Response to the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security

(Commercial Surveillance ANPR, R111004)

Data & Society Research Institute is pleased to submit a response to the Advanced Notice of Proposed Rulemaking (ANPRM) published by the Federal Trade Commission (FTC) on Commercial Surveillance and Data Security.

Data & Society is an independent, nonprofit research institute studying the social implications of data-centric technologies and automation. We produce empirical research that challenges the power asymmetries created and amplified by technology in society, and work to help ensure that artificial intelligence (AI) systems are accountable to the communities within which they are applied.

We are pleased to see that the FTC is seriously considering rulemaking on commercial surveillance and data security. The commercial surveillance industry has permeated business practices in the digital age and made avoiding data collection and its effects impossible for consumers.

Our comments argue that the FTC must pursue rulemaking to curb the rampant unfair and deceptive commercial surveillance and data security practices to which the commercial surveillance industry subjects consumers, particularly protected classes, children, and workers.

Specifically, we recommend that:

- The FTC pursues and creates rulemaking to combat unfair and deceptive commercial surveillance and data security practices.
- Commercial surveillance regulations mandate data access for research.
- Commercial surveillance regulations include transparent assessment practices, paths to redress, and justice for impacted consumers.
- Commercial surveillance regulations include specific protections against harms to protected classes.[*]
- Special protections be enacted to protect children and teens.
- Special protections be enacted to protect workers.

1. The FTC must pursue rulemaking to combat the varying and specific ways commercial surveillance and data security harm consumers.

Consumers' personal, behavioral, and financial information is widely available for companies and governments to mine, often without consumer consent.[1] Such information is commonly misused via commercial surveillance practices that harm consumers, often in pernicious and unaccountable ways. Extensive evidence demonstrates this harm is borne disproportionately by protected classes, children, and workers, as we review below. However, unchecked industry wrongdoing has consequences for every individual and for society as a whole. All consumers are likely to face price discrimination,[2] misuse of sensitive medical,[3] behavioral,[4] and location information,[5] coercion via deceptive software interfaces called dark patterns,[6] and unaccountable administration of the information,[7] opportunities,[8] and people[9] presented to them (Q7). Many systems are designed not for fair trade with consumers, but for extracting information by maximizing the time people spend on a platform — trading instead on the product of their attention.[10] These deep asymmetries in the information available to firms and consumers enable the coercion and exploitation of consumers (Q8). The Commission to date has not adequately addressed the scope of these harms (Q9).

Commercial surveillance harms consumers not only personally but at the societal level. Evidence indicates that commercial surveillance has distorted US elections. Platform design enables consumer information to be used to target people in their capacity as voters, facilitating misinformation,[11] voter suppression,[12] and astroturfed manipulation of the tenor and content of political debate — often emerging outside the United States.[13] Each of these consequences flows from social media business practices which primarily classify (and mis-classify) consumers at ever-increasing levels of granularity and inference; this

[*] To ensure that historically marginalized groups receive protection from unfair and deceptive commercial surveillance and data security practices, any regulations the FTC pursues must include an expansive and intersectional approach to defining discrimination. In our comment, protected classes include those that are federally protected, and other communities that suffer from systemic discrimination. We believe that the FTC should include the protection of communities and the approach to addressing algorithmic discrimination laid out by the Office of Science and Technology Policy in its October 2022 "Blueprint for an AI Bill of Rights." https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

practice provides the engine for selling and disseminating political advertisements without sufficient oversight,[14] nor standard FEC disclosures.[15] Other societal harms of commercial surveillance include to consumer choice via threats to competition,[16] the chilling effects and repressive potential of increasing public-private data sharing,[17] and the public health effects of platform design decisions on mental health[18] and the fabric of communities at scale[19] (Q7).

As we explore more fully below, the groups most adversely impacted by commercial surveillance are protected classes, children, and workers. Consumers are routinely both targeted and excluded on the basis of their race, ethnicity, and gender; these practices are made possible through business models that are reliant on user tracking and personalized ads which definitionally stratify users and channel information provided to them. For instance, an investigation by The Markup found that Facebook was used to serve discriminatory advertisements for job opportunities, enabling advertisers to exclude people based on racial "affinities."[20] Google ads were found to target job opportunities on the basis of gender.[21] Discriminatory targeting of this nature has been documented in a number of domains, including in voter suppression efforts[22] and housing.[23] Harm to protected classes also results from algorithmic error and bias,[24] which has reinforced discrimination against protected classes in contexts such as false arrests,[25] online search results,[26] healthcare,[27] the judicial system,[28] and education[29] (Q7, Q8).

