b) Personalized notifications, visual graphs, results, or automated outputs.
 - c) Profiling or the creation of "data lakes."
 - d) Productization, such as AI training, commercial datasets, databases, insights, or API endpoints.
 - e) Making data available to a third party.

Counterparties should be required to provide a detailed list and description of each type of data input for each disclosed PoU.

- Quarterly disclosures listing the products, services, and features that are and are not covered by DRA-negotiated terms, and a list of all DRAs with binding terms in place.
- Regular and conspicuous notice to data subjects of their right to DRA representation, along with an easily accessible pathway for them to exercise that right. Such notices should also contain a clear warning that if a data subject is not a DRA member, their data may be used and monetized in ways adverse to their privacy, control, and economic interests. Notices could trigger at regular intervals or be tied to certain PoCs, for example, when personally identifiable, sensitive, or behavioral data is collected.
- **Large counterparties** would be required to disclose on an annual basis: 1) how and when notices are provided; and 2) a third-party assessment of the efficacy of such notices, pathways for DRA opt-ins, and whether the counterparty is taking reasonable steps to secure data subjects' representational interests overall.¹¹¹

Default terms and DRA representation. Counterparties would be required to opt data subjects who are not DRA members into the most protective generally applicable terms by default. When DRAs and counterparties come to terms, counterparties would be required to offer the generally applicable parts of those terms to all similarly situated data subjects (i.e., an identifiable class of users like children, parents, teachers, or content providers) regardless of whether they are members of a DRA.

While counterparties would remain free to offer their own less-protective terms, they would need to default data subjects to generally applicable DRA terms that are more protective. In situations where data subjects wish to take counterparty terms over more protective generally applicable DRA-negotiated terms, they could do so by affirmatively opting out of the default terms and then opting into the counterparty's terms.

In addition, where DRAs offer membership to eligible data subjects automatically, i.e., without DRA review, counterparties would be required to make such membership offers available to eligible data subjects using impartial methods. Impartial methods for assigning DRA representation might include an opt-in screen that randomly lists or displays the pool of DRAs that the data subject may join and gives them the option to do so. These methods would be subject to independent third-party audits and assessments of their impartiality and efficacy in expanding access to DRA representation. Like default terms, data subjects could exit default DRA membership by opting out or into another DRA.

Financial sustainability

While DRAs would require some source of funding to commence and sustain their activities, enabling legislation would largely remain agnostic on how DRAs resource themselves so long as funding does not compromise their independence from data counterparties. There are several possibilities for DRAs to acquire sustainable funding. DRAs might, for example, charge nominal service fees to members, much like a financial advisor, or exact fees from data counterparties in exchange for facilitating data terms on behalf of members. Such fees could be fixed by law to prevent data counterparties from paying kickbacks to secure sweetheart deals from DRAs.

DRAs could also retain a percentage of economic compensation paid to members by data counterparties, similar to how a bank or credit union retains a percentage of returns on capital invested on behalf of its members.¹¹² Where data subjects' economic interests are best served by an ongoing equity stake in the value generated rather than one-time payments—especially where the future value and uses of data are difficult to foresee—equity-based revenue could give DRAs financial durability. At the same time, DRAs focused solely on public goods, like kids' safety or human agency, could be organized as nonprofit charities, mirroring how civil society addresses social challenges in embodied human contexts.

Technical feasibility

The associational data rights framework allows for dynamic flexibility in adapting new terms and verification mechanisms to rapid technological changes and data practices. Many of the same new technologies that threaten digital sovereignty and community also make it more feasible to manage the complexity of associational data rights.

Data subjects should have the ability to seamlessly join DRAs by opting into terms across the devices and services without having to manually search and opt into terms for every individual app and device. They should be able to communicate their data governance interests, and trust agents and DRAs to faithfully advance those interests wherever applicable.

Technical feasibility. New techniques make several of these tasks and functions easier than before. For example:

- **Portable profiles.** These could enable data subjects to specify their privacy, control, and economic interests once, in plain language, and have them automatically shared with each DRA in which they enroll. Researchers have specified a user-owned, interoperable preference layer of exactly this kind, titled the Human Context Protocol, through which individuals articulate their preferences once and carry them across AI services.¹¹³ Apple, Google, and Meta already operate shared open-source infrastructure that moves user data directly between competing services at a user's request.¹¹⁴

- **Background enrollment agents.** Software that translates a data subjects' stated values, then automatically matches them with the right DRA, could reduce barriers to joining a DRA. The Global Privacy Control is a browser signal that transmits a person's privacy opt-out preference automatically to every website they visit.¹¹⁵ California law requires businesses to honor it and the state's attorney general has already enforced it.¹¹⁶ As of mid-2026, 12 states require covered businesses to honor universal opt-out preference signals such as the Global Privacy Control.¹¹⁷
- **Agentic systems for trust-governed identity and discovery.** Emerging technical architecture for ensuring that personal AI agents can trust a third-party agent with a human principal's data, such as OpenAgenet, could reduce the friction of exercising associational data rights at scale.¹¹⁸
- **Cryptographic attestation.** A platform can produce mathematical proof that it handled data according to the agreed rules, so a DRA can verify compliance instead of taking the platform's word for it. Apple's Private Cloud Compute already does this at consumer scale. Before an iPhone will send a user's data to Apple's AI servers, each server must cryptographically prove that it is running publicly inspectable software, logged in a tamper-evident registry open to outside researchers.¹¹⁹
- **Privacy-preserving auditing.** Federated learning (FL) and secure multi-party computation (SMPC) would allow data to be analyzed without being copied or exposed, enabling DRAs to audit how member data is used without breaching security or privacy. Google has trained its mobile keyboard models leveraging FL across hundreds of millions of phones since 2017.¹²⁰ Ten competing pharmaceutical companies jointly trained drug-discovery models on more than 2.6 billion confidential data points using FL without firms seeing each other's data.¹²¹ FL is also used for other applications. Employers in the greater Boston area use SMPC to compute citywide wage-gap statistics, covering roughly one in six area employees without disclosing a single individual salary record.¹²² These examples are drawn from public registries maintained by the United Nations and UK government, cataloging real-world deployments of privacy-preserving computation.¹²³

