Data Leverage: A Framework for Empowering the Public in its Relationship with Technology Companies

Nicholas Vincent
Northwestern University
nickvincent@u.northwestern.edu

Hanlin Li
Northwestern University

Nicole Tilly
Northwestern University

Stevie Chancellor
Northwestern University

Brent Hecht
Northwestern University

ABSTRACT

Many powerful computing technologies rely on data contributions from the public. This dependency suggests a potential source of leverage: by reducing, stopping, redirecting, or otherwise manipulating data contributions, people can influence and impact the effectiveness of these technologies. In this paper, we synthesize emerging research that helps people better understand and action this *data leverage*. Drawing on prior work in areas including machine learning, human-computer interaction, and fairness and accountability in computing, we present a framework for understanding data leverage that highlights new opportunities to empower the public in its relationships with technology companies. Our framework also points towards ways that policymakers can augment data leverage as a means of changing the balance of power between the public and tech companies.

CCS CONCEPTS

• **Human-centered computing → Collaborative and social computing theory, concepts and paradigms**.

KEYWORDS

data leverage, data strikes, data poisoning, conscious data contribution

ACM Reference Format:
Nicholas Vincent, Hanlin Li, Nicole Tilly, Stevie Chancellor, and Brent Hecht. 2020. Data Leverage: A Framework for Empowering the Public in its Relationship with Technology Companies. In *Proceedings of (forthcoming) 2021 Conference on Fairness, Accountability, and Transparency (preprint).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

This preprint is an early working draft of a paper that will be presented at the 2021 Conference on Fairness, Accountability, and Transparency (FAccT 2021).

1 INTRODUCTION

In August, 2020, the most valuable five technology companies were valued at $7 trillion [95]. This valuation is driven in part by highly complex models that use data generated by everyday users to recommend content, rank search results, and provide many other services [24, 98, 131]. More generally, powerful and economically productive technologies used by many companies rely on data generated by large, diverse groups of people to fulfill user needs [7, 24, 98] and drive decision making [25].

The reliance of powerful technologies on what scholars have called "data labor" [7, 98, 118] presents an enormous opportunity for the public to gain more power in its relationships with technology companies. Data labor is the multitude of data-generating actions people engage in when they use computing technologies. By tapping this source of power, the public could demand changes related to many issues of great concern [5, 58, 71], such as diminished privacy [23, 39], discriminatory technology [5, 43, 71, 92], labor rights [56, 94], and economic inequality between tech operators and data producers [24, 98, 121]. Armed with knowledge about how these technologies work and tools to action this knowledge, the public could potentially interfere with recommender systems, search engines, image classifiers, and other technologies for the purpose of demanding that tech companies address these issues.

In this paper, we provide a definition of the concept of "data leverage" and discuss how the concept can be made operational. Simply put, data leverage refers to influence that members of the public have over tech companies because important computing technologies rely on the public's data contributions. Data leverage includes power achieved by *harming* data-dependent technologies, such as "data strikes" [118] and "data poisoning attacks" [44], as well as power achieved by *helping* to improve alternative technologies and thereby create increased competition [117]. The concept of data leverage seeks to capture an emergent theme in fields that help to make up the FAccT community, including human-computer interaction (HCI), social computing, society and technology studies (STS), and areas of machine learning (ML) research that seek to advance fairness, justice, and a human-centered perspective (e.g. [5, 7, 19, 28, 51, 82, 117, 118, 120]). Our goal with this paper is to make clear the connections between the research happening in these fields and, through the concept of data leverage, show that the proverbial whole of this framework is greater than the sum of its disciplinary parts. In doing so, our framework highlights substantial untapped potential for future research and policy interventions that support and amplify data leverage, and can thereby further empower the public in its relationship with technology companies.

The primary contributions of this work are to (1) define data leverage at a high level, (2) provide a framework of potential "data levers" and discuss prior work that has advanced our understanding of these levers, (3) outline an initial assessment of strengths and weaknesses of each data lever in the public's "tool belt", and (4) highlight how the data leverage concept provides research and policy opportunities. Critically, many lines of research have the

preprint, 2021, online
2020. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

potential to amplify data leverage, and using data leverage as a lens raises the stakes for the impact of these research areas. We pay particular attention to factors that might facilitate the use of data leverage (e.g. policy interventions) or that prevent groups from exerting data leverage (drawing on the literature on "non-use" of technology) [11–14, 75, 102, 128]).

1.1 Background and Definitions

We first present a formal definition of data leverage. While aiming to be comprehensive, our definitions are working definitions. Data leverage is an emergent topic in a rapidly advancing field, and we aim to advance and open the discussion around data leverage, not conclude it.

- *Leverage*: a person or group's *power* to influence an organization. A group with substantial leverage over a particular organization could make demands and possibly enact change.
- *Data leverage*: power derived from intelligent technologies' dependence on user-generated data. Data leverage becomes available if an external group influences an organization by threatening to engage in, or directly engaging in actions that harm an organization or help competitors.
- *Data levers*: the specific types of actions individuals or groups engage in to exert data leverage. For instance, data strikes, one of the data levers we discuss below, operate by cutting off the flow of data to tech companies.

2 RELATED WORK

In this paper, we argue that data leverage is a useful framework across numerous computational fields and related research areas. However, there are no central definitions of this emergent idea given the areas' interdisciplinary nature. In this section, we situate data leverage relative to the FAccT literature, and then discuss four additional areas that contribute to the idea of data leverage.

2.1 Data Leverage and FAccT Research

Data leverage very directly builds on calls from the FAccT community to conduct research that explicitly addresses the issues of fairness, justice, and human-centeredness of computing systems [5, 28, 32]. Responding to this call, researchers have made great progress on technical solutions to issues of fairness [32]. However, technical solutions are limited in their ability to address unfair ML technologies (see e.g. [5, 19, 43, 47]). Most directly, Abebe et al. recently called for computing researchers to reflect on their approaches toward social change and laid out a series of "roles" for computing research [5]. We believe engaging with data leverage is one way for computing research to respond to this call.

Kulynych et al. propose that "Protective Optimization Technologies" (POTs) could help those affected by algorithmic systems address the negative impacts of these systems [71]. More generally, the framework of POTs suggests a way to contest or subvert optimization technologies, perhaps adopting techniques from data poisoning (which we further address below) [71, 115]. The POTs concept was influential on our data leverage framework: we see data leverage and POTs as highly synergistic concepts, and in many cases a particular example of a POT enables people to exert data leverage.

2.2 Data as Labor

Data leverage is heavily informed from work that claims that "data is labor". Building on Posner and Weyl [98], Arrieta Ibarra et al. argue that data should be considered labor, not an "exhaust" emitted in the process of using technology, and we must rethink the economic relationships underlying the collection and use of data [7]. The relationship between data-generating laborers and the companies that benefit from this data is very asymmetric. Not only do people have very little knowledge of — let alone agency over — how their data contributions are used, but the economic winnings from powerful intelligent technologies are reaped by tech companies [98]. To mitigate this inequality, Posner and Weyl called for the formation of "data unions", which can collectively negotiate with technology companies on behalf of data laborers [98].

The discussion around data labor has inspired computational work that aims to understand data labor, for instance by measuring the value of various types of public data to online platforms [68, 87, 119, 120]. Researchers have explored ways to measure the economic value of data, for instance looking at the relationship between Wikipedia — the product of data contributions from the public — and a variety of real-world economic outcomes such as tourism and investment. [60, 129]. Building on the data as labor concept, several papers have explored early concepts of data leverage, investigating how people might withhold or redirect their data labor to force a data-dependent organization to change its practices[117, 118].

2.3 Insights for Data Leverage from Technology Use/Non-Use

Data leverage concepts are heavily informed by work from HCI and STS that focuses on the notions of technology use and "non-use", and the spectrum of tech use in between.

Selwyn and Wyatt called attention to the need to understand those who do not use new technologies [105, 128]. Selwyn, in particular, documents that some people engage in an ideological refusal to use certain technology "despite being able to do so in practice." [105] Further calls to study non-use in HCI have been amplified in the years since [10, 102], ultimately arguing that non-use as a concept is highly relevant to HCI and STS [102].

Use and non-use exist on a spectrum [14, 128]. Different forms of use and non-use depends on a person's decision to engage with a technology and the social and technical decisions that take place if and when a user decides to depart [12, 22, 104]. Critically, many factors can influence non-use, such as exclusion [128], social capital [75], socioeconomic factors [11, 14], and so anyone seeking to use data leverage to broadly empower the public must contend with these factors. Attempts to support data leverage could exclude or disproportionately benefit certain groups following existing patterns in how technology excludes and benefits these groups.

One theme that consistently comes up in non-use literature is that it is not easy for people to refrain from use when it comes to products that have some benefit in their life, even if the benefit(s) come with a host of drawbacks. Challenges include the struggles of "relapsing" and "withdrawing" from social media [12, 13], along with issues related to social media profiles as a form of public presentation [74]. Recently, Saxena et al. reviewed many of these typologies of non-use [103]. In one salient example, Brubaker et al. study individuals who left Grindr, a geo-social dating app, - "even among those who deleted the app, only a minority tried to close their accounts or remove personal data...[putting them] in a paradoxical position of thinking they have left while their profile - or data - continues on." [22]

On the other hand, the very same non-use literature also suggests that users already engage in protest actions for reasons relating to privacy, data use, addiction, and other reasons [12, 13, 82, 112]. Relatedly, focusing on the case of bioethics, Benjamin makes the case that broad support of “informed refusal” provides a means to developing a justice-oriented paradigm of science and technology [17]; in other words, there already exist non-users who engage in informed refusal. Finally, Casemajor et al. and Portwood-Stacer argue that non-participation in digital media can be an explicitly political action[27, 97].

