The Data Freedom Act[1]

What's At Stake

The immense economic importance of data presents one of the most important policy challenges of our time. Yet to many, the nature of the problem remains opaque. The processes by which data gives rise to value differ from the processes by which value was produced in the 20th century. Therefore, traditional ways of thinking about property, investment, and productivity often serve us poorly in this context.

Yet we cannot afford to remain confused. Because data nearly always contains information about groups, communities, and networks (in addition to individuals), it cannot be treated as conventional personal property without leading to distortions and market failures. This difficulty has resulted in an imbalanced economy in which powerful private businesses wield inappropriate power over millions by harnessing their information.

The power dynamic regarding data mirrors our society's growing inequality. It is time for legislators to address the policy vacuum that has allowed millions to be denied their rightful share in the data economy.

When Value Comes From Network Effects, Who Owns the Network?

Data about people is always the output of a network of social activity. Even apparently "individual" data, such as a particular consumer's shopping habits or travel itinerary, is a product of the social world in which that person lives. For example, lists of items Jane purchases, and places she visits, also contain information about what her friends and family buy, and where they like to go.[2] As a result, data about individuals cannot be understood as "belonging" exclusively to those individuals.

Here are a few more examples that illustrate why data belongs more properly to communities, groups, and networks, than to individuals:

- Genetic data: Whenever people reveal their own genetic data, they also reveal much about their family members.

---

[1] This draft proposal was assembled by RadicalxChange Foundation Ltd. with the volunteer help of more than 20 prominent academics, entrepreneurs, and activists, who participated in a multi-month research and brainstorming process. A final draft of the report will contain a full list of contributors.

[2] The Data Freedom Act is informed by a model of social, overlapping claims to data. This view of data, which challenges more familiar notions of individual data ownership, is echoed by top researchers in the fields of data privacy, security, and network economics. See, e.g., Delacroix and Lawrence, 2019, https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz014/5579842; Benzell and Collis, 2019: http://ide.mit.edu/sites/default/files/publications/Multi-Sided%20Platform%20Strategy%2C%20Taxation%20and%20Regulation%20October%202019.pdf

- Social graphs: Every individual's social networking data, such as their contacts or friend lists, also contains important information about the social networks of those friends and contacts.
- Multiparty Records: Text or email conversations, group photos, calendar entries for meetings, and many other records of social life, record many peoples' activities--not only those of the person who chooses to divulge or exploit the records.
- Literally all data about every particular individual--what they eat for breakfast, what radio stations they like, and what diseases they have--can be combined with other public or private data to make better predictions about other people, especially their friends, family, and colleagues.

Thus, every person's data can harm the interests of others in his or her network.

Another interesting observation supports the idea that data really should belong to groups rather than individuals. Namely, "individual" data only acquires its vast financial value when combined with the data of other individuals, forming collective datasets.

In short, where a single person's data has little apparent utility, the combined data of many people can become exponentially more valuable. As the numbers of people increase, different individuals' datasets can "complement" one another, powering rich, reliable predictions and inferences--even about individuals and communities who never willingly shared any information about themselves.[3]

This simple insight--that data emerges from networks, and derives its value from network effects--is the key to understanding the problems of the data economy. Our traditional notions of individual property rights are a mismatch for data because, unlike most other kinds of property, people who decide to give data away cheaply very seriously affect the interests of others around them. A new economic model that conceives of data as the property of larger groups and networks is necessary to restore fairness and user control.

We cannot afford to ignore this problem. It goes without saying that the power derived from data can be terribly abused.[4] And even short of obvious abuse, it can be used to influence consumer and citizen behavior in ways that raise much more serious concerns than the advertising techniques of the 20th century.[5] Even more significantly, machine learning and artificial intelligence techniques will improve exponentially, transforming large datasets into powerful instruments of social and political control.

---

[3] For more on data's increasing returns characteristics, see Li, Nirei, Yamana, 2019: https://www.rieti.go.jp/jp/publications/dp/19e022.pdf

[4] See Facebook's experiments affecting users' moods, https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/; Cambridge Analytica scandal generally; and Renee DiResta's work on political actors using social media campaigns to influence politics: https://www.ribbonfarm.com/2018/11/28/the-digital-maginot-line/, https://yalereview.yale.edu/computational-propaganda

[5] Research on Youtube and extremism helpfully summarized by Tristan Harris of the Center for Humane Technology: https://vimeo.com/332532972

Economic injustice also threatens. Imagine a machine learning algorithm that makes editing easy. Such a product could be worth billions, and it could undermine the job security of precisely those people whose data labor made it possible: editors. Without meaningful change, the immense value of the data of millions of people will accrue exclusively to the few who succeed in winning the races to a handful of powerful new technologies.

Lawmakers' Options

It is difficult to imagine a future in which individuals or communities wrest back meaningful leverage, absent policy change. Large institutions have extremely durable advantages in gathering data and using it to train algorithms.[6] Lawmakers must address the situation.

But what would the ideal policy look like? Data-driven businesses, eager to avoid new rules, are busily promoting incremental changes to their practices.[7] Moreover, some privacy advocates fret that policies enhancing users' power to negotiate over their data will encourage them to hand yet more more information to big businesses.[8]

An ideal policy response would strike a flexible balance between the benefits of a robust data economy and the long-term interests of individuals and communities. Because the problem is so complex, it is a poor candidate for precise social planning: Market mechanisms must be harnessed to some degree to strike a satisfactory balance. However, no market mechanism will improve matters unless communities, groups, and networks acquire meaningful bargaining power over their data interests. This is why we believe increased bargaining power should be the principal aim of any comprehensive new data policy.

Until now, concerned lawmakers have largely gravitated toward strengthening privacy protections as a means of helping consumers control their data.[9] This is an important step in the right direction. However, stronger privacy rules are only a half-measure--they do not address the deeper problems of the data economy.

Why Isn't Privacy Legislation Enough?

The legitimate interests that individuals and communities have in their data extend beyond privacy. There are at least two other kinds of important interests, which we might call "financial" interests and "control" interests. These can be infringed even when privacy is not.

---

[6] See Jaron Lanier on "Siren Servers" in *Who Owns the Future* and elsewhere.

[7] See, e.g., Google's 2019 policies: https://www.washingtonpost.com/technology/2019/05/07/google-vows-greater-user-privacy-after-decades-data-collection/

[8] See Elettra Bietti for more on the perverse incentive worry: https://ethics.harvard.edu/elettra-bietti-may-13-2019

[9] See, e.g., the GDPR. See also the California Consumer Privacy Act: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

Financial interests refer to the interests that individuals and communities have in the economic value of data pertaining to them. To illustrate, let us say that a number of people trade access to personal data for the use of a convenient digital service. That digital service then aggregates their individual data, generating a pooled dataset, insights from which can be sold for many times more than the summed value of the services provided to the individuals. Here, financial interests are being dis-served. The community as a whole is getting a bad deal, even if no one involved has any privacy concerns.

Control interests in data refer to the interests of individuals and communities in determining the purposes for which information about them is used. Just as one might decline to work for an employer who behaves illegally or unethically, individuals and communities may wish to withhold their data from certain parties or purposes for any number of legitimate reasons. Again, this is true even if their data could be anonymized in such a way that no traditional privacy interests would be implicated.