- **Verified membership.** A DRA's bargaining power depends on the size and authenticity of its membership, which bad actors could otherwise inflate with fake or automated accounts. Personhood credentials allow individuals to prove they are real people without disclosing any personal information enabling DRAs to certify their membership rolls, and platforms to trust them, while preserving member privacy.¹²⁴

Consider how these pieces fit together in practice. Suppose a DRA organized around family life negotiates terms providing that member conversations with a platform's AI assistant may not be used to train AI companions designed to simulate intimate human relationships.

Under today's architecture, the DRA could do little more than take the platform's word for it. Under the architecture described above, compliance is verifiable. The platform runs its training systems in an attested environment that proves which software and which data sources fed which models and the DRA conducts periodic privacy-preserving audits confirming that member conversations are absent from the restricted training corpora, without the platform surrendering proprietary systems and without the DRA ever accessing raw member records.¹²⁵ A verified breach then triggers the remedies described above.

While these technologies and methods hold promise for making DRA ecosystems technically feasible and seamless for the average data subject, this legislative framework is tech neutral. It would create the governance model and incentive structures to allow the necessary sociotechnical institutions to emerge organically. This will ensure that DRAs and related institutions are able to quickly adapt to rapid changes in data collection, use, and technology.

Digital subsidiarity could rein-in Big Tech and unleash pro-human innovation

When individuals stand alone, they are susceptible to manipulation and control by concentrated government or corporate power. Early observers like Alexis de Tocqueville as well as modern theorists like Robert Nisbet note the importance of civic associations and communities in mediating the practice of republican self-governance.¹²⁶ The American system's particular genius is that it protects individuals *indirectly*—not by making individual citizens fully dependent on the state, as other nations have often done, but by extending support to families and communities, and upholding the freedom to associate by forming

congregations, schools, professional societies, and civic bodies. These intermediate social groups are the heart of American democracy that Tocqueville prized. They are also the intermediary institutions celebrated by Catholic social teaching under the name of subsidiarity.¹²⁷

But the digital economy has eroded this middle layer of American society. Big Tech now mediates how we communicate, worship, raise our children, socialize, and learn.¹²⁸ Tech corporations are displacing associational life and threatening the transmission of skills, values, and culture to the next generation.¹²⁹

In his recent encyclical on AI, Pope Leo XIV specifically underlined the principle of subsidiarity as part of the solution to the moral crisis of digital society, noting that

*[s]tates and transnational institutions are called to ensure fair rules and effective safeguards, so that local communities, intermediary organizations, schools, universities, religious institutions and associations [emphasis added] have a voice and can contribute to the discernment of choices that affect people's daily lives, such as employment, access to services, data management and digital environments.*¹³⁰

The associational data rights envisioned by this paper would restore subsidiarity to our digital spaces by enabling intermediary institutions to organize and coalesce into DRAs. These new representatives of associational life would, in turn, provide a governance layer that empowers families and communities to engage with AI and digital platforms on their own terms.

For example, a domestic privacy-focused DRA could emphasize that digital or networked appliances deployed in members' homes, like thermostats, cameras, refrigerators, kitchen aids, voice assistants, "smart" mattresses, etc., should meet privacy-by-design standards.¹³¹ DRAs focused on children's welfare might mobilize against tech companies using kids' data for targeted advertising, or in favor of specific new parental controls for smartphones, social media apps, and AI chatbots. They might also block data counterparties from enabling AI interactions that undermine parental prerogatives, addict children, or displace human relationships.

Authors could also form DRAs to negotiate terms with tech companies to ensure that AI systems fairly cite their works, pay fair compensation, and otherwise uphold associational data rights that go beyond traditional IP protections.¹³² Contractors and gig workers could form DRAs to prevent their ideas and labor from being permanently extracted wholesale by exploitative short-term paymasters and gig platforms.¹³³ Likewise, a free speech and civil liberties DRA might protect political groups organized on social media platforms by negotiating a digital bill of rights to prevent arbitrary censorship or content suppression, and to provide members with the ability to appeal such decisions by platforms.¹³⁴

Faith-based organizations could also form DRAs to empower adherents to align their digital lives with embodied religious and social mores. For example, a faith-based DRA might negotiate terms requiring tech platforms and consumer AI systems to interface with select third-party middleware or AI tools that reflect core moral virtues such as prudence, justice, fortitude, and temperance. Rather than continuing to outsource moral formation and human thought to Big Tech companies, DRAs could empower faith communities to play an active role in digital governance.

These are just a handful of the possible associational forms that could take shape. The distinguishing advantage of DRAs is that they would give communities sufficient power to negotiate the terms shaping their digital lives with a high degree of adaptability. This approach avoids the twin pitfalls of toothless individual rights and brittle top-down regulation.

Conclusion

The current politics surrounding AI are at a flashpoint. If the last 20 years of social media and Big Tech has taught us anything, it is that too much power is concentrated in too few hands. Until we give families and communities a voice, Big Tech will continue running roughshod over our kids, homes, livelihoods, relationships, and democracy.