In closely related work, Li et al. conducted a survey to better understand "protest users", people who stop or change their use of tech to protest tech companies[82]. The survey results suggested that there is a large number of people interested in protest use: half of respondents were interested in becoming protest users of a company, and 30% were already engaged in protest use.

Overall, understanding non-use is enormously helpful in understanding the potential impact of data leverage. As we will further discuss below, data leverage raises the stakes of non-use: in some potential cases, giving non-users more power and in other cases excluding non-users.

2.4 Insights for Data Leverage from ML Research

The ability for data leverage to influence organizations assumes that actions by data contributors can alter the performance of a data-dependent system, e.g. an ML system. Two particularly relevant areas of research are those that answer questions around (1) the effectiveness of adversarial attacks on data-dependent systems and (2) the relationship between a system’s performance and changes to underlying data.

There is an enormous literature that considers the case of adversaries attempting to attack ML systems [9, 18, 29, 44, 53, 73, 76, 79, 89, 96, 108, 109, 111]. As early as 2004, authors began to explore the “shilling” of recommender systems, or “lying” to a system so that a system recommends certain products [73]. In early work on adversarial ML Barreno et al. developed a taxonomy of attacks on ML systems [9]. They focus particularly on attacks in which an adversary "mis-trains" a system, a subcategory of attacks called *data poisoning*. These attacks have been studied against many ML systems [9, 18, 96, 108, 109, 111]. Accordingly, much work has been done on counteracting shilling (e.g. [29, 53, 76, 89]), which may be of concern to groups who want to use shilling to exert data leverage.

Recently, researchers have explored advanced "data poisoning" techniques that use sophisticated methods to optimally harm ML systems [44, 79], which can be much more effective than unsophisticated attacks (like providing random or average ratings to many items [73]).

This literature has a highly symbiotic relationship with research on data leverage: conceptually, data leverage builds on adversarial ML and data poisoning, and at the same time data leverage further raises the stakes of this already high-stakes domain: data poisoning is not just relevant to issues of security and privacy, but is relevant to the power relationships between users and tech companies. Even data poisoning research that takes a strictly security-oriented perspective could be used by those seeking to wield (or defend against) data leverage. Future work that directly builds on connections between adversarial ML and data leverage that we highlight in this paper will be a particularly fruitful direction for future work.

Finally, there is a large literature that seeks to understand the relationship between the amount of training data a model has access to and model performance (e.g. [30, 36, 45, 59]). This literature is highly relevant to data leverage, which involves manipulating the training data available to an organization. In general, many authors have found diminishing returns of additional data across many contexts and algorithms. Some work has studied how to scale datasets in light of diminishing returns [20].

2.5 Insights for Data Leverage from Data Activism

Last, this paper joins the literature on data activism in STS in exploring how the public’s efforts may change practices of the technology industry. Data activism is a relatively new form of civic participation in response to big data’s pervasive role in public life [8]. The most relevant initiative in this space is the open data movement, which aims to democratize information that is currently only accessible to the state or businesses [54]. For example, Baack studied an open data project in Finland and highlighted the intermediary role of data activists between the public and operators of intelligent technologies [8].

Currently, data activism encompasses a variety of practices that aim to affect technology design, development, and deployment. Data leverage can be seen as a subset of data activism with a specific focus on empowering the public to influence the performance of data-dependent technologies through data. Milan and Van der Velden provided a typology of data activism that further illustrated the various specialized activities in this space — proactive and reactive data activism [88]. Proactive data activism refers to activists directly influencing software development or databases through open source projects or collaborating with institutions. On the other hand, reactive data activism is activists acting against data-collecting entities through adversarial behaviors such as employing encryption tools. As seen below, data leverage falls into both types of data activism but focuses on directly influencing the flow of data.

More broadly, prior work on data activism has unveiled a rich space for research to guide practices of data activism [33], to which this paper directly contributes. In particular, Lehtiniemi and Ruckenstein called for "linking knowledge production to data activism practice" to gain a comprehensive understanding of data’s role in the public sphere [78]. Data leverage research is well positioned to answer this call. Equipped with the knowledge and expertise to understand data's role in computing, researchers can provide the public with valuable information to identify and employ effective data leverage practices.

3 DATA LEVERAGE FRAMEWORK

In this section, we establish our framework of data leverage. For each of our three data levers, we define the data levers and any variants, grounded in past work that could be reinterpreted within the proposed framework of data leverage. Next, we provide practical examples of each data lever and describe the likely factors that will control how effective a given lever is. Table 1 includes a short summary of the data levers, their definitions, and several examples of each.

3.1 Data Strikes

Data strikes involve withholding or deleting data to reduce the amount of data an organization has available to train and operate data-dependent technologies. Although the term data strike is relatively new, the concept builds on the well-studied practices of stopping or changing technology use as a form of protest, as discussed above in Related Work. For instance, groups have participated in prominent boycotts against companies like Facebook and Uber [52, 106]. In another example, people use ad blocking software, depriving companies of data about the success of their ad placements [26].

3.1.1 Data Strikes Variants. The most basic form of a data strike is a *withholding-based data strike.* In some cases, users can withhold data by stopping their technology use, reducing their use, or continuing to use a technology with anti-data collection privacy-protection tools (e.g. tracking blockers [85]). However, in jurisdictions where regulation allows users to delete their past data (e.g. based on laws like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) [101, 123]), users can also engage in *deletion-based data strikes.* The effectivness of such strikes will depend on how well regulations are able to force companies to regularly retrain their intelligent technologies (so as to "clean out" weights learned using now-deleted data).

Data strikes can be further categorized based on coordination. Data strikes are certainly possible without serious coordination: for instance, people seeking to start an informally-organized data strike might broadly call for other users to delete as much as they are able or willing and recruit additional participants in a snowball-like fashion. Given the success of hashtag activism [63] and other forms of online collective action that operate without central leadership [84], this kind of a data strike is plausible. However, "targeted" [9] data strikes have the potential for a small group of data strikers to achieve disproportionate impact [118]. Following Barreno et al.'s definition of "targeted" attacks on ML systems, in a targeted data strike, organizers might encourage participants to delete specific data points or recruit particularly valuable participants. For example, data strikers could try to reduce performance for a specific genre of movie recommendations, while leaving performance for other genres untouched. Leaders might also recruit specific users to join their data strike – power users have disproportionate influence on systems [40, 126, 127] and withholding or deleting their data may be more impactful.

3.1.2 What Do Data Strikes Look Like in Practice? Data strikes have pragmatic grounding in the non-use literature mentioned above. An individual that chooses to use a platform less frequently or avoid a feature of that platform reduces the amount of data they provide. In this way, a person's choices about use and non-use affect much how data that person generates. There exists a number of HCI studies in the use and non-use domain that provide empirical examples of what could be conceptualized as data strikes such as Facebook non/use and Twitter non/use (e.g. [11–14, 104]. In other work, non-use and abstention from social media is sometimes conceptualized as both performative and political [97].

Privacy and surveillance research also lends itself to uncovering specific privacy-focused behaviors that can be seen as data strikes. For example, one easy way to attack tracking technologies is to use anti-tracking browser extensions to limit or remove the amount of data online trackers collect [26, 82, 85]. Studies about algorithm transparency also provided early evidence suggesting that people engage with data strike-like behaviors as a result of dissatisfaction with the opaqueness of algorithmic systems such as stopping producing reviews for review platforms [41, 42]. Additionally, research on online communities presented case studies of both Reddit moderators and community members striking by disabling and leaving their communities, respectively [86, 91].

3.1.3 How can Data Strikes be Effective? The effectiveness of a data strike can be captured in terms of what impact it could have on a data-dependent system. For machine learning, a data strike can be evaluated in terms of the data that "goes missing", and the extent to which that data is crucial to a model's performance. Does the missing data noticeably degrade a system's performance, move a classifier's decision boundary (or hyperplane, etc.) in a meaningful way, or otherwise change the outputs of some system?

To understand the effectiveness of data strikes, researchers and strike leaders might look to research on data scaling and learning curves, which describes the relationship between ML performance and the amount of data available for training (e.g. [30, 36, 45, 59]). Findings from this literature could be used to produce a best guess as to the effectiveness of a strike. Some early work has taken methods from this literature to more explicitly simulate how effective data strikes might be in certain contexts [118]. If researchers have shown a model needs a certain number of observations in its training set to be effective (e.g. [30]), data strike organizers could use that research to guide their strike (i.e. to aim for a certain number of participants).

In summary, data strikes are a data lever available to anyone who can withhold or delete their data. Behaviors studied in HCI and privacy include data strikes: refusing to use a technology, abandoning a technology, and other ways people change their technology use in protest all allow people to exert data leverage.

3.2 Data Poisoning

A data poisoning attack is an adversarial attack that inserts inaccurate or harmful training data into a data-dependent technology, thereby mis-training the model [9]. Whereas data strikes harm performance by reducing the amount of available training data, data poisoning aims to get technology operators to train models using data that was created with the intention of thwarting the operator

Table 1: A list of data levers, short definitions for each, and several examples.