Privacy legislation therefore cannot suffice. The interests that it protects do not include the legitimate financial and control interests at issue. To see why, it helps to notice that privacy is a somewhat narrow, individualistic concept: Privacy interests are often closely held, only covering information likely to be held by an individual and his or her family and close friends. Financial and control interests, however, extend much further into social networks. Entire communities--geographic, cultural, professional, or otherwise--are jointly responsible for the creation of vast datasets that can only be appropriately managed by the community as a whole. Think, for example, of professional editors whose work goes into natural language editing algorithms; or genetic communities who wish to broadly disseminate information about hereditary diseases for research purposes, without letting it fall into the hands of discriminatory insurers.

Privacy is the wrong metaphor. "Data as labor," though still imperfect, has important advantages.

Why the Labor Metaphor?

It is useful to consider the parallels between peoples' interests in their data and workers' interests in their labor.

Laborers have *de facto* financial and control interests. They may negotiate a share in the fruits of their labor, and may withhold their labor from anyone they do not wish to serve.

Yet, historically as today, those interests are undermined when large numbers of laborers must negotiate on an individual basis against a relatively small number of powerful employers.[10] Labor unions arose as a means of rebalancing the distortions caused by such market concentration. When they work properly, unions transform exploitative, failing labor markets into fairer negotiating environments.

---

[10] See Azar, Marinescu, and Steinbaum on the effects of labor market concentration: http://www.marinescu.eu/AzarMarinescuSteinbaum.pdf

The current bargaining situation between Data Producers (ordinary citizens of the digital world) and Data Buyers (digital platforms, advertisers, and the like) constitutes a market failure. This is evident, for example, in the practical impossibility of simple market behaviors such as avoiding the use of particular digital services, and renegotiating contracts like privacy policies on an individual basis. It is also evident in analyses showing that the owners of large social networks (such as Facebook) destroy far more value for others than they capture for themselves through their monetization interventions such as targeted advertising.[11]

Basic features of a fair marketplace, such as meaningful opt-out possibilities, and widely-shared ownership in widely-used platforms, will become thinkable only when data interests become the subject of collective bargaining.

The Case for Data Coalitions

The idea of creating intermediaries with legal fiduciary duties to shield ordinary people from the vicissitudes of the data economy has a somewhat controversial history. Proponents see it as accomplishing some combination of the following goals:[12]

- Establishing reliable advocates for individuals' data interests, analogous to legal or financial fiduciaries
- Leveraging market forces to help reveal the value of a complex, hard-to-value asset (i.e., data)
- Empowering and incentivizing entrepreneurs to think creatively about how to advance the data interests of individuals and communities
- Bolstering the bargaining power of individuals and communities, as a counterweight to the network-effect-driven market power of digital platforms

Others, however, worry about unwanted consequences including:[13]

- Creating a perverse incentive (either for all people, or for the most vulnerable in particular) to sell more data and accept more surveillance by private businesses
- Creating profit-motivated data intermediaries that exploit individuals just as much as status quo businesses
- Technical challenges in data custody and processing
- Unfair situations in which some people are in a position to wrongly profit from the value of other peoples' data

---

[11] Benzell and Collis, 2019: http://ide.mit.edu/sites/default/files/publications/Multi-Sided%20Platform%20Strategy%2C%20Taxation%20and%20Regulation%20October%202019.pdf

[12] See Delacroix and Lawrence, 2019, https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz014/5579842; Lanier and Weyl, 2018 https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society

[13] See Bo Waggoner surveying various relevant views: https://www.bowaggoner.com/blahg/2019/04-28-data-is-capital/index.html

Here, we have made an effort to map the problem space and sketch a fairly detailed solution. Our proposal takes seriously the worries above, and robustly addresses them. We envision a new class of business entities, called Data Coalitions, which would:

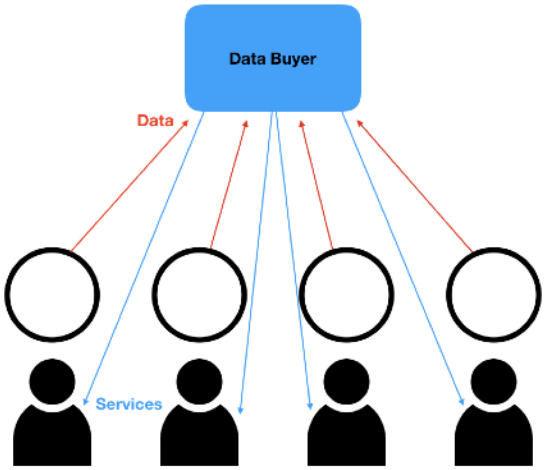
- owe strict duties to the individuals and groups who join them;
- have special exemptions from a new set of rules regarding the treatment of data; and
- be regulated by a new administrative body (the “Data Relations Board”).

The aim is for Data Coalitions to benefit individuals and communities by affording them dramatically increased bargaining power. Such bargaining power could be used, first, to receive a fair share of income generated from data pertaining to them, but also—at least as importantly—to protect their privacy and control how their data is used by others. The legislation attempts to preclude various possibilities that could lead to “races to the bottom” between Data Coalitions, or that could enable businesses to undermine or circumvent Data Coalitions. And it builds in sufficient flexibility for technical challenges to be addressed. Given the complexity of the subject matter, certain issues must be addressed by subsequent regulations. However, this proposal embodies a comprehensive effort to sketch in substantial detail a legislative framework that could serve as the basis for a fairer data economy.

Improving the Bargaining Situation

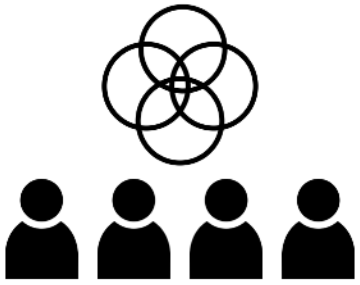
To understand the aim of the legislation, it is useful to reflect upon the reasons Data Producers are in such a difficult bargaining position today, and the unique challenges posed by bargaining for data.

We typically think of data like the picture above. Different people have different, distinct sets of data (represented by the circles above their heads). These people exchange their data with data “buyers” such as apps and platforms, which repay them with free or low-cost services, as below:



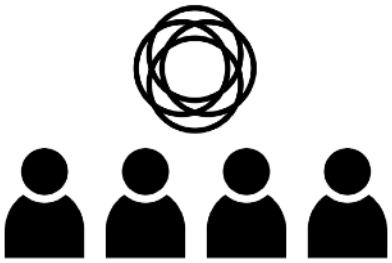
What’s wrong with this picture? Why doesn’t it depict a fair transaction? After all, even though there are relatively few Data Buyers compared to Data Producers (people), the Data Buyers are in intense competition with one another.