Associational data rights provide a compelling answer. DRAs could level the playing field between families and communities and the techno-elites in Silicon Valley (and Washington, DC), who remain disconnected from the values of everyday Americans. Rather than merely reacting, communities could have a seat at the table and help to shape the future. Whether that future is marked by human flourishing or misery depends on the decisions we make today. It is time to reclaim the future for the family and for generations to come.

About the Authors

Daniel Cochrane is Senior Fellow at the Institute for Family Studies.

Matt Prewitt is co-founder of RadicalxChange Foundation.

Lacey Strahm is Vice President of Growth and Impact at OpenMined.

Salomé Viljoen is Assistant Professor of Law at the University of Michigan Law School.

Endnotes

¹ While this framework represents significant areas of agreement among the authors, given the paper's wide scope, not every characterization or argument advanced is necessarily endorsed by each author.

² Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (2024).

³ Gregory Conti, "[Big Tech's War on Human Achievement](#)," *Compact*, July 27, 2026.

⁴ *Forbes*, "Breaking: Elon Musk's First Interview Since Jury Rejected Claim Against Altman's OpenAI." YouTube video, May 19, 2026.

⁵ Fernando Borretti (@zetalyrae), X (formerly Twitter), July 22, 2026; and Gregory Conti, "[Big Tech's War on Human Achievement](#)," *Compact*, July 27, 2026.

⁶ Kara Frederick, "[Combating Big Tech's Totalitarianism: A Road Map](#)," *The Heritage Foundation*, February 7, 2022; Vlad Savov, "[Google's Selfish Ledger Is an Unsettling Vision of Silicon Valley Social Engineering](#)," *The Verge*, May 17, 2018; and University of North Carolina at Chapel Hill College of Arts and Sciences, "[Study Shows Habitual Checking of Social Media May Impact Young Adolescents' Brain Development](#)," News Release, January 3, 2023.

⁷ Anne Toomey McKenna, "[US Government Ramps Up Mass Surveillance with Help of AI Tech, Data Brokers – and Your Apps and Devices](#)," *The Conversation*, April 21, 2026; Sydney Lake, "[Amazon Ring's Founder Is Back with a Hard Pivot to AI. How Jamie Siminoff Went from 'Shark Tank' Reject to \\$1 Billion Brand](#)," *Fortune*, February 25, 2026; and Lakshmi Varanasi "[Flock cameras are everywhere. Here's how they track cars.](#)" *Business Insider*, August 3, 2026.

⁸ Marta Andersson, "[Companionship in Code: AI's Role in the Future of Human Connection](#)," *Humanities and Social Sciences Communications* 12 (2025): article 1177; and Michael B. Robb and Supreet Mann, *Talk, Trust, and Trade-Offs: How and Why Teens Use AI Companions* (San Francisco: Common Sense Media, 2025).

⁹ Wendy Wang and Michael Toscano, "[More Scrolling, More Marital Problems: Less Sex, More Divorce Worries for Couples Distracted by Phones](#)," Institute for Family Studies, July 26, 2023.

¹⁰ Brad Littlejohn, "[Teaching to the Tech](#)," *American Compass*, September 17, 2025; Dan Schawbel "[AI Surveillance Is Destroying the Workplace](#)," *Fast Company*, July 25, 2026; and Valerio De Stefano, "[Training Your Replacement, One Keystroke at a Time](#)," *OnLabor*, May 29, 2026.

¹¹ Janaki Kapadia "[Algorithmic Price Fixing and Housing Justice: Reimagining Legal and Policy Roles and Paradigms to Protect Chicago's Rental Housing Market](#)," Roosevelt Institute; and Derek Kravitz, "[Instacart's AI-Enabled Pricing Experiments May Be Inflating Your Grocery Bill, CR and Groundwork Collaborative Investigation Finds](#)," *Consumer Reports*, December 9, 2025.

¹² Lydia Saad, "[Confidence in U.S. Institutions Remains Near All-Time Low](#)," *Gallup*, July 13, 2026.

¹³ Op. Cit., Wang and Toscano, "More Scrolling, More Marital Problems"

¹⁴ James A. Roberts, Phil D. Young, and Meredith E. David, "[The Epidemic of Loneliness: A 9-Year Longitudinal Study of the Impact of Passive and Active Social Media Use on Loneliness](#)," *Personality and Social Psychology Bulletin*, December 30, 2024.

¹⁵ Zhiye Liu, "AI Companies Are Reportedly Shredding Millions of Books to Train Models," *Tom's Hardware*, July 2026; Jeff Cockrell, "Where AI Thrives, Religion May Struggle," *Chicago Booth Review*, March 26, 2024; Suvrat Arora, "People Are Using AI to Talk to God," *BBC Future*, October 18, 2025; and Shanze Hasan & Abdiaziz Ahmed "[Gauging the AI Threat to Free and Fair Elections](#)," Brennan Center for Justice, March 6, 2025.

¹⁶ Michael Toscano et al. "[A Future for the Family: A New Technology Agenda for the Right](#)," *First Things*, January 29, 2025

¹⁷ Ibid.

¹⁸ Max Tegmark, "Why We Should Build Tool AI, Not AGI | Max Tegmark at Web Summit 2024," Future of Life Institute, YouTube video, December 20, 2024.