Data Lever	Short Definition	Examples
Data Strike	withhold or delete data	Quit using a platform; install privacy tools
Data Poisoning	contribute harmful data	Fake data in user profile; click randomly; manipulated images
Conscious Data Contribution	contribute data to competitor	switch to a new search engine; transfer old photos to new platform

of that system. A user might engage in simple forms of data poisoning: for instance, someone who dislikes pop music might use an online music platform to play a playlist of pop music when they step away from their device with the intention of "tricking" a recommender system into using their data to recommend pop music to similar pop-hating users. A classic example of data poisoning is the coordinated effort and long-standing presence of a sexually explicit Google search result returned for former U.S. Senator Rick Santorum's name in the 2000s [49]. Another familiar example is the use of fake reviews to promote certain products [73].

3.2.1 Data Poisoning Variants. The notion of data poisoning is familiar to the ML community through adversarial ML (see e.g [9, 18, 96, 108, 109, 111]) and obfuscation (see e.g. [23, 61]).

There are many ways an individual, acting alone, can engage in data poisoning. Techniques for obfuscation described by Brunton and Nissenbaum are all accessible means of data poisoning for individuals. For instance, users might trade accounts (drawing on Brunton and Nissenbaum) or fill in some parts of their profile with fake information [31]. As another example, past work discusses an attack that involves following particular Twitter users to throw off Twitter's profiling [90]. These approaches are generally available to an individual acting alone.

The distinction between coordinated data poisoning and uncoordinated attacks is important. In general, most ML literature assumes some degree of coordination behind an attack. Typically, adversarial ML papers frame data poisoning as a contest between a single attacker and a defender/victim. In a coordinated data strike, however, the "single attacker" is an organized collective.

Coordinated poisoning efforts, like the Santorum "Google Bombing" example above, could achieve substantially outsized effects compared to uncoordinated efforts: a very small group of effective data poisoners could seriously damage an ML system.

To identify specific subcategories of coordinated data poisoning, we can look to taxonomies from researchers in adversarial ML to see what knowledge an attacker requires and what specific systems are vulnerable to attacks [9, 96]. In general, to execute a coordinated variant of a data poisoning attack, it will be necessary to find the appropriate technique for a particular technology in the adversarial ML literature.

Shilling, a form of data poisoning, is an action individuals may take to bolster the credibility of untrustworthy data technologies or producers [53, 73, 76]. Unlike the other poisoning examples, this type of data leverage serves to manipulate the algorithm to more favorably recommend a product that does not deserve it. We liken this to the oft-repeated idiom of putting "lipstick on a pig". Relatedly, to support schilling, data poisoners might manipulate data-driven systems that identify and remove fraudulent or false reviews [83, 93].

So far, we focused heavily on literature that specifically studies ML, but data leverage extends beyond ML system. As with other forms of data leverage, data poisoning applies more generally to any data-dependent technology. Tahmasebian et al. provide a taxonomy and discussion of data poisoning attacks against crowdsourcing "truth inference" systems [113].

3.2.2 What Does Data Poisoning Look Like in Practice? Almost any platform is vulnerable to deceptive interactions from users, and there are numerous ways to engage in data poisoning in practice. In the wild, there have been many cases of data poisoning attacks directly performed by users. For example, a restaurant owner, unsatisfied with Yelp's handling of his restaurant's reviews, explicitly invited customers to provide one-star ratings in exchange for a discount [34]. In the context of the gig economy, drivers sometimes provide false information about their availability status so Uber's and Lyft's assignment algorithms would work in their favor [77].

In a simple example, users might use technology in a deceptive manner, by watching videos they dislike, searching for content they are not interested in, or lying about their personal attributes. They might even use deception-support tools like the location-spoofing software conceptualized by Van Kleek et al. to engage in "computationally-mediated pro-social deception" [116].

By combining findings and tools from HCI and ML, more complex forms of data poisoning may be possible. Users might employ HCI tools like browser extensions (as in [61, 80]) or web platforms (as in [130]) that help them participate in coordinated data poisoning with sophisticated means of producing poisoned data taken from ML work [44, 109]. Imagine a data poisoning platform, modeled on existing social computing platforms [70] that provides users with bespoke poisoned data that they can use. Users could upload images poisoned with pixel-level manipulation to spoof image recognition systems, or take suggestions of specific content to interact with that will fool recommender systems.

Data poisoners might even take inspiration from research on adversarial evasion attacks [109]. Recent work has developed tools to help users protect their own images from facial recognition systems (i.e. "evade" the system [96]). Shan et al. show that their tool, Fawkes, can imperceptibly alter images so that state-of-the-art facial recognition cannot recognize the altered images [109]. Such tools could easily be adapted for data leverage purposes.

3.2.3 How can Data Poisoning be Effective? We expect poisoning-based data leverage to require a high level of technical literacy to use, but have very high potential impact in cases in which data poisoning works. Fundamentally, data poisoners are engaging in a contest with data poisoning counter-researchers. This means any data poisoning technique runs the risk of becoming outdated — if a company's data scientists find a solution or potentially share it with others, the public might lose leverage [109, 111]. This means that progress in adversarial ML could actually end up reducing the public's data leverage, in which case non-poisoning data levers would become more important.

There are several reasons to believe data poisoning could be a powerful source of data leverage. Recent work on sophisticated data poisoning suggests that very small amounts of poisoned data (e.g. using less than 1% of a training set in [48], using 3% of a training set in [111]) can change the outputs of a classifier. Even unsophisticated data poisoning by a majority of users could so completely poison a dataset as to make it unusable.

Another interesting outcome of data poisoning is its potential conversion to a data strike. In the case in which an organization can detect and delete poisoned data with great accuracy, data poisoning reduces to a data strike. Sometimes, detectable data poisoning could be used to replicate a data strike. For instance, search engine users could use data poisoning tools like obfuscation AdNauseum [61] — which clicks all ads in a user's browser — to effectively make their ad click data useless, forcing the search engine operator to delete it.

Data poisoning can have sociotechnical effects and consequences, given its inherent ties to deception. Data poisoning efforts necessarily influence the technical system, and in places where users interact with algorithmic outputs, poisoning can have larger consequences on other users and their use of a site. Consider someone who lies on a dating site, a surprisingly common phenomenon [55, 114]. The user may accidentally poison their own recommendations for possible partners and make others' dating experience worse off.

A critical part of research that treats data poisoning as a form of data leverage will be navigating ethical and legal challenges around when data poisoning is acceptable, building off a variety of work along these lines (e.g. [23, 48, 109, 116]). Whether a particular instance of poisoning is interpreted to be political dissidence or sabotage depends on the society where it is enacted and on case-by-case specifics. Data poisoning efforts could be so severe that existing laws around computer abuse or fraud may come into play, such as the United States' Computer Fraud and Abuse Act (CFAA) or laws around fraud [2, 62]. At what point does data poisoning cross the line of intentional misuse and abuse?

To summarize, data poisoning attacks are another source of data leverage, requiring people to provide data-dependent technologies with modified and deceptive data. Data poisoning has high potential, but runs the risk of being nullified by advances in data poisoning defense or legislation. Like data strikes, data poisoning attacks stand to benefit from research findings and tools.

3.3 Conscious Data Contribution

The above tactics operate by harming, or threatening to a harm, an organization's technologies. However, there are cases in which harmful tactics may be ineffective or undesired — perhaps users do not have the regulatory support needed to delete past data [122], or a new technique for detecting poisoned data foils their poisoning attack. Additionally, in contexts where harmful tactics are undesired because an organization's technologies may actively provide benefits to others (e.g. imagine an ML model that is well known to improve public health outcomes), individuals may wish to avoid data levers that harm those technologies.

"Conscious data contribution" (CDC) provides a promising alternative to harm-based data leverage. Instead of deleting, withholding, or poisoning data, people give their data to an organization that they support [117] with the goal of using the increased competition as a source of leverage. A particularly exciting aspect of CDC is that while small data strikes struggle because of diminishing returns, CDC by a small group of users takes advantage of diminishing returns: a small group can have an outsized effect. We return to this point later in our assessment of data levers.

CDC is related to the "data donation" concept explored in the context of data ethics [99], and in some cases participation in human computation or crowdsourcing systems [100] could qualify as CDC . People using CDC for data leverage are similar to people engaging in "political consumption" [69], but instead of voting with their wallet, they are voting with their data.

3.3.1 CDC Variants. Variants of CDC closely mirror variants of data strikes because CDC in a sense mirrors data strikes — where data strikes take, CDC gives. Here, we discuss variants of CDC that involve giving new data to an organization, variants that involve transferring historical data, as well as the difference between coordinated and uncoordinated CDC.

The easiest form of CDC is to simply start using another technology with the intention of producing useful data for the organization that operates the technology, by joining a new platform or downloading an alternative app. Sometimes, these CDC campaigns may also involve a data strike if a user moves from one platform to another, as is the case in abandoning Google and moving to DuckDuckGo. In other words, cases in which people move from one technology to another incorporate both a data strike and CDC.

In jurisdictions in which companies allow users to download their data in a portable and accessible manner, users could engage in CDC by making a large contribution of historical data to an organization. Realistically, the degree of data portability needed to engage in CDC would likely come about through data portability laws [1]. Many services already allow users to download or otherwise access some of their data contributions, although how useful these data downloads are to other companies remains to be seen [64].

While coordinated data strikes and data poisoning might seek to hurt a particular aspect of some system, coordinated CDC has the potential to enhance specific aspects of a technology's capabilities. In a coordinated CDC campaign, organizers might instruct participants to donate specific types of data, or organizers might seek out specific people to join a campaign, in an effort to focus on contributions towards a specific goal. For instance, in the recommendation context, CDC leaders might seek out comedy movies fans to contribute data to a comedy movie recommender, instead of trying to solicit data about every movie genre.