The answer is that the picture above is fundamentally misleading. It misunderstands the nature of data itself, and the time has come to discard it as a model of the data marketplace. In reality people don’t have distinct, hermetically-sealed datasets. Rather, they have overlapping ones, like this:

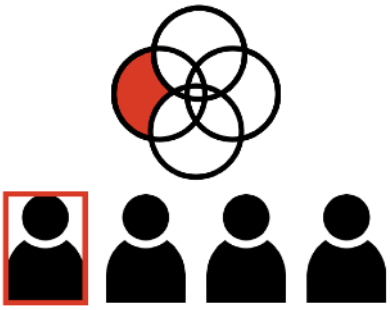


In fact, the closer people are to one another in a social network, the more heavily their datasets overlap. They contain many data points that are literally the same, such as the record of an email exchange between multiple parties, or common photographs of a group. The amount of

such concurrence is higher between people who are close to one another socially. Thus, the closer people are to one another socially, the more heavily their datasets overlap, like this:

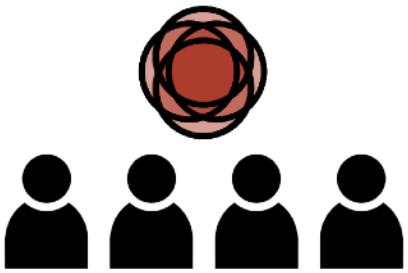


The phenomenon of overlapping datasets means that individuals have much less bargaining power than might be expected. If one person decides they don't like what they are getting in exchange for their data, they can't withhold anything like the entirety of their dataset—because they can't stop others from revealing large swathes of their data. Rather, the data an individual can withhold--and thus the extent of their practical bargaining leverage—is limited to their unique data:



This unique slice, of course, gets smaller as the network grows. And the problems do not stop there. Because, as suggested above, each individual's data actually contains information about other individuals *which those other individuals' datasets do not themselves contain*. Suppose, for example, that nothing in my medical history suggests a high cancer risk. But if many of my family members have had cancer, it is far more likely that I will suffer from it as well. This means that the most heavily overlapping sections of the collective dataset are in fact the most data-rich parts *for each individual*. The middle parts of the Venn diagram are *the most valuable parts*,

which yield the strongest predictions. And yet these are precisely the sections for which no individual can effectively bargain.



This explains why the debate about whether the financial returns to data increase or decrease with scale is not straightforward.[14] Data—especially data about people—has aspects of both increasing and decreasing returns that cannot be easily teased apart.

In many respects, Data Producers are now suffering the worst of both worlds. Their weak ability to defend their data interests seems to reflect a decreasing returns scenario, in which their unique marginal data points constitute their only leverage. Yet, personal data has obvious applications whose value increase nonlinearly with scale, at least over certain unknowable intervals.[15] Businesses collecting data at scale capture the entirety of those rich pockets of value, cutting Data Producers out of the bargain.

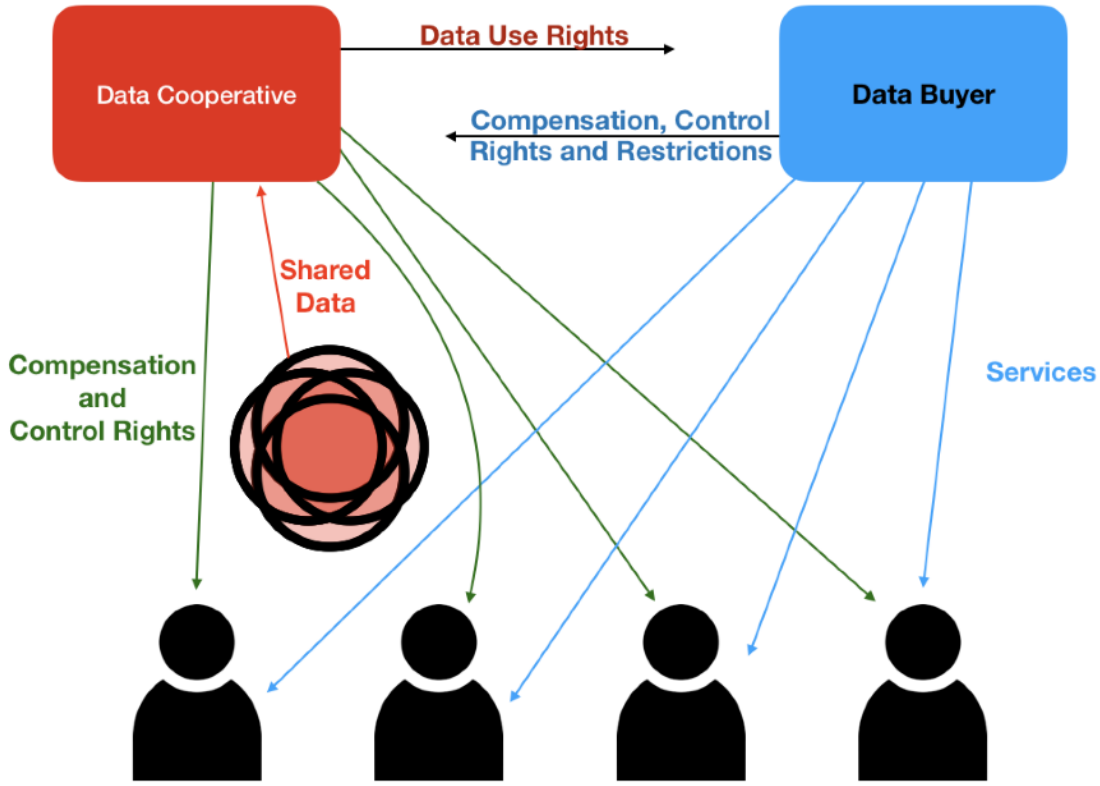
Moreover, the overlapping nature of people's interests in data means that a market in which individuals act as distinct bargaining units will always fail. In essence, individuals infringe the legitimate interests of other individuals whenever they contract bilaterally with a Data Buyer.

A collective bargaining system could squarely address each of these problems by interposing Data Coalitions that take account of their Members' overlapping interests. Below is a sketch of the architecture this legislation envisions:

---

[14] See Google economist Hal Varian's presentation on this issue: http://www.learconference2015.com/wp-content/uploads/2014/11/Varian-slides.pdf; see also see Li, Nirei, Yamana, 2019: https://www.rieti.go.jp/jp/publications/dp/19e022.pdf

[15] Id.



The figure above depicts what collective bargaining through Data Coalitions would look like. By assigning large swathes of data, flowing from many parties, to a Data Coalition with strong fiduciary duties, Data Producers would be able to bargain for the true, collective value of their data.

An Overview of the Proposed Legislation

The Data Relations Board

The Data Freedom Act would create the Data Relations Board, a quasi-judicial administrative body, in order to adjudicate disputes arising under the Act and promulgate rules clarifying it. Modeled loosely on traditional labor relations boards, it would play an important role interpreting the Act and helping it evolve with a changing technological environment.

Defining Data Coalitions

Data Coalitions would be a new class of legislatively defined business entities, either for profit or non-profit, and subject to a strict set of rules governing their operation.

In essence, they would be collective bargaining entities that ordinary natural persons, Data Producers, could interpose between themselves and the businesses that collect or use their

data. The method of this interposition is simple. Data Producers would assign exclusive rights to use all or some of their data to Data Coalitions, thus becoming "Members". Having done this, other businesses ("Data Buyers" or "Non Data Coalition Businesses") would be required to negotiate with the relevant Data Coalition in order to collect, maintain, or commercially exploit the relevant data of those Data Producers. The Data Coalition would thus step into its Members' shoes as an agent to negotiate privacy policies, terms of use, and other data-related contracts with Non Data Coalition Businesses.

A Data Coalition's rights to a Data Producer's data would be defined contractually. For example, Data Producer X might assign to Coalition Y the exclusive right to all interests in the data produced by her web browsing activity. This expansive assignment, having been made and publicly registered, would preclude any third party Z from directly collecting data about X's browsing activity without Coalition Y's permission. In other words, the Act would statutorily shift the enforcement burden from Data Producer X, to third party Z, to respect X's exclusive assignment of rights to Coalition Y.