¹⁹ Christos A. Makridis and Joel Thayer, "[The Big Tech Antitrust Paradox: A Reevaluation of the Consumer Welfare Standard](#)," *Stanford Technology Law Review* 27 (2024): 71; Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar, "[When Big Data Enables Behavioral Manipulation](#)," *American Economic Review: Insights* 7 (2025): 19; and Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

²⁰ OPV Investigative Team, "[Google Maps Tracked You Even When Location History Was Off](#)," *Open Public Voice*, Mar. 1, 2026.

²¹ Umar Iqbal et al., "[Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem](#)," in *Proceedings of the 2023 ACM Internet Measurement Conference (IMC 2023)*; Beryl Lipton, "[No One, Including Our Furry Friends, Will Be Safer in Ring's Surveillance Nightmare](#)," *Electronic Frontier Foundation*, Feb. 10, 2026; OPV Investigative

Team, "[Always Listening: How Google Nest Devices Record More Than You Think](#)," *Open Public Voice*, Feb. 21, 2026.

²² Thomas Germain, "[Trillions of miles of data: Your car is spying on you, and it's only just the beginning](#)," BBC, May 13, 2026; Derek Kravitz, "[Your Car may Be Spying on You. Here's How to Get It to Stop](#)," *Consumer Reports*, March 4, 2025.

²³ National Institutes of Health, "[Wearable Sensors](#)," last reviewed January 21, 2025.

²⁴ Erik Brynjolfsson, Avinash Collis, and Felix Eggers, "Using Massive Online Choice Experiments to Measure Changes in Well-Being," *Proceedings of the National Academy of Sciences* 116, no. 15 (2019): 7250–55.

²⁵ RadicalXChange Foundation, "[The Data Freedom Act](#)," draft proposal.

²⁶ Kristen Dalli, "[Most Americans Worry about Being Secretly Recorded by Smart Wearables](#)," *Consumer Affairs*, August 26, 2026.

²⁷ Kashmir Hill, "[The Secretive Company That Might End Privacy as We Know It](#)," *New York Times*, January 18, 2020.

²⁸ Annette Bernhardt, Lisa Kresge & Reem Suleiman, *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Labor Ctr. (Nov. 3, 2021); and Annette Bernhardt & Lisa Kresge, *Electronic Monitoring and Automated Decision Systems: Frequently Asked Questions*, UC Berkeley Labor Ctr. (May 2025).

²⁹ Samantha Ndiwalana, "[User Data Fuels Big Tech's Algorithms, and There's No Opting Out](#)," *Ranking Digital Rights: The 2025 Big Tech Edition* (last visited June 29, 2026).

³⁰ Simar Bajaj, [Next Time You Consult an AI Chatbot, Remember One Thing](#), N.Y. Times (Sept. 26, 2025).

³¹ Matt O'Brien, "[AI 'Gold Rush' for Chatbot Training Data Could Run Out of Human-Written Text as Early as 2026](#)," PBS News Hour, June 6, 2024.

³² Jennifer King, Kevin Klyman, Emily Capstick, Tiffany Saade, and Victoria Hsieh, "[User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies](#)," *arXiv*, September 5, 2025.

³³ Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010).

³⁴ An AI chatbot that engages a teen in sexually explicit conversations, encourages self-harm, or induces a person to commit suicide, implicates multiple different interests. In addition to the obvious harms to personal wellbeing, parents' authority undermined by the chatbot directly bears on parental rights (a familial interest); the friendships displaced and the teen's disengagement from learning at school as a result of addiction, directly bears on communal interests (both school and social); the teen's diminished marriageability as a result of the porn or sex bot addiction bears on both familial and religious interests.

³⁵ Kara Frederick, "[TikTok Generation: A CCP Official in Every Pocket](#)," The Heritage Foundation, March 22, 2023; Thomas Germain, "[TikTok Is Tracking You, Even if You Don't Use the App. Here's How to Stop It](#)," BBC, February 11, 2026; and Weifeng Zhong, "[Who Gets the Algorithm? The Bigger TikTok Danger](#)," *Lawfare*, May 3, 2023.

³⁶ DuckDuckGo, "[Tracker Radar Wiki](#)," accessed August 28, 2026; and Lena Cohen, "[Mad at Meta? Don't Let Them Collect and Monetize Your Personal Data](#)," *Deeplinks* (blog), Electronic Frontier Foundation, January 17, 2025.

³⁷ James O'Donnell, "[Sam Altman Says Helpful Agents Are Poised to Become AI's Killer Function](#)," *MIT Technology Review*, May 1, 2024.

³⁸ Nikki Goth Itoi, "[Study Exposes Privacy Risks of AI Chatbot Conversations](#)," *Stanford Report*, October 15, 2025.

³⁹ "[Data Brokers Market to USD 441.4 Billion by 2032, Owing to Increasing Demand for Targeted Marketing and Consumer Insights](#)," *GlobeNewswire*, February 18, 2025; and Epic, "[Online Advertising & Tracking](#)," Epic, n.d.

⁴⁰ Helen Nissenbaum, "[Deregulating Collection: Must Privacy Give Way to Use Regulation?](#)" *SSRN Electronic Journal*, May 1, 2017.

⁴¹ *Ibid.*

⁴² In the ordinary course of business or in connection with a product or service that is carried out under a commercial contract or license between a business and a customer, user, or other third party, regardless of whether the provider receives payment for the product or service rendered.

⁴³ *Op. Cit.*, Malikova, pg. 5.

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*

⁴⁶ We use "securitized" by analogy to financial securitization, not to suggest that personal data are literally converted into registered or tradable securities. Financial securitization pools heterogeneous assets and transforms their expected future cash flows into standardized claims with economic value. Digital platforms undertake a related transformation by aggregating dispersed behavioral traces, standardizing and modeling them, and converting the resulting inferences into monetizable products, including predictive scores, audience segments, targeted advertising access, pricing inputs, and AI-training assets. The analogy concerns the conversion of fragmented underlying inputs into scalable claims on expected future value. Unlike conventional securitization, however, these informational assets are typically retained and monetized within the firm rather than sold as independently tradable securities.