CDC is relatively unexplored compared to data poisoning and data strikes, and has interesting intersections with incentives. "Data markets" give users the ability to sell their data to companies in an open market, [6, 65]. While data markets allow users to exert some degree of data leverage by giving them choices about to whom they will sell data, people may be forced to prioritize their personal economic incentives over attempts to gain leverage. Data markets run into issues around the fact that many organizations can use the same data, and the fact that any data with a social component often has information about more than one person [6, 16, 66]. The concept of donating data as a form of leverage is also related to crowdsourcing, human computation, and social computing: under our definition, people who choose to contribute data to protein-folding games are also engaging in a form of CDC [38], with the potential to exert leverage against other organizations interested in protein folding.

It may be possible to engage in CDC in which contributions involve telling a company which old observations to ignore (or downweight). Recommender system researchers have shown that allowing users to filter/delete their old data could actually improve recommendations [124]. This can be seen as a counterpart to data poisoning: instead of generating damaging data, users might clean up data they produced in the past that is now creating undesirable outcomes.

3.3.2 What Does CDC Look Like in Practice. As mentioned above, providing data to human computation technologies, crowdsourcing systems, and user-generated content platforms is often a form of CDC because users are aiming to increase the performance of these technologies relative to their competitors. For example, in 2015, due to the lack of support from Reddit administrators for moderators, community members migrated to alternative platforms such as Voat and Snapzu [91]. In doing so, these users performed an act of CDC that explicitly supported Reddit's competitors. Moreover, because of the participatory nature of technologies that involve human computation, crowdsourcing, and user-generated content, an individual user's CDC action may further lead to people in the user's social network engaging with CDC and thereby achieve greater impact on these technologies[46, 72].

However, CDC actions are not always directly visible because data generated by the public are sometimes only accessible to developers and operators of technologies, e.g. log data and advertising data. Nonetheless, various research initiatives have sparked interests that can be seen as CDC in support of research for social good. For example, volunteers in Silva et al.'s study contributed data about their Facebook political ads to researchers for monitoring and auditing purposes [110].

3.3.3 How can CDC be Effective? CDC has a lower barrier to entry than data strikes and data poisoning, because it is possible to engage in CDC without completely quitting use of an existing technology. Despite this advantage of CDC, a critical question for CDC will be whether "helping a competitor" actually exerts any leverage on the original party. For instance, a group of CDC users might be able to seriously improve the ML technologies of a small new start-up. However, even with improved performance, other factors like platform lock-in, challenges in switching, etc. might prevent the start up from seriously competing with the original target of leverage, thus reducing the chance that the original target changes their behaviors or practices. In other words, the existence of a competitor may be an unreliable source of leverage. Of course, in some cases, standing up a viable competitor that has better practices (e.g. better privacy policy, does not deploy harmful technologies, revenue sharing with users) could be an achievement it its own right.

Like data strikes, a key factor regarding the effectiveness of CDC will be the degree of participation. The more people that participate in CDC, the more powerful it will become, and the general degree of effectiveness might be estimated from ML findings. A critical distinction between data strikes and CDC is that while small data strikes may struggle to escape the flat, diminishing portion of ML learning curves, CDC by a small group can actually provide a huge boost to ML performance. We expand on this comparison in the following Assessment section.

In other words, estimating the success of a particular CDC campaign will require combining findings from ML, HCI, and perhaps even collective action. This synthesis is promising direction for future work.

To summarize, CDC allows users to exert data leverage by making contributions to organizations they wish to support, who can compete with the original target of data leverage. CDC has a low barrier to entry and laws or tools that support the transfer of data will make CDC even easier to engage in. CDC also can benefit from the same ML findings that drive data strikes: by understanding the relationship between ML performance and data, those seeking to wield CDC might target their contributions to maximally help improve ML performance.

4 ASSESSING DATA LEVERS

In this section, we expand on our three categories of data leverage through comparison, describing axes that evaluate strengths and weaknesses of each data lever: the *barrier-to-entry* to use a data lever, how *ethical and legal considerations* might complicate the use of a data lever, and finally the *potential impact* of each data lever. Table 2 contains a brief summary of the key points from this section.

4.1 Barriers to Entry

In general, CDC has the lowest barrier to entry of the data levers we identified because it does not require stopping or changing the use of existing technologies, which prior work indicates can be challenging because of sociotechnical factors (e.g. [12, 13, 104]). For CDC, a person can continue using existing technologies operated by an organization against which they want to exert leverage while providing data to a competitor of the target organization [66, 117]. The main challenges here are regulatory and technical: do laws help people move their data [1], and do tools exist to make data transfer realistic? For instance, in the case of transfer-based CDC, it must be practical for users to download or transfer their data, and for other organizations to use that data.

Next, data strikes have a medium barrier to entry: they may disrupt the use of online platforms, but do not always entirely force a user to stop using them like a traditional boycott. For instance, a user who relies on Facebook to communicate with distant family members could stop engaging with sponsored content on Facebook but continue messaging their family member. An Amazon user might continue buying products, but stop leaving ratings and reviews. Like we mention above, prior work has found a number of barriers to completely stopping the use of online technologies [13, 82, 104], including lost social connections, lack of alternatives, etc. An important downside of data strikes is that they hurt the

Table 2: Summary of key points from our assessment of data levers. See Section 4 for detailed discussion.

Data Lever	Barriers to Entry	Legal and Ethical Considerations	Potential Impact
Data Strike	*moderate*: -non-use is challenging -hurts participating users -need for privacy tools	*lower*: -need privacy laws to delete data -harming tech may be undesirable	*moderate*: -small group has small effect -large group can have huge impact
Data Poisoning	*higher*: -time/effort/bandwidth costs -may require ML knowledge -may require extra coordination	*higher*: -potentially illegal -harming tech may be undesirable -inherently deceptive	*moderate*: -small group can have huge effects -if caught, "reduces" to a strike -constant arms race
Conscious Data Contribution	*lower*: -can continue using existing tech	*moderate*: -make harmful technologies better -privacy concerns of sharing data	*moderate*: -small group can have large effects -large group faces diminishing returns

performance of technologies for participating users: by cutting off data contributions, an individual reduces their own ability to benefit from a system. The effect of a data strike will almost always be most pronounced on the strike participants [118]. We emphasize that, to some degree, data strikes are already happening, but stand to benefit from explicit coordination around strike activities, e.g. suggestions about tools to employ or platforms to avoid.

Finally, data poisoning likely has a high barrier to entry, requiring users to go out their way to create convincing poisoned data. Even indiscriminate data poisoning, which can be performed without special tools (e.g. by interacting with content you dislike), requires serious effort. Sophisticated poisoning might require advanced tech skills, using scripts and browser extensions to generate carefully crafted poisoned data like pixel-level modification of images. Thus, it will be important to consider findings relating to the public's web skills and digital literacy [57], and to consider how users understand data-dependent technologies, e.g. following work on folk theories of algorithms [35].

Additionally, all three data levers have differential access based on the bandwidth and Internet infrastructural resources. Data strikes are likely the least limited by bandwidth. However, where Internet infrastructure is limited, striking may be challenging if the goal is to strike against a singular Internet provider (like Facebook Free Basics [107]). In countries where the Internet is easy to access and has relatively high bandwidth caps, poisoning data by letting music stream for hours or actively manipulating multimedia does not impact access to the web. In contrast, in places where Internet access is limited [37], poisoning data may be difficult if not impossible.

Because data poisoning has the highest barrier-to-entry, it likely is the data lever at highest risk of exacerbating existing inequalities. The people most positioned to perform data poisoning attacks are ML researchers, technologists, and those with high internet skills, an already relatively privileged group. Nonetheless, these groups could use this privilege for good (there is precedent of tech worker organizing [3]).

Specific data leverage campaigns may differ in their coordination needs, with higher coordination raising the barrier to entry. In theory, large-scale data leverage is possible without formal organization: recent boycotts using Twitter hashtags is one real-world example [63]. However, certain data levers require coordinated effort among a group to see impact, e.g. deleting or manipulating specific data points to alter ML outputs [44].

4.2 Legal and Ethical Considerations

There are complex intersections of legal and ethical considerations for data leverage techniques. Beginning with data strikes, withholding-based data strikes require almost no regulatory support as users can simply cease using platforms (keeping in mind the differential barrier to entry concerns discussed above), and privacy laws [123] and privacy tools [23] can make it possible to engage in withholding-based data strikes without quitting a technology. Data levers that require agency over historical data (i.e. deletion-based data strikes and CDC using historical data) require regulatory support to ensure that (1) companies actually delete data and (2) companies are not "data laundering" by retaining model weights trained on old data. Many companies opt not to give users the option to delete past data to preserve their business interests. Examples of relevant legislation include right to be forgotten legislation and data portability regulations [1, 123].

The legality of data poisoning is likely to remain an open question, and interdisciplinary work between computer scientists and legal scholars will be critical to understand the legal viability of data poisoning of different types and in different jurisdictions. Brunton and Nissenbaum discuss at length the ethics of obfuscation, and their arguments apply directly to the use of data levers. Participants must contend with the potential dishonesty and waste of data poisoning, and the potential downstream effects of harm-based data leverage. There are many potential harms that stem from poisoning a system that blocks hate speech or helps make medical diagnoses. But simply switching to CDC is no panacea: many technologies, while profitable or useful to organizations, are harmful to certain groups and society more broadly. Examples of potentially harmful technologies include discriminatory facial recognition systems, credit scoring systems, psychometric profiling, and more (see e.g. [71] for a detailed list of examples, and [5] for additional discussion).