As mentioned, Data Coalitions would be required to operate according to a strict set of rules and fiduciary duties. These include duties to:

- submit certain decisions to Member votes;
- under certain circumstances, share revenues and control rights with other Data Coalitions;
- "watermark" data transmitted to third parties, so that the third parties may have ready evidence that their data is lawfully obtained;
- transmit a certain portion of its profits to Members;
- treat all members and prospective Members fairly;
- never sell shares of the company to Non Data Coalition Businesses;
- never enter into certain anti-competitive agreements with third parties;
- make all data pertaining to Members available for those Members to port to other Data Coalitions using convenient, industry-standard methods;
- never enter into contractual agreements with Members that exceed six months;
- never sell to third parties a permanent right to use any Member data; and
- negotiate meaningful and proportionate future interests in any products or lines of business created by third parties using Members' data.

Below, several of the key provisions are explained in greater detail.

Democratic Governance of Coalitions

1. *Data Coalitions shall make available to Members a convenient means to submit private votes from time to time.*
2. *Data Coalitions shall allocate at least one-third of the seats on their board of directors or equivalent governing body to representatives chosen by Members, and who shall be up for reelection at least once per year. This requirement shall not apply to Data Coalitions that are sole proprietorships.*

3. *Data Coalitions cannot take certain actions without prior approval by Members, secured through a democratic process. Conversely Data Coalitions must take these actions if Members have demanded them by a democratic process. The actions are:*
    a. *Changes to the Data Coalition's Statement of Purpose.*
    b. *Boycotting a Non Data Coalition Business.*
    c. *Ending a boycott of a Non Data Coalition Business.*
    d. *Entering into or terminating a major agreement with a third party that will materially impact some or all users.*

In order for Data Coalitions to have the leverage to effectively bargain on behalf of large groups of Members, they would need the power to bind Members to decisions with which some Members disagree. Therefore, certain safeguards need to be in place. Not all of those safeguards are in the provision excerpted above--for example, other provisions limit potential harm by requiring Data Coalitions never to permanently sell any Member's data, and forbidding contracts that prevent Members from being bound to a Coalition for more than six months (see draft legislation below).

Nonetheless, just as labor unions must obtain the consent of members before calling a strike, Data Coalitions must obtain democratic Member consent before calling a data boycott that could disrupt Members' lives by cutting off access to private services, or taking other actions that could alter the fundamental bargain between Data Coalitions and Members.

Control and Profit Sharing Between Coalitions

1. *Where two or more Data Coalitions possess concurrent rights to data which is significantly overlapping in its content, and which pertains to Members of the different Coalitions, each of the relevant Data Coalitions has a claim upon the use of such data. They may exercise their rights as follows:*
    a. *The most-restrictive rule governing the use of the data, which is embodied in the Statement of Purpose of a relevant Data Coalition, and where the relevant Members of that Data Coalition and other relevant Data Coalitions who have more-restrictive rules shall total at least 25% of the relevant Members, shall limit the use of the data.*
    b. *Subject to (i), a majority of relevant Members, acting through votes or through negotiating rights delegated to their Data Coalitions, shall have the power to prevent any less-restrictive or less-privacy-preserving uses of the data by any other Data Coalition.*
    c. *All Data Coalitions with relevant Members shall have a proportional right to revenues earned by other Data Coalitions through the use of the data.*

One of the most important possible failure modes for this system of Data Coalitions is a “race to the bottom” dynamic, in which some Data Coalitions could undermine the leverage of others by offering unreasonably favorable terms to Data Buyers.

To see why, imagine a small group of socially-connected Data Producers--such as a family. A majority of the family wishes to maintain a very high standard of privacy, or monetize their data only under extraordinary circumstances, and has joined a Data Coalition that pursues those priorities. However, one troublesome brother has joined a different Data Coalition that readily looks to convert data into income streams.

The troublesome brother might spoil things for the rest of the family. By making his personal data available to paying customers, he divulges much about the rest of the family’s data, such as where they vacation, their approximate level of wealth, their probable tastes in various consumer items, their race, their likely vulnerability to certain diseases, and much more. They therefore cannot maintain their privacy. And, should they wish to sell access to their data, they could not get a fair market price--because a large part of their information could be gotten by proxy, through a deal with the troublesome brother’s Data Coalition.

To prevent this kind of scenario from spoiling the entire scheme, Data Coalitions need to be able to make claims upon one another. The Data Coalition representing the majority of the impacted Data Producers must be able to enjoin the Coalition representing a minority interest from exploiting the overlapping data on more permissive terms. Thus, if a democratically determined majority of Data Producers wish to keep an overlapping dataset private, it must be kept private, even if this impacts multiple Data Coalitions. Moreover, if a majority accepts a certain degree of privacy loss in exchange for payment, the payment must be fairly divided between all Coalitions representing relevant Data Producers.

Notably, these inter-Coalition claims should not be decided on a strictly majoritarian basis. Certain kinds of strong interests--for example, highly sensitive privacy interests--should be able to outweigh even a strong majority interest in monetizing data. Data Coalitions, then, must have clear lines of communication with one another, and a well-developed framework for working together actively to craft equitable solutions. Disputes that inevitably arise between them would be refereed by the Data Relations Board, which would play an important role in developing relevant rules and jurisprudence.

No Permanent Data Alienation; Ongoing Interest Requirements

1. ***Permanent Data Sales Prohibited.*** *Data Coalitions may not permanently sell any data, or rights to use, access, or possess any data to any third party. All agreements to sell data, or rights to use, access, or possess data, must:*
    a. *be time-limited, with a period of no more than one year;*
    b. *require deletion by the third party at the end of the time period;*
    c. *prohibit the third party's maintenance of the data after the time period in any form from which the initial data may be significantly reconstructed; and*
    d. *negotiate a meaningful and proportionate future interest in any products or services depending upon the data, as detailed in [section XYZ below].*
2. ***Requirement to Negotiate Meaningful and Proportionate Ongoing Rights.*** *Where Data Coalitions make agreements permitting third parties to use data to construct algorithms; train machine learning or artificial intelligence technology; build statistical or computational models; or otherwise build any product, service, or tool through the use of the data that will continue to exist after the third party's right to use, access, or possess the original data has expired, the Data Coalition must retain certain ongoing rights. These ongoing rights must:*
    a. *include rights to meaningfully influence or control the present and future uses of such products, services, or tools, and to share in the revenues derived from them; and*
    b. *such rights must be reasonably proportionate, taking into account both the possible value to the third party of the ongoing product, service, or tool, and its possible implications for Members' interests.*

This section of the legislation represents perhaps the largest departure from existing law.

The first provision would forbid any Data Coalition from selling a permanent or absolute right to use or maintain any data obtained from them. Accordingly, all "sales" of data by Data Coalitions would really be time-limited "leases" lasting no more than one year.

This is, in certain respects, the core of the legislation. Without it, the bargaining power of all Data Coalitions would be undermined by a secondary market in which data sold by the least protective Coalition would be resold by its purchaser, thus eliminating the ability of all other Data Coalitions and their Members with an interest in that data to protect it or benefit from it.[16]

---

[16] Data use that preserves differential privacy to a reasonable degree, and/or precludes secondary markets is neither unprecedented nor unfeasible. RIPL.org's platform, which provides research access to sensitive government information, without abridging government's ownership of the data, is just one example.