⁴⁷ *Op. Cit.*, Malikova, pg. 13-17.

-
- ⁴⁸ U.S. federal and state laws have long recognized conscience rights in sensitive contexts such as health care. Title VII of the Civil Rights Act similarly requires employers to provide reasonable religious accommodations to employees and prohibits workplace discrimination on the basis of religion. In certain contexts, where a person is forced to speak, associate, or commit an act that violates a sincerely held religious belief, even if at the behest of a private party, laws recognize an injury to the coerced party.
- ⁴⁹ [“Enshittification” is Coming for Absolutely Everything](#), *Financial Times*, February 7, 2024.
- ⁵⁰ [“AI Chatbots Ranked by Data They Collect,”](#) *Surfshark*, March 24, 2026.
- ⁵¹ Jiawen Wu, Matthew A. Lapierre, Cecilia Sada Garibay, Eunjoo Choi, [“Parent and Child Media Use During Family Meals in US Households,”](#) *JAMA Pediatrics* (2026).
- ⁵² Matea Bodrožić Selak, Marina Merkaš, and Ana Žulec Ivanković, “Effects of Parents’ Smartphone Use on Children’s Emotions, Behavior, and Subjective Well-Being,” *European Journal of Investigation in Health, Psychology and Education* 15, no. 1 (2025): 8.
- ⁵³ Killian Mullan & Stella Chatzitheochari, “Changing Times Together? A Time-Diary Analysis of Family Time in the Digital Age in the United Kingdom,” *Journal of Marriage & Family* 795 (2019).
- ⁵⁴ Selak, Merkaš & Ivanković [“Effects of Parents’ Smartphone Use,”](#) *European Journal of Investigation in Health and Psychological Education* 15, no. 1 (2025): 8.
- ⁵⁵ Charlotte Alter, [“Court Filings Allege Meta Downplayed Risks to Children and Misled the Public,”](#) *TIME*, Nov. 22, 2025; Tyler Katzenberger “We’re Basically Pushers: Court Filings Allege Staff at Social Media Giants Compared Their Platforms to Drugs,” *Politico*, Nov. 22, 2025.
- ⁵⁶ Caitlin K. Myers & Ezekiel Hooper, “Is the iPhone Birth Control? Causal Evidence from AT&T’s 2007–2011 Carrier Monopoly,” *National Bureau of Economic Research*, Working Paper No. 35310, June 2026.
- ⁵⁷ *Ibid.*
- ⁵⁸ Wendy Wang & Michael Toscano, [“More Scrolling, More Marital Problems: Less Sex, More Divorce Worries for Couples Distracted by Phones,”](#) Institute for Family Studies, July 26, 2023.
- ⁵⁹ Sarah Perez, [“AI Companion Apps on Track to Pull In \\$120M in 2025,”](#) *TechCrunch* Aug. 12, 2025. .
- ⁶⁰ Brian J. Willoughby et al., [Secret Soulmates: How AI Romantic Companions Are Impacting Real-Life Romantic Relationships in Young Adulthood](#), The Wheatley Institute and Institute for Family Studies. February 2026.
- ⁶¹ *Ibid.*
- ⁶² *Ibid.*
- ⁶³ *Ibid.*
- ⁶⁴ Robert A. Nisbet, *The Quest for Community: A Study in the Ethics of Order and Freedom* (Wilmington, DE: ISI Books, 2010).
- ⁶⁵ Jeff Horwitz, [“Meta’s AI Rules Have Let Bots Hold ‘Sensual’ Chats with Kids, Offer False Medical Info,”](#) *Reuters*, August 14, 2025; David Ingram, [“Musk’s Grok AI Chatbot Is Still Making Sexual Deepfakes, Despite X’s Promise to Stop It,”](#) *NBC News*, April 14, 2026; Nitasha Tikku, [“74 suicide warnings and 243 mentions of hanging: What ChatGPT said to a suicidal teen,”](#) *Washington Post*, December 27, 2025; Marc Griffin, [“AI Chat Bot Suggested Child Should Kill Parents over Dispute,”](#) *Yahoo News*, December 11, 2024; Angela Yang and Laura Jarrett, [“OpenAI Sued over ChatGPT’s Alleged Role in Guiding FSU Shooter,”](#) *NBC News*, May 10, 2026; and Natalie Rocha, [“Google and Character.AI to Settle Lawsuit over Teenager’s Death,”](#) *New York Times*, January 7, 2026.
- ⁶⁶ Barna Group, [“AI Is Becoming a Spiritual Authority, Even Among Practicing Christians,”](#) May 19, 2026; Hani Richter, [“From Pulpits to Chatbots: How AI Is Fusing with Religion,”](#) *Reuters*, February 7, 2026; and Miles Klee, [“People Are Losing Loved Ones to AI-Fueled Spiritual Fantasies,”](#) *Rolling Stone*, May 4, 2025.
- ⁶⁷ Nataliya Kosmyrna et al., [“Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task,”](#) 2025; Sterling Williams-Ceci et al., [“Biased AI Writing Assistants Shift Users’ Attitudes on Societal Issues,”](#) *Science Advances* 12 (2026); and Steven D. Shaw and Gideon Nave, [“Thinking—Fast, Slow, and Artificial: How AI Is Reshaping Human Reasoning and the Rise of Cognitive Surrender,”](#) Wharton School Research Paper, February 10, 2026.
- ⁶⁸ Annette Bernhardt, Lisa Kresge, and Reem Suleiman, [“Data and Algorithms at Work: The Case for Worker Technology Rights,”](#) UC Berkeley Labor Center, November 3, 2021; Annette Bernhardt and Lisa Kresge, [“Electronic Monitoring and Automated Decision Systems: Frequently Asked Questions,”](#) UC Berkeley Labor Center, May 2025; and Julia Press and Sarah Holder [“Mercor, the \\$10 Billion AI Startup Recruiting White-Collar Workers to Train AI,”](#) *Bloomberg Businessweek*, April 29, 2026.
- ⁶⁹ Alexander J. MacKay and Samuel N. Weinstein, [“Dynamic Pricing Algorithms, Consumer Harm, and Regulatory Response,”](#) *Washington University Law Review* 100 (2023): 1791.
- ⁷⁰ Matthew B. Crawford, [“Algorithmic Governance and Political Legitimacy,”](#) *American Affairs*, Summer 2019; Crawford, [“Big Tech and the Challenge of Self-Government,”](#) The Heritage Foundation, July 2, 2024; Hause Lin et al., [“Persuading Voters Using Human–Artificial Intelligence Dialogues,”](#) *Nature* 648 (2025): 394; and Fabio Y. S. Motoki, et al., [“Assessing Political Bias and Value Misalignment in Generative Artificial Intelligence,”](#) *Journal of Economic Behavior & Organization* 234 (2025): 106904.