CDC has two legal and ethical challenges specific to its mechanisms as a data lever. First, there is the potential that data contributions might help a harmful technology and second, there is the potential that data contributions by one person might violate the privacy of other people, as data is rarely truly "individual" [6, 16].

We hypothesize that data strikes will face fewer legal and ethical challenges than other data levers. The basic actions of data strikes (deleting and withholding data) can be justified purely on a privacy-oriented or personal-preference basis. CDC is generally also easy to justify, though CDC participants must weigh the potential downsides discussed above. Finally, data poisoning is the most complex form of leverage to justify ethically and legally.

4.3 Potential Impact

Data strikes and data poisoning harm data-dependent technologies, while CDC improves the performance of a data-dependent technology that can then compete with a target technology. As such, we can measure potential impact in terms of performance improvement/degradation, as well as any downstream effects (e.g. performance degradation leads to users leaving a platform). Ultimately, we are interested in how likely a data lever is to successfully change an organization's behavior.

One relevant finding from prior work is how data strikes interact with diminishing returns of data. In general, ML performance exhibits diminishing returns: a system can only get so accurate. As such, when an organization accumulates a large amount of data and begins to receive diminishing returns from additional data, they are not very vulnerable to small data strikes. Most technologies using big data are robust to the inclusion of any one individual in the training data [67, 121]. To a company with billions of users, a small data strike simply may not matter. Large data strikes, on the other hand, could be hugely effective.

The potential impact of data poisoning is huge: a large-scale data poisoning attack could render a dataset completely unusable. This approach is also appealing from a bargaining perspective: a group could poison some data contributions, and make some demand in return for the "antidote". However, the enormous research interest in detecting data poisoning means that the would-be poisoners face a constant arms race with researchers. In the worst case scenario, they will be caught, their poisoned data deleted, and the end effect will be equivalent to a data strike.

CDC campaigns, which improve technology performance, operate in the opposite direction of data strikes. Small-scale CDC could be very high impact: echoing the Pareto rule, about 20% of the users of a system could help a competitor get around 80% of the best-case performance [117]. This could be done quickly and effectively with a coordinated effort of power users. On the other hand, once returns begin to diminish, the marginal effect of additional people engaging in CDC begins to fall.

Data markets in particular are an untested complement to CDC. On one hand, the infrastructure for data markets would make CDC substantially easier: if people can easily sell their data to competing buyers, they can factor issues of leverage into their selling decisions. At the extreme, data markets could support large-scale collective bargaining around data. On the other hand, there are major concerns around privacy and the economic outcomes of data markets [6, 65], and there exists an obvious concern that economic incentives could outweigh data leverage concerns and create new ethical issues.

Given the current evidence, we believe that all the data levers we described above have a place in the toolbelt of those seeking to change the relationship between tech companies and the public. A critical challenge for data leverage researchers will be identifying the correct tool for a specific job: given the technologies a target organization uses, a realistic estimate of how many people might participate in data leverage, and knowledge about the resources available to participants, which data lever is most effective?

5 DISCUSSION

Our goal is for this paper to motivate interest in data leverage as a valuable framework in fields like FAccT, HCI, ML, and STS. To this end, we discuss key takeaways from our data leverage framework. First, we discuss the key question of who might expect to benefit from data leverage, and highlight how data leverage might backfire. Next, we summarize key opportunities for researchers, particularly those working in or around FAccT topics. Finally, we summarize opportunities for policy that can amplify and augment data leverage.

5.1 Who Does Data Leverage Benefit?

Who stands to benefit from data leverage is a question of critical concern: researchers interested in studying, supporting, or amplifying data leverage to reduce inequalities must contend with unequal access to data leverage. We expect inequalities in access to data leverage to mirror known patterns in access to technology, and other sources of power more generally. However, our framework suggests that data poisoning and CDC in particular might allow small groups to have outsized and disproportionate impacts. A group of users with needs not currently met by existing technologies might engage in mass CDC to support a competitor to existing tech companies. In another scenario, a small but highly coordinated group might benefit from sophisticated data poisoning techniques that require coordination and knowledge, but not mass participation. Critically, researchers can play an active role by developing tools and promoting policy that distributes data leverage.

5.2 Data Leverage and Commons Data

An important data leverage case to consider is data leverage exerted against organizations that provide "commons" (broadly construed) datasets (e.g. Wikipedia, OpenStreetMap) and datasets that, while technically privately owned, effectively act like a "commons" for research (e.g. Reddit, public Twitter posts). By manipulating commons data sources, it may be possible to exert data leverage against any organization drawing on that particular dataset. Many such resources are enormously influential in ML research — and more broadly, in socio-technical research spanning computer science and social science [4, 15, 21].

By impacting a commons dataset, people can impact any technologies that are "downstream" from that dataset. Whether a given change is helpful or harmful depends on the technology. A concerted effort to vandalize Wikipedia might have harmful downstream impacts on a variety of ML systems (notably, vandalism has appeared humorously in some prominent Google search results [125]). However, the ability to make use of commons datasets may be gated by capital. A salient example is that of GPT-3, OpenAI's high profile language model that used training data from Wikipedia and Reddit, among other sources [21]. The immense amount of computing resources needed to train GPT-3 means that only organizations with enormous resources can benefit from data labor that improves Wikipedia and Reddit. This creates potentially complex dynamics: while an attack on Wikipedia data could harm numerous organizations, improvements to Wikipedia data could disproportionately help organizations with the capital to train models like GPT-3. These exact dynamics warrant further investigation, as they also may impact whether data leverage could lead to a computing paradigm in which power is distributed more broadly.

5.3 Can Data Leverage Research Backfire?

We have presented data leverage as a means to empower the public to address growing concerns around computing systems that exacerbate inequalities and create negative societal outcomes, and we assume issues around access to data leverage can be addressed or mitigated. However, it seems possible that research, tools, and policy intended to help data leverage achieve these goals could in fact do the opposite, and instead empower groups to perpetuate inequalities and achieve socially harmful outcomes. For instance, hate groups take advantage of "data voids" in search engines to insert hateful content and influence model development [50]. Why wouldn't these groups also try to use data leverage tools for similar ends?

There is no clear answer to this problem, but there are steps that data leverage researchers can take to avoid a "backfire" outcome. When designing tools to support data leverage, designers might consider heuristic preventative design from Li et al. [80]. When possible, designers would try to make harmful uses of a technology more challenging. For instance, a data poisoning tool might only help users poison certain types of images known to be important to a particular company or technology and prevent access to others.

We expect data leverage to have the aggregate effect of distributing heavily-concentrated power more so than aggregating power, and therefore tend to help more than harm. Still, planning to address the ways in which data leverage may backfire should be a top priority for the field going forward.

5.4 Key Research Opportunities for Data Leverage

The data leverage concept presents exciting research opportunities for many fields. By studying data leverage, researchers in FAccT, ML, HCI, and STS have unique opportunities to amplify data leverage.

Data leverage presents a new way to externally pressure corporate change. Most relevant to the FAccT community, this might involve exerting leverage so that a tech company stops the use of a harmful algorithm [71], or pushing for new economic relationships between data contributors and AI operators in which the benefits of AI are shared more broadly [98]. This enables researchers to more actively pursue pro-social research roles and goals [5].

Next, there is enormous potential to study machine learning systems with data leverage in mind. Using simulations, future work could build a catalog of results that activists could draw on to make predictions, such as "if we get x participants to engage in a data strike against technology y, we can expect to bring down accuracy of technology by $z\%$, which will likely be enough to encourage company c to make the changes we are demanding". As data leverage becomes more mainstream, there may also be opportunities to study real-world data strikes and data poisoning attacks and answer questions such as: What is the actual effect of real-world data levers on data-dependent systems? What are the downstream effects on revenue, user retention, actual changes in company behavior, etc.?

The data levers mentioned above point to several design opportunities for computing researchers. Future work could build upon the collective action literature and develop tools to coordinate data strikes or data poisoning. For example, because collective action's progress is often opaque to individual participants and thereby negatively impacts their engagement, future work may adopt tactics from prior work on boycott-assisting technologies and display the impact of the public's data strike or poisoning (e.g. this technology has lost 3% of data) [80]. Such tools could also consider automatic data strikes or data poisoning, similar to AdNauseam Howe and Nissenbaum, to lower the barrier to entry for the public.

In addition to data strikes and poisoning, the research community may also support CDC by addressing data compatibility and portability issues across platforms and technologies. User-generated data are often highly context-dependent. For example, ratings for the same restaurant or hotel may vary significantly across review platforms [41, 81]. Directly transferring data from one technology to another as an act of CDC may run into compatibility issues and even negatively affect the latter's performance. Researchers could support development of software or tools that automatically translate one technology's data into another technology's schema to ensure CDC's success.

5.5 Key Policy Opportunities for Data Leverage

There are many data levers that are not available to the public without regulatory support. As such, data leverage research should be deeply engaged with policy by highlighting high-impact regulations that are especially likely to amplify data leverage and address negative impacts.

Following directly from our assessment of data levers above, we suggest a variety of ways policy can support data leverage:

- Data portability laws will directly enhance CDC, enabling users to contribute data they helped generate in the past.
- Right-to-delete laws will enhance data strikes, assuming these laws also account for the possibility that companies might "launder" deleted data in model weights.
- Transparency laws that make data collection more apparent may help foster broader support for data leverage movements.