The second provision, concerning ongoing interests, closes a loophole in the first provision. A crucially important use of data is its use in training machine learning algorithms or artificial intelligence systems. Such systems, which are often highly opaque, can extract and retain much of the use-value from data even after the original data itself has been deleted. This provision requires all Data Coalitions to be cognizant of that reality. It imposes upon them a duty to negotiate “reasonably proportionate” financial and/or control interests in any and all outputs of data, including machine learning algorithms or artificial intelligence systems, even when those outputs outlast the actual data.

Anticipated Objections

Why do people deserve compensation for data that they generate in the ordinary course of their lives? Isn’t most data just “exhaust”?

This is an important argument. However, it seeks to lock in peoples’ present disempowerment with respect to their data.

First, not all of the data we produce looks like “exhaust". Much of it looks instead like creative or productive output that simply falls outside of IP protection. Think, for example, of the intellectual work that sits behind our choices of which Wikipedia articles to read, which books to buy, and which topics to discuss with our friends and colleagues. Hardly valueless, this information constitutes valuable input to large-scale conversations—yet it is now scraped and captured mostly by large companies.

Second, and perhaps more importantly, it is questionable whether any information is truly “exhaust”. The notion of "exhaust" implies "valueless to everyone", but oddly, in the context of data we use it to mean "valueless to its creator but valuable to others”. If someone wants to tap your exhaust pipe, “exhaust” is the wrong word for what it is emitting.

In sum, the appropriation of other people’s work is always exploitative unless accompanied by a fair wage. The argument that it is permissible to appropriate the (data) product of other peoples’ work without paying them "because they were going to produce it anyway” assumes impossible, counterfactual knowledge. It does not stand scrutiny.

Isn’t there a principal-agent problem between Data Producers and Data Coalitions?

In every field where principals give agents special access or sensitive information—such as legal representation, or money management—agents are in a position to exploit principals.

Data Coalitions are no exception. This legislation takes pains to mitigate these inherent conflicts using a mixture of Member “exit and voice”, and hard-coded fiduciary responsibilities.

First, no Data Coalition is permitted to contract with any Data Producer for a period of longer than six months.[17] This combined with strict data mobility requirements[18] means that at least every six months Data Producers have the opportunity to abandon Data Coalitions with which they are not satisfied.

Second, as detailed above, a number of crucial decisions by Data Coalitions must be directly ratified by Member vote.[19]

Third, the legislation erects several rules that combine to incentivize Data Coalitions to grow by adding additional Members--that is, to improve the terms of the bargain--rather than to increase profits by more aggressively monetizing the data of existing Members. First, Data Coalitions that decide to severely restrict new membership are likely to expose themselves to more claims of undermining the interests of other Data Coalitions. Second, Data Coalitions must remit at least 80% of their revenues after costs to Members—except that Coalitions with larger numbers of Members may be permitted to retain a higher portion of revenues. This incentivizes Coalitions to seek growth in Membership numbers, instead of growth in per-Member profits.

Doesn’t this encourage people to accept more private surveillance?

This legislation would increase Data Producers’ leverage to pursue whatever priorities they choose. Some Data Coalitions would likely pursue monetization and seek to sell significant access to Member data. However, businesses seeking to use such data would have to pay for it more dearly than they do today, and Data Producers would receive far more value in exchange.[20]

Other Data Coalitions would prioritize privacy and control interests. Data Producers could readily choose to join those Data Coalitions, and protect their data far more effectively than is currently feasible.

We believe Data Producers must be allowed to sacrifice privacy for money, within certain limits. The legislation restricts only their ability to undermine the privacy or bargaining power of other Data Producers.

---

[17] Data Freedom Act, Section 1(E)(vi).

[18] Data Freedom Act, Section 1(G).

[19] Data Freedom Act, Section 1(F).

[20] Such value would not be limited to cash--it would also include ongoing equity interests. See Data Freedom Act, Section 1(N) on “Meaningful and Proportionate Ongoing Rights”.

Doesn't this commodify data?

This legislation seeks to strike an elegant balance between commodification and other values.

In the present economy, data is already a commodity—and a very dysfunctional one. This legislation, especially in light of the all-important restriction on permanent data sales, decreases the extent to which data may be treated as a pure commodity by erecting barriers before businesses that would seek to cheaply collect and exploit data. Without halting or banning the information trade, it enables individuals and communities to safeguard their data, or sell it much more dearly—even if that means disrupting business as usual for data-harvesting economic actors.

Finally, the restriction on permanent alienation of data by Coalitions should suffice to prove that this legislation does not seek to increase data commodification. One of the hallmarks of commodities is that all-encompassing interests to them may be readily transferred. Here, however, the ability of Data Coalitions to sell "absolute title" to data has been removed. The legislation thus encourages the aggregation of data in forms that make it more valuable, while forbidding it from then being treated as a pure commodity. The aim is to shift power toward now-powerless participants in the data economy—and then to keep it there.

Wouldn't it be simpler to just tax Data Buyers?

A well-designed tax could certainly improve upon the status quo. However, a Data Coalition ecosystem would accomplish several positive things that a new tax regime could not.

First, Data Coalitions would serve as the collective bargainers for large groups of individuals, stepping into their shoes for purposes of negotiating privacy policies, terms of service, and other complex consumer contracts. This would help address the notorious problem of unreadable, incomprehensible "click-wrap" agreements—one of the most troublesome market failures of the digital economy.

Second, Data Coalitions would serve as incentive-aligned, professional advocates for their Members' interests in a complex environment. The assistance of an informed fiduciary, who stands to profit by better serving consumers, could lead to creative solutions balancing privacy, monetization, and other interests. Individuals with limited information and narrow interests, and policymakers attempting to understand the values of entire populations, are both poorly-positioned to devise such creative solutions.

Third, and perhaps most importantly, Data Coalitions would drive a market-based process by which Data Producers efficiently configured themselves into the interest groups that best match their interests. This elaborate sorting of individuals into interest groups is an exceedingly complex problem that governments are ill-equipped to solve. If a government tried, for example, to advocate for all consumers at the same time (e.g., through a tax), then politically less-influential minority interest groups would see their interests overwhelmed by majority interests. A Data Coalition system would uniquely facilitate the emergence of dynamic balance of complex interests.

Wouldn't this increase inequality between people with more and less valuable data?

It is true that this legislation would permit some people to receive more compensation than others for the value of their data. But it is not clear how large these differences would be, or whether they would track existing inequalities.

The primary effect of the legislation, however, would be distinctly egalitarian. Namely, it would convert capital income (enjoyed by the shareholders of companies that exploit the value of data) into labor income (enjoyed by the providers of the data). This would constitute a very real limit on the ability of the wealthy few to capture the value generated by the data economy.

Conclusion

Data, especially data about people, is not a traditional personal asset, because many parties have shared, overlapping legitimate interests in it. Because our present legal framework does not treat data as a shared asset, individuals are unable to vindicate their legitimate interests in controlling its use, profiting from it, or keeping it private.