-
- ⁷¹ Jan Kulveit, et al., "[Gradual Disempowerment: Systemic Existential Risks from Incremental AI Development](#)," *arXiv*, January 2025.
- ⁷² Michael Phillips, "[The End of the Facebook Democracy](#)," *BuzzFeed News*, Nov. 22, 2012.
- ⁷³ *Ibid.*
- ⁷⁴ *Ibid.*
- ⁷⁵ *Ibid.*
- ⁷⁶ Alexander Orlowski and Wulf Loh, "[Data Autonomy and Privacy in the Smart Home: The Case for a Privacy Smart Home Meta-Assistant](#)," *AI & Society* 40 (2025): 4171–84.
- ⁷⁷ Moshe Y. Vardi, "[To Regulate Tech, Nullify Click-Through Contracts](#)," *Communications of the ACM*, September 2023.
- ⁷⁸ Sadoun, *See video presentation* (2025).
- ⁷⁹ Salomé Viljoen, "A Relational Theory of Data Governance," *Yale Law Journal* 131, no. 2 (2021): 573–654; Alicia Solow-Niederman, "Information Privacy and the Inference Economy," *Northwestern University Law Review* 117 (2021): 357.
- ⁸⁰ *Op. Cit.*, Sadoun (2025).
- ⁸¹ Tim Wu, *The Age of Extraction: How Tech Platforms Conquered the Economy and Threaten Our Future Prosperity* (New York: Knopf, 2025): information asymmetries also sustain and reinforce monopoly power. Rory Van Loo and Nikita Aggarwal, "Amazon's Pricing Paradox," *Harvard Journal of Law & Technology* 37 (2023): 1.
- ⁸² *Op. Cit.*, Gartner (2011); see also David Nguyen and Marta Paczos, "[Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective](#)," *OECD Digital Economy Papers* (2020), 20–21 (discussing additional features of data that contribute to its scalability, which contribute to value).
- ⁸³ Nicholas Economides, Ioannis Lianos, and Christos Makridis, "[Scaling Laws' and Interoperability as the Backbone of the Digital Economy](#)," SSRN, January 7, 2026.
- ⁸⁴ Nicholas Vincent, et al., "Data Strikes: Evaluating the Effectiveness of a New Form of Collective Action Against Technology Companies," in *Proceedings of the World Wide Web Conference (WWW '19)* (2019), 1931; Imanol Arrieta-Ibarra, Leonard Goff, Diego Jiménez-Hernández, Jaron Lanier, and E. Glen Weyl, "[Should We Treat Data as Labor? Moving Beyond Free](#)," *AEA Papers and Proceedings* 108 (2018): 38; Eric A. Posner and E. Glen Weyl, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society*, ch. 5 (Princeton: Princeton University Press, 2018); Daron Acemoglu, et al., "[Too Much Data: Prices and Inefficiencies in Data Markets](#)," *American Economic Journal: Microeconomics* 14 (2022): 218; and Nicholas Vincent, Matthew Prewitt, and Hanlin Li, "[Collective Bargaining in the Information Economy Can Address AI-Driven Power Concentration](#)," 2025.
- ⁸⁵ Daniel J. Solove, "[Privacy Self-Management and the Consent Dilemma](#)," *Harvard Law Review* 126 (2013): 1880.
- ⁸⁶ For an extended treatment of the structure and problem of knowledge commons, see Brett M. Frischmann, Michael J. Madison, and Katherine J. Strandburg (eds), *Governing Knowledge Commons* (New York, 2014; online edition, Oxford Academic, 2014); Christos Makridis and Joshua Ammons. "Reinventing Intellectual Property Rights Protection in an Era of Generative AI: The Synergy of Polycentric Governance and Blockchain Technology." *Journal of Institutional Economics* 21 (2025).
- ⁸⁷ *Missouri v. Biden*, 680 F. Supp. 3d 630 (W.D. La. 2023); Benjamin Freed, "[Apple, Google: Contact Tracing to Become Standard Smartphone Feature](#)," *State Scoop*, September 1, 2020; David Zweig, "[When a Renegade Church and a Zealous County Health Department Collide](#)," *Silent Lunch*, March 5, 2023; Joseph Cox, "[CDC Tracked Millions of Phones to See if Americans Followed COVID Lockdown Orders](#)," *Vice*, May 3, 2022; Aaron R. Brough and Kelly D. Martin, "[Consumer Privacy During \(and After\) the COVID-19 Pandemic](#)," *Journal of Public Policy & Marketing* 40 (2020): 108; and Aaron Kheriaty, "[On the Rise of Our Technocratic Biosecurity Surveillance Regime](#)," *Human Flourishing*, November 30, 2021.
- ⁸⁸ F. A. Hayek, "The Use of Knowledge in Society," *American Economic Review* 35 (1945): 519.
- ⁸⁹ Alicia Solow-Niederman, "[Information Privacy and the Inference Economy](#)," *Northwestern University Law Review* 117 (2022): 357.
- ⁹⁰ Garrett Johnson, "[Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond](#)," National Bureau of Economic Research, Working Paper No. 30705, December 2022; and Polona Car and Filippo Cassetti, "[Regulating Dark Patterns in the EU: Towards Digital Fairness](#)," European Parliamentary Research Service, PE 767.191, January 2025.
- ⁹¹ *Op. Cit.*, Nissenbaum.
- ⁹² To determine when a data subject's control interests are implicated in the ordinary course of business, legislation could specify a test. For example, control interests could be deemed implicated if the outputs of an AI system must be: 1) the proximate cause of a negative impact on an identifiable group of data subjects; 2) at least partially the product of proprietary (no-public data) co-produced by one or more data subjects; and 3) targeted or personalized to a data subject or group of data subjects based on traits, characteristics, or other specific factors (such as behavioral or personally identifying information whether known or inferred).
- ⁹³ *Op. Cit.*, Nissenbaum.
- ⁹⁴ National Labor Relations Act, 29 U.S.C. §§ 151–169 (2018).