We note that these policy suggestions are generally aligned with policy framed around privacy. This suggests a potential "win-win" situation, in which policy supports consumer privacy and enhances data leverage.

6 CONCLUSION

In this paper, we have presented the concept of data leverage and developed a framework for using data leverage to give the public more influence over technology companies. Drawing on a variety of research areas, we described and assessed data levers available to the public. We highlighted key areas where researchers and policymakers can amplify leverage and work to ensure data leverage distributes power more broadly than the status quo.

REFERENCES

[1] 2018. Art. 20 GDPR – Right to data portability | General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-20-gdpr

[2] 2020. 18 U.S. Code § 1030 - Fraud and related activity in connection with computers. https://www.law.cornell.edu/uscode/text/18/1030 [Online; accessed 7. Oct. 2020].

[3] 2020. Tech Workers Coalition. https://techworkerscoalition.org [Online; accessed 6. Oct. 2020].

[4] 2020. Wikipedia:Academic studies of Wikipedia - Wikipedia. https://en.wikipedia.org/w/index.php?title=Wikipedia:Academic_studies_of_Wikipedia&oldid=971074694 [Online; accessed 29. Sep. 2020].

[5] Rediet Abebe, Solon Barocas, Jon Kleinberg, Karen Levy, Manish Raghavan, and David G Robinson. 2020. Roles for computing in social change. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 252–260.

[6] Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar. 2019. *Too much data: Prices and inefficiencies in data markets*. Technical Report. National Bureau of Economic Research.

[7] Imanol Arrieta Ibarra, Leonard Goff, Diego Jiménez Hernández, Jaron Lanier, and E Weyl. 2018. Should We Treat Data as Labor? Moving Beyond 'Free'. *American Economic Association Papers & Proceedings* 1, 1 (2018).

[8] Stefan Baack. 2015. Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society* 2, 2 (2015), 2053951715594634. https://doi.org/10.1177/2053951715594634 arXiv:https://doi.org/10.1177/2053951715594634

[9] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D Joseph, and J Doug Tygar. 2006. Can machine learning be secure?. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. 16–25.

[10] Ames Morgan G. Brubaker Jed R. Burrell Jenna Dourish Paul Baumer, Eric PS. 2014. Refusing, Limiting, Departing: Why We Should Study Technology Non-Use. In *CHI EA '14: CHI '14 Extended Abstracts on Human Factors in Computing Systems*. 65–68.

[11] Eric PS Baumer. 2018. Socioeconomic Inequalities in the Non use of Facebook. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.

[12] Eric PS Baumer, Phil Adams, Vera D Khovanskaya, Tony C Liao, Madeline E Smith, Victoria Schwanda Sosik, and Kaiton Williams. 2013. Limiting, leaving, and (re) lapsing: an exploration of facebook non-use practices and experiences. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3257–3266.

[13] Eric PS Baumer, Shion Guha, Emily Quan, David Mimno, and Geri K Gay. 2015. Missing photos, suffering withdrawal, or finding freedom? How experiences of social media non-use influence the likelihood of reversion. *Social Media+ Society* 1, 2 (2015), 2056305115614851.

[14] Eric PS Baumer, Shion Guha, Patrick Skeba, and Geraldine Gay. 2019. All Users are (Not) Created Equal: Predictors Vary for Different Forms of Facebook Non/use. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–28.

[15] Jason Baumgartner, Savvas Zannettou, Brian Keegan, Megan Squire, and Jeremy Blackburn. 2020. The pushshift reddit dataset. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 14. 830–839.

[16] Omri Ben-Shahar. 2019. Data Pollution. *Journal of Legal Analysis* 11 (2019), 104–159. Publisher: Narnia.

[17] Ruha Benjamin. 2016. Informed refusal: Toward a justice-based bioethics. *Science, Technology, & Human Values* 41, 6 (2016), 967–990. Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[18] Battista Biggio, Blaine Nelson, and Pavel Laskov. 2012. Poisoning attacks against support vector machines. *arXiv preprint arXiv:1206.6389* (2012).

[19] Reuben Binns. 2018. Fairness in machine learning: Lessons from political philosophy. In *Conference on Fairness, Accountability and Transparency*. 149–159.

[20] Michael Bloodgood and Chris Callison-Burch. 2010. Bucking the trend: large-scale cost-focused active learning for statistical machine translation. In *Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics*. Association for Computational Linguistics, 854–864.

[21] Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeffrey Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. 2020. Language Models are Few-Shot Learners. arXiv:cs.CL/2005.14165

[22] Jed R Brubaker, Mike Ananny, and Kate Crawford. 2016. Departing glances: A sociotechnical account of 'leaving'Grindr. *New Media & Society* 18, 3 (2016), 373–390.

[23] Finn Brunton and Helen Fay Nissenbaum. 2015. *Obfuscation: a user's guide for privacy and protest*. MIT Press, Cambridge, Massachusetts.

[24] Erik Brynjolfsson and Andrew McAfee. 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.

[25] Erik Brynjolfsson and Kristina McElheran. 2016. The rapid adoption of data-driven decision-making. *American Economic Review* 106, 5 (2016), 133–39.

[26] Ceren Budak, Sharad Goel, Justin Rao, and Georgios Zervas. 2016. Understanding Emerging Threats to Online Advertising. In *Proceedings of the 2016 ACM Conference on Economics and Computation (EC '16)*. ACM, New York, NY, USA, 561–578. https://doi.org/10.1145/2940716.2940787 event-place: Maastricht, The Netherlands.

[27] Nathalie Casemajor, Stıfmmode\acutee\elseé\fiphane Couture, Mauricio Delfin, Matthew Goerzen, and Alessandro Delfanti. 2015. Non-participation in digital media: toward a framework of mediated political action. *Media, Culture & Society* 37, 6 (May 2015), 850–866. https://doi.org/10.1177/0163443715584098 Publisher: SAGE Publications Ltd.

[28] Stevie Chancellor, Eric PS Baumer, and Munmun De Choudhury. 2019. Who is the" Human" in Human-Centered Machine Learning: The Case of Predicting Mental Health from Social Media. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–32.

[29] Paul-Alexandru Chirita, Wolfgang Nejdl, and Cristian Zamfir. 2005. Preventing shilling attacks in online recommender systems. In *Proceedings of the 7th annual ACM international workshop on Web information and data management*. 67–74.

[30] Junghwan Cho, Kyewook Lee, Ellie Shin, Garry Choy, and Synho Do. 2015. How much data is needed to train a medical image deep learning system to achieve necessary high accuracy? *arXiv preprint arXiv:1511.06348* (2015).

[31] Max Cho. 2011. Unsell Yourself—A Protest Model Against Facebook. *Yale Law & Technology* (2011).

[32] Alexandra Chouldechova and Aaron Roth. 2020. A snapshot of the frontiers of fairness in machine learning. *Commun. ACM* 63, 5 (2020), 82–89.

[33] Nick Couldry and Alison Powell. 2014. Big data from the bottom up. *Big Data & Society* 1, 2 (2014), 2053951714539277.

[34] Zachary Crockett. [n.d.]. *The restaurant owner who asked for 1-star Yelp reviews*. https://thehustle.co/botto-bistro-1-star-yelp/

[35] Michael A. DeVito, Jeremy Birnholtz, Jeffery T. Hancock, Megan French, and Sunny Liu. 2018. How People Form Folk Theories of Social Media Feeds and What It Means for How We Study Self-Presentation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173694

[36] Thomas G Dietterich and Eun Bae Kong. 1995. *Machine learning bias, statistical bias, and statistical variance of decision tree algorithms*. Technical Report. Technical report, Department of Computer Science, Oregon State University.

[37] Michaelanne Dye, David Nemer, Laura R Pina, Nithya Sambasivan, Amy S Bruckman, and Neha Kumar. 2017. Locating the Internet in the Parks of Havana. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3867–3878.

[38] Christopher B Eiben, Justin B Siegel, Jacob B Bale, Seth Cooper, Firas Khatib, Betty W Shen, Barry L Stoddard, Zoran Popovic, and David Baker. 2012. Increased Diels-Alderase activity through backbone remodeling guided by Foldit players. *Nature biotechnology* 30, 2 (2012), 190–192.

[39] Michael D. Ekstrand, Rezvan Joshaghani, and Hoda Mehrpouyan. 2018. Privacy for All: Ensuring Fair and Equitable Privacy Protections *(Proceedings of Machine Learning Research)*, Sorelle A. Friedler and Christo Wilson (Eds.), Vol. 81. PMLR, New York, NY, USA, 35–47. http://proceedings.mlr.press/v81/ekstrand18a.html

[40] Farzad Eskandanian, Nasim Sonboli, and Bamshad Mobasher. 2019. Power of the Few: Analyzing the Impact of Influential Users in Collaborative Recommender Systems. In *Proceedings of the 27th ACM Conference on User Modeling, Adaptation and Personalization*. 225–233.

[41] Motahhare Eslami, Kristen Vaccaro, Karrie Karahalios, and Kevin Hamilton. 2017. " Be Careful; Things Can Be Worse than They Appear": Understanding Biased Algorithms and Users' Behavior Around Them in Rating Platforms.. In *ICWSM*. 62–71.

[42] Motahhare Eslami, Kristen Vaccaro, Min Kyung Lee, Amit Elazari Bar On, Eric Gilbert, and Karrie Karahalios. 2019. User attitudes towards algorithmic opacity and transparency in online reviewing platforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.