This legislative proposal aims to erect a reasonable system for managing these shared interests in data. It would establish tightly regulated collective bargaining entities, called Data Coalitions, which would pursue their Members' varying interests from a vastly better bargaining position. It would establish fiduciary and other duties governing those Coalitions. It would require democratic Member control over key aspects of Coalitions' conduct. It would enable Data Coalitions to make special claims against one another to prevent a "race to the bottom" in which some undermined the interests of others. And it would establish a Data Relations Board to adjudicate the complex issues arising under these rules, and to ensure that the framework evolved with the changing technological landscape.

This framework is intended to strengthen the hand of participants in the digital economy who currently have no meaningful leverage behind their efforts to protect their privacy, control the uses of their information, or share in the profits that they co-create. We hope it will be a step in the right direction.

Data Freedom Act -- Draft Legislation

This bill would enact the Data Freedom Act of 2020. It would establish a new class of regulated entity called Data Coalitions, whose purpose is to work on behalf of Data Producers to help them protect their privacy, control how their data is used by others, and receive a share of income generated from data pertaining to them.

The bill would impose certain duties upon Data Coalitions, including a duty to submit certain decisions to Member votes; a duty to "watermark" data transmitted to third parties; a duty to transmit a certain percentage of its per-Member profits to Members; a duty not to sell shares of the company to Non Data Coalition Businesses; a duty under certain circumstances to share revenues and control rights with other Data Coalitions; a duty not to sell to third parties a permanent right to use any Member data; a duty not to enter into certain anti-competitive agreements with third parties; a duty to make all data pertaining to Members available for those Members to port to other Data Coalitions using convenient, industry-standard methods; a duty to limit compensation differences between Members; a duty not to discriminate against prospective Members; a duty not to enter into contractual agreements with Members that exceed a certain duration; and a duty to negotiate meaningful and proportionate future interests in any products or lines of business created by third parties using Members' data.

The bill would impose certain duties on businesses other than Data Coalitions, including a duty to make all the data they hold pertaining to citizens of this jurisdiction available to be ported to Data Coalitions using convenient, industry-standard methods; a duty to negotiate contractual policies relating to privacy and data with Data Coalitions; a duty to refrain from entering into agreements with Members of Data Coalitions that contradict the terms agreed to with their Data Coalitions; and a duty not to retaliate or discriminate against persons for joining Data Coalitions.

The bill would establish a Data Relations Board which would adjudicate disputes arising under the provisions of this bill.

1) **<u>The legislature finds and declares that:</u>**

    a) Powered by relatively recent advances in technology, the data economy has unleashed tremendous productivity, improved the lives of many, and has the potential to further benefit countless individuals, communities, businesses, and fields of endeavor.

b) However, the data economy's rapid development also has eroded individuals' ability to defend certain vital interests, such as their right to privacy. Existing privacy legislation represents an attempt to restore individuals' ability to maintain their privacy, but it has not comprehensively addressed the problems of the data economy.

c) In many cases, when ordinary individuals transmit data to businesses, they either do so unwittingly or because they have no practical choice. It is not possible for most individuals to read and understand the privacy policies that govern their everyday activities, and even if they could read and understand them, it would be practically impossible either to renegotiate those policies or to consistently avoid using services with unsatisfactory ones. Many central aspects of social and economic life cannot be participated in without using certain services, and many individuals do not have a realistic option of foregoing participation in those aspects of social and economic life because of their dissatisfaction with particular services' privacy policies or data use practices.

d) Certain concerns about the consequences of the data economy go beyond privacy. For example, data about individuals and communities now represents a vital ingredient in the provision of goods and services, not only to those individuals and communities but also to third parties. Businesses depending on the sale or use of such data have disrupted large sectors of the economy and gained trillions of dollars in value. Yet the individuals and communities who provide the data, or allow it to be collected, or who are impacted by its surreptitious collection, have not benefited in a proportionate manner from that economic activity.

e) Individuals' data enables their behavior to be affected by advertisers or other third parties armed with sophisticated analyses of their behavioral patterns. Individuals have a legitimate interest in reducing the degree to which third parties can affect their behavior in this way.

f) The highly concentrated and unequal participation in the value generated by data has contributed to high and growing levels of inequality.

g) The paradigm of "personal data" cannot comprehensively address the challenges of the data economy. This is because data is frequently interpersonal. Information pertaining to one person frequently also pertains to other people in their family, community, or network. Therefore, any system formalizing individuals' interests in their data must take into account data's social and interpersonal characteristics.

h) Therefore, it is the intent of the legislature to establish a legislative and regulatory framework within which individuals can effectively work together to defend their legitimate interests. This bill would:

i) Establish a new class of regulated entity called Data Coalitions, to which ordinary individuals ("Data Producers") could assign certain rights to use some or all of their data (thus becoming "Members" of the Data Coalition);
ii) Impose certain duties and responsibilities upon Data Coalitions to prevent abuse and align their incentives with Members;
iii) Impose certain duties on businesses other than Data Coalitions in order to enable Data Coalitions to effectively represent and defend their Members' interests.
iv) Establish a Data Relations Board to promulgate rules and adjudicate disputes arising under the terms of this bill.

2) <u>Data Coalitions:</u>

1. Establishing Data Coalitions

Data Coalitions are established as a new class of business entity with special duties, rights, and features, as defined in this Section.

a. **For Profit or Nonprofit.** A Data Coalition may be organized as any for-profit or non-profit entity, partnership, or sole proprietorship that would otherwise be authorized to do business, and whose form does not prevent it from operating as prescribed in this Section.
b. **Registration and Disclosure Requirement.** Every Data Coalition must register with the Data Relations Board, providing such information as the Board may deem necessary to initially certify and periodically renew its right to operate as a Data Coalition. Further, Data Coalitions must maintain an up-to-date record with the Data Relations Board, which shall be made accessible to the public, sufficient to inform the public of the nature and extent of the rights and interests that each Member has assigned to the Data Coalition.
c. **Independence Requirement.** A Non Data Coalition Business may not own shares or possess any other form of beneficial or control interests in a Data Coalition.
d. **Restrictions on Income From Other Activities.** A Data Coalition may not earn more than 10% of its income in a calendar year from business activities other than representing its Members' data interests. Membership fees and revenue from training courses or other data-related services offered to Members fall within the scope of representing Members' data interests.
e. **Contracts Between Data Coalitions and Members**
    i. **Statement of Purpose.** Every Data Coalition must maintain a clear and concise Statement of Purpose, which shall be incorporated into the contract between a Data Coalition and its Members, and which explains

the essential aims and priorities it pursues on behalf of all of its Members. It shall articulate, among other things, the principles that guide its decisions, and the tradeoffs that it may occasionally make between defending its Members' privacy, monetizing their data, exerting control over downstream uses of their data, and other important Member interests.

ii. **Uniform Contracts.** A Data Coalition must offer the same contract to all Members and prospective Members during the same period of time.

iii. **Limits on Member Compensation Differences Within Coalitions.** Data Coalitions must enact a policy defining maximum differences in the rates of compensation between Members during the same time period. This policy must be susceptible to periodic change through a democratic process.

iv. **Nondiscrimination.** A Data Coalition shall publish clear, non-discretionary membership eligibility criteria, and shall accept as a Member any Data Producer who meets them. No Data Coalition shall discriminate on the basis of race, sex, religion, sexual orientation, national origin. Furthermore, no Data Coalition shall discriminate on the basis of past, present, or future membership in any other Data Coalition, or other anti-competitive grounds. The Data Relations Board shall have broad authority to enumerate new categories of impermissible discrimination on public policy grounds.