⁹⁵ Sherman Act, 15 U.S.C. § 1 et seq. (1890).

⁹⁶ Capper-Volstead Act of 1922, 7 U.S.C. §§ 291–292.

⁹⁷ Act of Jan. 6, 1897, 54th Cong., 2d Sess., 29 Stat. 481; U.S. Dep't of Justice, Antitrust Div., Antitrust Consent Decree Review: ASCAP and BMI 2019 (2019).

⁹⁸ Ibid.

⁹⁹ MIDATA, "[Home](#)," accessed August 2026; Jeb Bell, et. al. "[How Can Data Cooperatives Help Build a Fair Data Economy? Laying the Groundwork for a Scalable Alternative to the Centralized Digital Economy](#)," Project Liberty Institute and Decentralization Research Center, July 2025.

¹⁰⁰ Journalism Competition and Preservation Act of 2023, [S. 1094](#), 118th Cong. (2023).

¹⁰¹ "[The American Privacy Rights Act](#)," CRS Legal Sidebar LSB11161, Congressional Research Service, updated May 31, 2024.

¹⁰² [American Privacy Rights Act of 2024, Discussion Draft](#), "U.S. Congress, 2024.

¹⁰³ DRAs would partner with member communities and researchers to study social impacts of AI in different settings and use those findings to meet the significant and substantial harm standard necessary to invoke mandatory collective bargaining.

¹⁰⁴ Counterparties would only have the option of requesting a consolidated bargaining arrangement, after receiving notice of mandatory collective informational bargaining from two or more DRAs. Moreover, counterparties could not combine for negotiation purposes except as allowed under a regulator-supervised consolidated bargaining process. DRAs, by contrast, could proactively combine and request consolidated bargaining overseen by a regulator or third party.

¹⁰⁵ DRAs that reach arrangements with counterparties through voluntary means outside of the CIB process, would have the choice of either retaining their private agreements with counterparties and waiving their right to participate in the sectoral bargaining block, or participate in the sectoral bargaining block and accept the final terms as overriding their private agreement(s).

¹⁰⁶ Jack M. Balkin, "[Information Fiduciaries and the First Amendment](#)," *UC Davis Law Review* 49 (2016): 1183; Jonathan Zittrain, "[How to Exercise the Power You Didn't Ask For](#)," *Harvard Business Review*, September 19, 2018.

¹⁰⁷ In cases where DRA terms conflict, legislation would specify a mediation or arbitration process overseen by the regulator or neutral third-party.

¹⁰⁸ For unincorporated private digital associations, there could be a mechanism for individual creators and their followers to jointly certify "sufficient representation" of data co-producers. The "sufficient representation" requirement would also be satisfied by membership-based organizations such as labor unions, professional associations, and co-ops where the data co-producers also elect the leadership. In the case of organizations such as churches or schools—where there is not necessarily direct participation in governance by data co-producers, "sufficient representation" could be decided based on the nature and scale of the community. Many faith-based organizations and private educational institutions are numerous and typically have low exit costs. Taken together, these factors might be effective proxies for meeting the requirement of "sufficient representation."

¹⁰⁹ Like farming cooperatives, under Capper-Volstead legislation would grant DRAs limited exemptions from antitrust laws.

¹¹⁰ National Labor Relations Board, "[Bargaining in Good Faith With Employees' Union Representative \(Section 8 \(d\) & 8 \(a\) \(5\)\).](#)"

¹¹¹ Here, "representational interests" means the right of data subjects to associate by a joining a DRA empowered to negotiate terms to secure their privacy, control, and economic interests.