[43] Virginia Eubanks. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

[44] Minghong Fang, Neil Zhenqiang Gong, and Jia Liu. 2020. *Influence Function based Data Poisoning Attacks to Top-N Recommender Systems*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3366423.3380072

[45] Rosa L Figueroa, Qing Zeng-Treitler, Sasikiran Kandula, and Long H Ngo. 2012. Predicting sample size required for classification performance. *BMC medical informatics and decision making* 12, 1 (2012), 8. https://link.springer.com/article/10.1186/1472-6947-12-8 Publisher: Springer.
[46] David Garcia, Pavlin Mavrodiev, and Frank Schweitzer. 2013. Social resilience in online communities: The autopsy of friendster. In *Proceedings of the first ACM conference on Online social networks*. 39–50.
[47] Timnit Gebru. 2019. Oxford Handbook on AI Ethics Book Chapter on Race and Gender. *arXiv preprint arXiv:1908.06165* (2019).
[48] Jonas Geiping, Liam Fowl, W. Ronny Huang, Wojciech Czaja, Gavin Taylor, Michael Moeller, and Tom Goldstein. 2020. Witches' Brew: Industrial Scale Data Poisoning via Gradient Matching. arXiv:cs.CV/2009.02276
[49] Tarleton Gillespie. 2017. Algorithmically recognizable: Santorum's Google problem, and Google's Santorum problem. *Information, communication & society* 20, 1 (2017), 63–80.
[50] Michael Golebiewski and Danah Boyd. 2019. Data voids: Where missing data can easily be exploited. *Data & Society* (2019).
[51] Ben Green. 2018. 'Fair' Risk Assessments: A Precarious Approach for Criminal Justice Reform. In *5th Workshop on fairness, accountability, and transparency in machine learning*.
[52] Rebecca Greenfield, Sarah Frier, and Ben Brody. 2018. NAACP Seeks Week-Long Facebook Boycott Over Racial Targeting. *Bloomberg.com* (Dec. 2018). https://www.bloomberg.com/news/articles/2018-12-17/naacp-calls-for-week-long-facebook-boycott-over-racial-targeting
[53] Ihsan Gunes, Cihan Kaleli, Alper Bilge, and Huseyin Polat. 2014. Shilling attacks against recommender systems: a comprehensive survey. *Artificial Intelligence Review* 42, 4 (2014), 767–799. Publisher: Springer.
[54] Michael Gurstein. 2011. Open data: Empowering the empowered or effective data use for everyone? *First Monday* 16 (02 2011). https://doi.org/10.5210/fm.v16i2.3316
[55] Jeffrey T Hancock, Catalina Toma, and Nicole Ellison. 2007. The truth about lying in online dating profiles. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 449–452.
[56] Kotaro Hara, Abigail Adams, Kristy Milland, Saiph Savage, Chris Callison-Burch, and Jeffrey P Bigham. 2018. A Data-Driven Analysis of Workers' Earnings on Amazon Mechanical Turk. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 449.
[57] Eszter Hargittai. 2005. Survey measures of web-oriented digital literacy. *Social science computer review* 23, 3 (2005), 371–379.
[58] B Hecht, L Wilcox, JP Bigham, J Schöning, E Hoque, J Ernst, Y Bisk, L De Russis, L Yarosh, B Anjum, and others. 2018. It's time to do something: Mitigating the negative impacts of computing through a change to the peer review process.
[59] Joel Hestness, Sharan Narang, Newsha Ardalani, Gregory Diamos, Heewoo Jun, Hassan Kianinejad, Md Patwary, Mostofa Ali, Yang Yang, and Yanqi Zhou. 2017. Deep learning scaling is predictable, empirically. *arXiv preprint arXiv:1712.00409* (2017).
[60] Marit Hinnosaar, Toomas Hinnosaar, Michael E Kummer, and Olga Slivko. 2019. Wikipedia matters. *Available at SSRN 3046400* (2019).
[61] Daniel C Howe and Helen Nissenbaum. 2017. Engineering Privacy and Protest: A Case Study of AdNauseam.. In *IWPE@ SP*. 57–64.
[62] Kate Mathews Hunt. 2015. Gaming the system: Fake online reviews v. consumer law. *Computer law & security review* 31, 1 (2015), 3–25.
[63] Sarah J Jackson, Moya Bailey, and Brooke Foucault Welles. 2020. *# HashtagActivism: Networks of Race and Gender Justice*. MIT Press.
[64] Ross James. 2020. How to use Google Takeout to download your Google data - Business Insider. *Business Insider* (Jan 2020). https://www.businessinsider.com/what-is-google-takeout
[65] Ruoxi Jia, David Dao, Boxin Wang, Frances Ann Hubis, Nick Hynes, Nezihe Merve Gürel, Bo Li, Ce Zhang, Dawn Song, and Costas J Spanos. 2019. Towards Efficient Data Valuation Based on the Shapley Value. In *The 22nd International Conference on Artificial Intelligence and Statistics*. 1167–1176.
[66] Charles I Jones and Christopher Tonetti. 2019. *Nonrivalry and the Economics of Data*. Technical Report. National Bureau of Economic Research.
[67] Pang Wei Koh and Percy Liang. 2017. Understanding Black-box Predictions via Influence Functions. In *International Conference on Machine Learning*. PMLR, 1885–1894. http://proceedings.mlr.press/v70/koh17a
[68] Pang Wei W Koh, Kai-Siang Ang, Hubert Teo, and Percy S Liang. 2019. On the accuracy of influence functions for measuring group effects. In *Advances in Neural Information Processing Systems*. 5254–5264.
[69] Sebastian Koos. 2012. What drives political consumption in Europe? A multi-level analysis on individual characteristics, opportunity structures and globalization. *Acta Sociologica* 55, 1 (March 2012), 37–57. https://doi.org/10.1177/0001699311431594
[70] Robert E Kraut, Paul Resnick, Sara Kiesler, Moira Burke, Yan Chen, Niki Kittur, Joseph Konstan, Yuqing Ren, and John Riedl. 2012. *Building successful online communities: Evidence-based social design*. Mit Press.
[71] Bogdan Kulynych, Rebekah Overdorf, Carmela Troncoso, and Seda Gürses. 2020. POTs: protective optimization technologies. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 177–188.
[72] Shamanth Kumar, Reza Zafarani, and Huan Liu. 2011. Understanding User Migration Patterns in Social Media.. In *AAAI*, Vol. 11. 8–11.
[73] Shyong K Lam and John Riedl. 2004. Shilling recommender systems for fun and profit. In *Proceedings of the 13th international conference on World Wide Web*. 393–402.
[74] Cliff Lampe, Nicole B. Ellison, and Charles Steinfeld. 2008. Changes in Use and Perception of Facebook. In *Proceedings of the 2008 conference on Computer supported cooperative work*. 721–730.
[75] Cliff Lampe, Jessica Vitak, and Nicole Ellison. 2013. Users and nonusers: Interactions between levels of adoption and social capital. In *Proceedings of the 2013 conference on Computer supported cooperative work*. 809–820.
[76] Jong-Seok Lee and Dan Zhu. 2012. Shilling attack detection—a new approach for a trustworthy recommender system. *INFORMS Journal on Computing* 24, 1 (2012), 117–131. Publisher: INFORMS.
[77] Min Kyung Lee, Daniel Kusbit, Evan Metsky, and Laura Dabbish. 2015. Working with machines: The impact of algorithmic and data-driven management on human workers. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 1603–1612.
[78] Tuukka Lehtiniemi and Minna Ruckenstein. 2018. The social imaginaries of data activism. *Big Data & Society* 6, 1 (2018), 2053951718821146.
[79] Bo Li, Yining Wang, Aarti Singh, and Yevgeniy Vorobeychik. 2016. Data poisoning attacks on factorization-based collaborative filtering. In *Advances in neural information processing systems*. 1885–1893.
[80] Hanlin Li, Bodhi Alarcon, Sara M. Espinosa, and Brent Hecht. 2018. Out of Site: Empowering a New Approach to Online Boycotts. *Proceedings of the 2018 Computer-Supported Cooperative Work and Social Computing (CSCW'2018 / PACM)* (2018).
[81] Hanlin Li and Brent Hecht. 2020. 3 Stars on Yelp, 4 Stars on Google Maps: A Cross-Platform Examination of Restaurant Ratings. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW (2020).
[82] Hanlin Li, Nicholas Vincent, Janice Tsai, Jofish Kaye, and Brent Hecht. 2019. How do people change their technology use in protest?: Understanding "protest users". *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 87.
[83] Jiwei Li, Myle Ott, Claire Cardie, and Eduard Hovy. 2014. Towards a general rule for identifying deceptive opinion spam. In *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. 1566–1576.
[84] Helen Margetts, Peter John, Scott Hale, and Taha Yasseri. 2015. *Political turbulence: How social media shape collective action*. Princeton University Press.
[85] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. 2018. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*. 103–116.
[86] J Nathan Matias. 2016. Going dark: Social factors in collective action against platform operators in the Reddit blackout. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 1138–1151.
[87] Connor McMahon, Isaac L Johnson, and Brent Hecht. 2017. The Substantial Interdependence of Wikipedia and Google: A Case Study on the Relationship Between Peer Production Communities and Information Technologies.. In *ICWSM*. 142–151.
[88] Stefania Milan and Lonneke Van der Velden. 2016. The alternative epistemologies of data activism. *Digital Culture & Society* 2, 2 (2016), 57–74.
[89] Bamshad Mobasher, Robin Burke, Runa Bhaumik, and Chad Williams. 2005. Effective attack models for shilling item-based collaborative filtering systems. In *Proceedings of the WebKDD Workshop*. Citeseer, 13–23.
[90] Yaroslav Nechaev, Francesco Corcoglioniti, and Claudio Giuliano. 2017. Concealing Interests of Passive Users in Social Media.. In *BlackMirror@ ISWC*.
[91] Edward Newell, David Jurgens, Haji Mohammad Saleem, Hardik Vala, Jad Sassine, Caitrin Armstrong, and Derek Ruths. 2016. User Migration in Online Social Networks: A Case Study on Reddit During a Period of Community Unrest.. In *ICWSM*. 279–288.
[92] Safiya Umoja Noble. 2018. *Algorithms of oppression: How search engines reinforce racism*. nyu Press.
[93] Myle Ott, Claire Cardie, and Jeff Hancock. 2012. Estimating the prevalence of deception in online review communities. In *Proceedings of the 21st international conference on World Wide Web*. 201–210.
[94] Kari Paul. 2020. Prime Day: activists protest against Amazon in cities across US. *the Guardian* (Apr 2020). https://www.theguardian.com/technology/2019/jul/15/prime-day-activists-plan-protests-in-us-cities-and-a-boycott-of-e-commerce-giant
[95] Business Paul R. La Monica. 2020. Tech's magnificent seven are worth $7.7 trillion. https://www.cnn.com/2020/08/20/investing/faang-microsoft-tesla/index.html [Online; accessed 6. Oct. 2020].
[96] Nikolaos Pitropakis, Emmanouil Panaousis, Thanassis Giannetsos, Eleftherios Anastasiadis, and George Loukas. 2019. A taxonomy and survey of attacks against machine learning. *Computer Science Review* 34 (Nov. 2019), 100199.