v. **Assignment of Negotiating Rights.** Members of a Data Coalition may assign to a Data Coalition a contractually defined licenses to represent their interests relating to some or all of the data that they generate or have generated other than in clear view of a broad public; for example by reaching bilateral contracts or agreements with Non Data Coalition Businesses that do not otherwise conflict with this Section.

vi. **Time Limits for Member Contracts.** No contract between a Data Coalition and a Member shall bind the Member for more than six months.

vii. **Membership in Multiple Data Coalitions.** Data Coalitions and Members may negotiate the terms under which Members shall be permitted to be simultaneous members of multiple Data Coalitions. Data Coalitions may not contractually impede Members' ability to join other Data Coalitions after their Membership has ended, or discriminate or retaliate against prospective Members on the basis of their past, present, or future Membership in other Data Coalitions.

f. **Member Control of Data Coalitions.**

i. Data Coalitions shall make available to Members a convenient means to submit private votes from time to time.
ii. Data Coalitions shall allocate at least one-third of the seats on their board of directors or equivalent governing body to representatives chosen by Members, and who shall be up for reelection at least once per year. This requirement shall not apply to Data Coalitions that are sole proprietorships.
iii. Data Coalitions cannot take certain actions without prior approval by Members, secured through a democratic process. Conversely Data Coalitions must take these actions if Members have demanded them by a democratic process. The actions are:
    1. Changes to the Data Coalition's Statement of Purpose.
    2. Boycotting a Non Data Coalition Business.
    3. Ending a boycott of a Non Data Coalition Business.
    4. Entering into or terminating a major agreement with a third party that will materially impact some or all users.
iv. Data Coalition Members must have a reasonable ability to initiate votes or equivalent democratic processes from time to time, in which Data Coalition policies may be adjusted or other actions may be demanded.

g. **Data Portability Requirement.** Data Coalitions shall make possible convenient, live, two-way, industry-standard programmatic access to all data covered by [existing privacy legislation]. Subject to the Data Producer's agreement with the Data Coalition, as well as to the other provisions of this Section, Data Coalitions shall make possible such programmatic access of a Data Producers' data to other specified Data Coalitions, upon verified request by the Data Producer.
h. **Reasonable Per-Member Profits.** All Data Coalitions shall report their financial information yearly to the Data Relations Board. The Data Relations Board shall ensure that, absent a compelling reason to do otherwise, the Data Coalition is remitting at least 80% of its income after expenses to its Members. Data Coalitions with larger numbers of Members may be permitted, pursuant rules to be promulgated by the Data Relations Board, to remit lower percentages of such income to Members, but in no case less than 65%.
i. **Watermarking Data.** Data Coalitions shall be required to use industry-standard technology to cryptographically "watermark" any Member data that comes into their care, and to subsequently maintain a chain of provenance on all data in their possession, so that all such data may be verifiably traced to its public or Member sources.

j. **Exclusivity.** Data Producers may assign rights to data to more than one Data Coalition. But Data Producers shall not intentionally assign conflicting rights to data to more than one Data Coalition, and Data Coalitions shall not knowingly accept assignment of such rights to data.

k. **Shared Revenue And Control Rights Between Data Coalitions For Overlapping Data.** Where two or more Data Coalitions possess concurrent rights to data which is significantly overlapping in its content, and which pertains to Members of the different Cooperatives, each of the relevant Data Coalitions has a claim upon the use of such data. They may exercise their rights as follows:
    i. The most-restrictive rule governing the use of the data, which is embodied in the Statement of Purpose of a relevant Data Coalition, and where the relevant Members of that Data Coalition and other relevant Data Coalitions who have more-restrictive rules shall total at least 25% of the relevant Members, shall limit the use of the data.
    ii. Subject to (i), a majority of relevant Members, acting through votes or through negotiating rights delegated to their Data Coalitions, shall have the power to prevent any less-restrictive or less-privacy-preserving uses of the data by any other Data Coalition.
    iii. All Data Coalitions with relevant Members shall have a proportional right to revenues earned by other Data Coalitions through the use of the data.

l. **Certain Anti-Competitive Agreements Prohibited.** Data Coalitions are prohibited from entering into agreements with third parties including Non Data Coalition Businesses where the agreement aims to restrict the Data Coalition's ability to do business with, or impede its Members' ability to use the services of, any Non Data Coalition Business or Businesses.

m. **Permanent Data Sales Prohibited.** Data Coalitions may not permanently sell any data, or rights to use, access, or possess any data to any third party. All agreements to sell data, or rights to use, access, or possess data, must:
    i. be time-limited, with a period of no more than one year;
    ii. require deletion by the third party at the end of the time period;
    iii. prohibit the third party's maintenance of the data after the time period in any form from which the initial data may be significantly reconstructed; and
    iv. negotiate a meaningful and proportionate future interest in any products or services depending upon the data, as detailed in [section XYZ below].

n. **Requirement to Negotiate Meaningful and Proportionate Ongoing Rights.** Where a Data Coalition makes an agreement permitting a third party to use its data to construct algorithms; train machine learning or artificial intelligence technology; build statistical or computational models; or otherwise build any

product, service, or tool through the use of the data that will continue to exist after the third party's right to use, access, or possess the original data has expired, the Data Coalition must retain certain ongoing rights. These ongoing rights must:

i. include rights to meaningfully influence or control the present and future uses of such products, services, or tools, and to share in the revenues derived from them; and

ii. such rights must be reasonably proportionate, taking into account both the possible value to the third party of the ongoing product, service, or tool, and its possible implications for Members' interests.

2. Requirements for Non Data Coalition Businesses:

a. **Data Portability Required.** Non Data Coalition Businesses shall make possible convenient, live, two-way, industry-standard programmatic access to all data covered by [existing privacy legislation]. Upon verified request by a Data Producer or Data Coalition, Non Data Coalition Businesses shall make such programmatic access available to a Data Coalition duly designated by a Data Producer.

b. **Good Faith Required.** A Non Data Coalition Business shall have a duty to negotiate in good faith with any Data Coalition. As part of the duty of good faith, a Non Data Coalition Business must permit any Data Coalition to accept terms that are the same in all respects to those it has agreed to with any other Data Coalition.

c. **Retaliation and Discrimination Against Data Coalition Members Prohibited.** Non Data Coalition Businesses shall not, by act or omission, retaliate or discriminate against any Data Producer, whether or not the Data Producer is a current or former customer of the business, by reason of the Data Producer's past, present, or future association with any Data Coalition. Discrimination or retaliation under this provision includes but is not limited to witholding interoperability, erecting burdens, costs, or inconveniences, or any other differential treatment motivated in substantial part to burden any Data Producers by reason of their past, present, or future association with any Data Coalition, or to dissuade Data Producers from associating with Data Coalitions.

d. **Agreements with Members Contradicting Agreements with Data Coalitions Prohibited.** Where a term in a contract between a Data Coalition Member and a Non Data Coalition Business contradicts a valid term in a contract between that Member's Data Coalition and the same Data Coalition Business, the latter term shall control and the former shall be void.

e. **Working With Members of Data Coalitions in the Absence of an Agreement with the Data Coalition.** Where a Non Data Coalition Business learns, through verified notice from a Data Coalition, that a Data Producer is a Member of that Data Coalition, it shall record and/or use no further data from that Data Producer, the rights to which have been assigned to the Data Coalition. If reasonably necessary and non-retaliatory, and reasonable notice is given to the Data Producer, it may cease to do business with that Data Producer, unless and until it has reached an agreement with the relevant Data Coalition. It may not, absent the Data Producer's express consent, delete or alter any data pertaining to that Data Producer, insofar as such data would have been maintained had the Data Producer not joined the Data Coalition.

f. **Reporting Revenues From Data.** Non Data Coalition Businesses shall be required to disclose the source and amount of revenues from the use of or transactions concerning data. The precise requirements of this provision shall be enumerated by the Data Relations Board and where possible shall harmonize with other applicable requirements.