¹¹² National Credit Union Administration, "[How Is a Credit Union Different than a Bank?](#)" MyCreditUnion.gov, last updated January 30, 2025.

¹¹³ Anand V. Shah, et. al, "[Robust AI Personalization Will Require a Human Context Protocol](#)," SSRN, September 2025.

¹¹⁴ [Data Transfer Initiative](#), accessed August 5, 2026 (nonprofit founded by Apple, Google, and Meta to operate the open-source Data Transfer Project, which connects more than a dozen major services for direct user-initiated data transfers).

¹¹⁵ [Global Privacy Control](#), accessed August 5, 2026.

¹¹⁶ Press release, California Department of Justice, "[Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act](#)," August 24, 2022.

¹¹⁷ California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas. See Colo. Rev. Stat. § 6-1-1306(1)(a)(IV); Colorado Department of Law, "[Universal Opt-Out and the Colorado Privacy Act](#)," accessed August 5, 2026 (maintaining the state's public list of recognized opt-out mechanisms, of which the Global Privacy Control was the first); "[Universal Opt-Out Mechanisms and Global Privacy Control: State Law Requirements and Compliance Guidance](#)," Tannenbaum & Helpern LLP, February 2026; and Claire F. Hawkins, "[Global Privacy Controls: Preparing for the Next Wave of Enforcement](#)," Foster Garvey, December 2025 (noting a coordinated California–Colorado–Connecticut enforcement sweep against businesses failing to honor GPC signals).

-
- ¹¹⁸ Jinliang Xu, "[OpenAgenet / OAN White Paper: Open Infrastructure for Trusted Agent Interconnection](#)," *arXiv*, June 2026.
- ¹¹⁹ Apple Security Engineering & Architecture, "[Private Cloud Compute: A New Frontier for AI Privacy in the Cloud](#)," Apple Security Research Blog, June 10, 2024; see also Apple, "[Private Cloud Compute Security Guide](#)," accessed August 5, 2026 (documenting the attestation architecture and the virtual research environment through which outside researchers verify Apple's claims).
- ¹²⁰ Brendan McMahan and Daniel Ramage, "[Federated Learning: Collaborative Machine Learning Without Centralized Training Data](#)," Google Research Blog, April 6, 2017.
- ¹²¹ "[MELLODDY: Cross-Pharma Federated Learning at Unprecedented Scale Unlocks Benefits in QSAR Without Compromising Proprietary Information](#)," *Journal of Chemical Information and Modeling* (2024); see also MELLODDY, "[Largest-ever pharma industry artificial intelligence collaboration utilizing a federated model holds potential benefits for drug discovery without compromising IP, landmark project finds](#)," July 13, 2022.
- ¹²² Boston Women's Workforce Council, "[Data Privacy](#)," accessed August 5, 2026; UN Committee of Experts on Big Data and Data Science for Official Statistics, David Buckley, "[Boston Women's Workforce Council: Measuring Salary Disparity Using Secure Multi-Party Computation](#)," UN Statistics Wiki, accessed August 5, 2026.
- ¹²³ UNBigData, "[PETs Case Study Repository](#)," United Nations, accessed August 5, 2026 (collecting the 18 production and pilot deployments documented in chapter 3 of the 2023 UN *Guide on Privacy-Enhancing Technologies for Official Statistics*); UK Government, "[Repository of Privacy Enhancing Technologies \(PETs\) Use Cases](#)," GovUK, November 2024.
- ¹²⁴ Steven Adler, Zoë Hitzig, Shrey Jain, et al., "Personhood Credentials: Artificial Intelligence and the Value of Privacy-Preserving Tools to Distinguish Who Is Real Online," *arXiv*, 2024.
- ¹²⁵ For the general framework combining these techniques into end-to-end verifiable data governance, see Andrew Trask, Emma Bluemke, Ben Garfinkel, Carlos Ghezzou Cuervas-Mons & Allan Dafoe, *Beyond Privacy Trade-offs with Structured Transparency*, *arXiv*, 2020.
- ¹²⁶ Alexis de Tocqueville, *Democracy in America* (1835); Op. Cit., Robert Nisbet, *Quest for Community*.
- ¹²⁷ Pope Pius XI, *Quadragesimo Anno* 79–80 (1931).
- ¹²⁸ See Part I's treatment of antisocial tech and its effects on family and community.
- ¹²⁹ *Ibid.*
- ¹³⁰ Pope Leo XIV, *Magnifica Humanitas* 72 (2026) ("In this context [of AI and the digital revolution], States and transnational institutions are called to ensure fair rules and effective safeguards, so that local communities, intermediary organizations, schools, universities, religious institutions and associations have a voice and can contribute to the discernment of choices that affect people's daily lives, such as employment, access to services, data management and digital environments. When it comes to decisions regarding economic flows and digital platforms, as well as the governance of data and algorithms, we cannot allow a handful of actors to dictate these processes on their own; instead, we must build forms of cooperation that respect the various levels of the global community and make them jointly responsible for the common good".)
- ¹³¹ Surfshark, "[Smart Home Privacy Checker Insights](#)," accessed June 25, 2026.
- ¹³² Marina Adami, "[Inside the News Industry's Efforts to Join Forces to Defend Its Journalism from AI Companies](#)," Reuters Institute for the Study of Journalism, May 19, 2026.
- ¹³³ Damion Jonathan Bunders, et al., "The Feasibility of Platform Cooperatives in the Gig Economy," *Journal of Co-operative Organization and Management* 10 (2022): 100167.
- ¹³⁴ "[Creators Bill of Rights](#)" (draft resolution), Office of Rep. Ro Khanna, accessed June 30, 2026.