https://doi.org/10.1016/j.cosrev.2019.100199 Publisher: Elsevier.
[97] Laura Portwood-Stacer. 2013. Media refusal and conspicuous non-consumption: The performative and political dimensions of Facebook abstention. *New Media & Society* 15, 7 (2013), 1041–1057.
[98] Eric A Posner and E Glen Weyl. 2018. *Radical Markets: Uprooting Capitalism and Democracy for a Just Society.* Princeton University Press.
[99] Barbara Prainsack. 2019. Data donation: How to resist the iLeviathan. In *The ethics of medical data donation.* Springer, Cham, 9–22.
[100] Alexander J Quinn and Benjamin B Bederson. 2011. Human computation: a survey and taxonomy of a growing field. In *Proceedings of the SIGCHI conference on human factors in computing systems.* ACM, 1403–1412.
[101] Adam Satariano. 2020. What the G.D.P.R., Europe's Tough New Data Law, Means for You. *N.Y. Times* (May 2020). https://www.nytimes.com/2018/05/06/technology/gdpr-european-privacy-law.html Publisher: The New York Times Company.
[102] Christine Satchell and Paul Dourish. 2009. Beyond the user: use and non-use in HCI. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7.* 9–16.
[103] Devansh Saxena, Patrick Skeba, Shion Guha, and Eric PS Baumer. 2020. Methods for Generating Typologies of Non/use. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–26.
[104] Sarita Yardi Schoenebeck. 2014. Giving up Twitter for Lent: how and why we take breaks from social media. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 773–782.
[105] Neil Selwyn. 2003. Apart from technology: understanding people's non-use of information and communication technologies in everyday life. *Technology in society* 25, 1 (2003), 99–116.
[106] Alana Semuels. 2017. Why #DeleteUber and Other Boycotts Matter . *Atlantic* (Feb 2017). https://www.theatlantic.com/business/archive/2017/02/why-deleteuber-and-other-boycotts-matter/517416
[107] Rijurekha Sen, Sohaib Ahmad, Amreesh Phokeer, Zaid Ahmed Farooq, Ihsan Ayyub Qazi, David Choffnes, and Krishna P Gummadi. 2017. Inside the walled garden: Deconstructing facebook's free basics program. *ACM SIGCOMM Computer Communication Review* 47, 5 (2017), 12–24.
[108] Ali Shafahi, W Ronny Huang, Mahyar Najibi, Octavian Suciu, Christoph Studer, Tudor Dumitras, and Tom Goldstein. 2018. Poison frogs! targeted clean-label poisoning attacks on neural networks. In *Advances in Neural Information Processing Systems.* 6103–6113.
[109] Shawn Shan, Emily Wenger, Jiayun Zhang, Huiying Li, Haitao Zheng, and Ben Y. Zhao. 2020. Fawkes: Protecting Privacy against Unauthorized Deep Learning Models. arXiv:cs.CR/2002.08327
[110] Márcio Silva, Lucas Santos de Oliveira, Athanasios Andreou, Pedro Olmo Vaz de Melo, Oana Goga, and Fabrício Benevenuto. 2020. Facebook Ads Monitor: An Independent Auditing System for Political Ads on Facebook. In *Proceedings of The Web Conference 2020.* 224–234.
[111] Jacob Steinhardt, Pang Wei W Koh, and Percy S Liang. 2017. Certified defenses for data poisoning attacks. In *Advances in neural information processing systems.* 3517–3529.
[112] Stefan Stieger, Christoph Burger, Manuel Bohn, and Martin Voracek. 2013. Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking* 16, 9 (2013), 629–634. Publisher: Mary Ann Liebert, Inc. 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA.
[113] Farnaz Tahmasebian, Li Xiong, Mani Sotoodeh, and Vaidy Sunderam. 2020. Crowdsourcing under data poisoning attacks: A comparative study. In *IFIP Annual Conference on Data and Applications Security and Privacy.* Springer, 310–332.
[114] Catalina L Toma and Jeffrey T Hancock. 2010. Reading between the lines: linguistic cues to deception in online dating profiles. In *Proceedings of the 2010 ACM conference on Computer supported cooperative work.* 5–8.
[115] Carmela Troncoso. 2019. Keynote Address: PETs, POTs, and Pitfalls: Rethinking the Protection of Users against Machine Learning. USENIX Association, Santa Clara, CA.
[116] Max Van Kleek, Dave Murray-Rust, Amy Guy, Kieron O'Hara, and Nigel Shadbolt. 2016. Computationally Mediated Pro-Social Deception. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16).* Association for Computing Machinery, New York, NY, USA, 552–563. https://doi.org/10.1145/2858036.2858060
[117] Nicholas Vincent and Brent Hecht. 2020. Can "Conscious Data Contribution" Help Users to Exert "Data Leverage" Against Technology Companies?
[118] Nicholas Vincent, Brent Hecht, and Shilad Sen. 2019. "Data Strikes": Evaluating the Effectiveness of New Forms of Collective Action Against Technology Platforms. In *Proceedings of The Web Conference 2019.*
[119] Nicholas Vincent, Isaac Johnson, and Brent Hecht. 2018. Examining Wikipedia with a broader lens: Quantifying the value of Wikipedia's relationships with other large-scale online communities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* 1–13.
[120] Nicholas Vincent, Isaac Johnson, Patrick Sheehan, and Brent Hecht. 2019. Measuring the importance of user-generated content to search engines. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 13. 505–516.
[121] Nicholas Vincent, Yichun Li, Renee Zha, and Brent Hecht. 2019. Mapping the Potential and Pitfalls of "Data Dividends" as a Means of Sharing the Profits of Artificial Intelligence. *arXiv preprint arXiv:1912.00757* (2019).
[122] Kaveh Waddell. 2020. California's New Privacy Rights Are Tough to Use, Consumer Reports Study Finds. *Consum. Rep.* (Oct 2020). https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use
[123] Daisuke Wakabayashi. 2018. California Passes Sweeping Law to Protect Online Privacy. *N.Y. Times* (Jun 2018). https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html
[124] Hongyi Wen, Longqi Yang, Michael Sobolev, and Deborah Estrin. 2018. Exploring recommendations under user-controlled data filtering. In *Proceedings of the 12th ACM Conference on Recommender Systems.* 72–76.
[125] John Wilmhoff. 2017. Tom Brady literally owns the Jets, says Google search. https://www.espn.com/sportsnation/story/_/page/170727QTP_BradyOwnsJets/google-glitch-causes-tom-brady-appear-new-york-jets-owner%7D Publication Title: ESPN.
[126] David C Wilson and Carlos E Seminario. 2013. When power users attack: assessing impacts in collaborative recommender systems. In *Proceedings of the 7th ACM conference on Recommender systems.* 427–430.
[127] David C Wilson and Carlos E Seminario. 2014. Evil twins: Modeling power users in attacks on recommender systems. In *International Conference on User Modeling, Adaptation, and Personalization.* Springer, 231–242.
[128] Sally ME Wyatt. 2003. Non-users also matter: The construction of users and non-users of the Internet. *Now users matter: The co-construction of users and technology* (2003), 67–79.
[129] Sean Xin Xu and Xiaoquan (Michael) Zhang. 2013. Impact of Wikipedia on Market Information Environment: Evidence on Management Disclosure and Investor Reaction. *MIS Quarterly* 37, 4 (Dec 2013), 1043–1068. http://www.jstor.org/stable/43825781
[130] Haoqi Zhang, Andrés Monroy-Hernández, Aaron Shaw, Sean A Munson, Elizabeth Gerber, Benjamin Mako Hill, Peter Kinnaird, Shelly D Farnham, and Patrick Minder. 2014. WeDo: end-to-end computer supported collective action. In *Eighth International AAAI Conference on Weblogs and Social Media.*
[131] Renjie Zhou, Samamon Khemmarat, and Lixin Gao. 2010. The impact of YouTube recommendation system on video views. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement.* ACM, 404–410.