3. Remedies

a. Any Data Producer harmed by a violation of this title by a Data Coalition or a Non Data Coalition Business, or any Data Coalition harmed by a violation of this title by a Non Data Coalition Business, may seek the following remedies by filing an action with the Data Relations Board:
    i. To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per incident or actual damages, whichever is greater.
    ii. Injunctive or declaratory relief.
    iii. Any other relief the Data Relations Board deems proper.
    iv. In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to: the nature and seriousness of the misconduct; the number of violations; the persistence of the misconduct; the length of time over which the misconduct occurred; the willfulness of the misconduct; and the defendant's assets, liabilities, and net worth.
b. A determination pursuant to this Section made by the Data Relations Board shall be appealable once pursuant to a process to be defined by the Data Relations Board, and is appealable thereafter to a civil court.

c. Actions pursuant to this Section may be brought by only if all of the following requirements are met:
    i. Prior to initiating any action for statutory damages on an individual or class-wide basis, a Data Producer or Data Coalition shall provide the defendant 30 days' written notice identifying the specific provisions of this title alleged to be violated. In the event a cure is possible, if within the 30 days the defendant actually cures the noticed violation and provides an express written statement that the violations have been cured and that no further violations shall occur, no action for individual or class-wide statutory damages may be initiated. No notice shall be required prior to a Data Producer or Data Coalition initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If the defendant continues to violate this title in breach of the express written statement provided to the consumer under this section, the Data Producer or Data Coalition may initiate an action against the defendant to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.
    ii. A party bringing an action as defined above shall notify the Attorney General within 30 days that the action has been filed.
    iii. The Attorney General, upon receiving such notice shall, within 30 days, do one of the following:
        1. Notify the consumer bringing the action of the Attorney General's intent to prosecute an action against the violation. If the Attorney General does not prosecute within six months, the consumer may proceed with the action.
        2. Refrain from acting within the 30 days, allowing the consumer bringing the action to proceed.
        3. Notify the consumer bringing the action that the consumer shall not proceed with the action.
    iv. Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other applicable laws.

4) <u>Data Relations Board:</u>

1. This Chapter shall be known as the Data Relations Board.

a. The government establishes a Data Relations Board which shall be independent of any other agency. The Board shall consist of five members appointed in accordance with subdivision (c) and shall conduct its business in accordance with this chapter.
b. Members of the commission shall be individuals with knowledge of, and expertise in two or more of economics, civil rights, data science or machine learning, and privacy, whether by experience or training.
c. Three members shall be appointed by the Governor, with one member each having experience in
    i. academia;
    ii. advocacy on behalf of consumers in the area of privacy, labor, or data rights;
    iii. and the technology industry.
d. One member shall be appointed by the Senate Committee on Rules.
e. One member shall be appointed by the Speaker of the Assembly.
f. Terms of appointment shall be five years and members shall be eligible for reappointment. Members shall hold no other concurrent public office. The Governor shall select one member to serve as chairperson. The Governor may remove members for neglect of duty or malfeasance in office, but no other reason. A vacancy shall not impair the other board members from carrying out their duties, and three members shall constitute a quorum.
g. Each member of the board shall receive a receive a reasonable salary.
h. The board shall be empowered to appoint an executive director who shall serve at the pleasure of the board, and who shall manage various administrative affairs of the board, and appoint other persons to carry out such work as may be necessary to enable the board to perform its duties. The government shall provide adequate resources for the board to carry out its work and adjudicate all matters before it in a timely and rigorous manner.

2. The Data Relations Board is charged with the following responsibilities:

a. To adopt or amend, by a majority of the Board's members, rules and regulations to carry out and effectuate the policies and purposes of this Act, and to govern the procedures of the Board.
b. To hear and resolve disputes arising under the Data Freedom Act of 2020 as a court of first impression, and to publicly communicate the reasoning behind its decisions in a manner that allows members of the public to act with a clear and up-to-date understanding of the board's interpretation of the Data Freedom Act of 2020.

c. To maintain a registry of Data Coalitions and decide contested matters relating to their registration or deregistration.
d. To hold hearings, subpoena witnesses, administer oaths, take the testimony or deposition of any person, and, in connection therewith, to issue subpoenas duces tecum to require the production and examination of any Data Coalition or non Data Coalition business's records pertaining to its compliance with the Data Freedom Act of 2020 or other matters falling under the board's jurisdiction.
e. To investigate charges of violations of the Data Freedom Act of 2020, and take any action and make any determinations in respect of these charges or alleged violations as the board deems necessary to effectuate the policies of the Data Freedom Act of 2020.
f. To bring an action in a court of competent jurisdiction to enforce any of its orders, decisions, or rulings, or to enforce the refusal to obey a subpoena. Upon issuance of a complaint charging that any business or person has engaged in a violation of the Data Freedom Act of 2020, the board may petition the court for appropriate temporary relief or restraining order.
g. To delegate its powers to any member of the board or to any person appointed by the board for the performance of its functions, except that no fewer than two board members may participate in the determination of any ruling or decision on the merits of any dispute coming before it.
h. Within its discretion, to conduct studies relating to questions of data, technology, economics, and related matters, which may be necessary to help it carry out its duties. The board shall report to the Legislature by October 15 of each year on its activities during the immediately preceding fiscal year. The board may enter into contracts to develop and maintain research and training programs designed to assist individuals and businesses in the discharge of their rights and responsibilities under the Data Freedom Act of 2020.

5) <u>For purposes of this title:</u>

1. "Data" means personal information as defined in [other relevant authority].
2. "Data Coalition" means any entity acting as a Data Coalition under the terms of this title.
3. "Member", as of a Data Coalition, means a Data Producer who has contractually assigned to certain rights to use the Data Producer's data to that Data Coalition.
4. "Non Data Coalition Business" means any sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that does business in the jurisdiction, and that satisfies one or more of the following thresholds:
    a. Has annual gross revenues in excess of twenty-five million dollars ($25,000,000).

   b. Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
   c. Derives 50 percent or more of its annual revenues from selling consumers' personal information.
5. "Data Producer" means a natural person who is a resident of the jurisdiction, as defined in [relevant authority].
6. Data that "pertains" to a Data Producer means data that has been lawfully assigned to a Data Coalition by that Data Producer.
7. "Agreement" means any contract or other agreement, whether written or unwritten, and whether express or implied.
8. "Control Right" means an enforceable contractual right to restrict, prohibit, or determine the uses of certain data.
9. A rule governing a use of data is more "restrictive" than another if, in order to preserve privacy, confidentiality, or control of the data, it would preclude the use of the data, where the other rule would not.