Commercial surveillance practices are especially harmful when lives and livelihoods are at stake, such as when they are used by employers to oversee workers or by public agencies to administer law and policy. For instance, the in-home healthcare industry increasingly relies on electronic visit verification systems to track home health care workers. These tools are frequently designed assuming care recipients are homebound and, by implementing geofencing, either limit the mobility of those receiving care or deny workers their earned pay.[30] Care workers and recipients are subjected to commercial surveillance tactics that degrade the quality of their work and work experience with no path to recourse. Similar problems are evident in the automated identification used by law enforcement; companies who report consumers to government authorities for violations may find their accounts shut off or assets frozen with no recourse.[31] Regulations must be pursued to curtail unfair and deceptive practices that will only multiply as the commercial surveillance industry grows.

2. The FTC should mandate that researchers have access to commercial surveillance platforms' data, in order to better characterize these harms.

Characterizing the unfair and deceptive nature of commercial surveillance is a central task for respondents to this call. Many of these harms are well-documented, including by investigative reporting done by outlets such as ProPublica,[32] and The Markup,[33] as well as by academic researchers[34] and community advocates, and via whistleblowers.[35] *However*, this evidence is much more challenging to obtain when data, systems, development processes, and internal evaluations are withheld on the grounds of intellectual property claims. Those working outside of technology companies have far too little visibility into proprietary systems to be able to answer fundamental questions about system behavior at scale. For instance, academic researchers have few means to investigate how often, and to what extent, algorithmic systems discriminate against protected classes and in which sectors discrimination is most rampant (Q54). While there is abundant evidence of widespread deceptive and unfair commercial practices, the precise rate and pervasiveness of harm is exceedingly hard to measure because there is no data repository or other system access infrastructure to enable systematic research. The most effective tactics for sourcing data available to independent researchers are adversarial research methods, which in turn rely on tenuous conditions such as crowdsourced data,[36] compelled disclosure via lawsuits,[37] or "sock-puppet" audits utilizing public-facing APIs.[38] In the absence of robust data access, much of this work also relies on methods that present their own privacy and research ethics challenges, such as scraping user behavior data[39] and severely constrained data sharing agreements with tech companies.[40]

As the FTC undertakes its rulemaking, we encourage the Commission to recognize that the available evidence has been shaped by deep asymmetries in access to the development and functioning of proprietary platforms. Indeed, this lack of transparency is best understood as deceptive and unfair in itself. For all the harms and risks to consumers we describe below, **perhaps the single most effective intervention that the FTC could take across the surveillance and data sectors would be to pry open the door so that independent actors can assess and challenge harmful systems.**[41] This could take the form of mandating public APIs to platforms, adapting protocols for sensitive data sharing such as those used in the US census, piloting new cross-sector models for data sharing known as "data trusts," providing safe harbor protections for researchers engaged in third-party auditing, establishing robust reporting requirements, or a combination of these strategies.

The FTC should mandate that companies of a sufficient size create research data access programs that provide safety- and privacy-balanced access to core outputs and functions of regulated systems. The FTC cannot reasonably expect to understand, define, and regulate all possible deceptive and harmful practices in the data surveillance and artificial intelligence industries; some future harms and errors are definitionally not yet knowable. However, by leveraging assessment practices and public documentation standards, the FTC could require all developers to assess their own products according to best practices, make some portion of those assessments public, incentivize and protect independent assessors, and thereby make use of the knowledge and skills of affected communities in holding the surveillance and data industries accountable.

Given the public interest in characterizing the extent of consumer harm, and in light of the deep asymmetries in platform data access, we encourage the FTC to:

- Recognize that available evidence on consumer harm has been fostered under a regime of technology firms' overreliance on intellectual property protections at the expense of the public interest.
- Support researchers to more effectively characterize surveillance harms though unlocking access to research data, which to date they have often had to expend resources in gathering adversarially.

- Mandate key firms and services provide public access to granular, up-to-date data feeds called APIs.
- Adapt and disseminate protocols for sensitive data sharing to support a range of uses and users, such as those used in the US census. These may also take the form of third-party intermediaries known as "data trusts."
- Establish robust reporting requirements by which researchers can better understand design decisions and model training methods, and incentivize independent assessment.
- Mandate that companies of a sufficient size create research access programs that provide safety- and privacy-balanced access to core outputs and functions of regulated systems.

3. The FTC's regulations should target specific means by which commercial surveillance and data security harm protected classes.

The rampant misuse of commercial data to harm protected classes requires FTC action to both prevent and address discrimination. A number of questions in the ANPR ask whether certain kinds of data use should be targeted or banned entirely (Q38, Q53, Q67) and whether rules should focus on types of data or apply generically (Q10, Q21, Q46, Q53). We respond that prohibiting data collection about protected classes would not itself provide an effective means of preventing harm. Research in AI fairness has demonstrated repeatedly that the proxies for sensitive data indicating membership in a protected class are plentiful throughout the data ecosystem, and that addressing the fairness risk created by these proxies is conceptually and technically challenging.[42] Proxies for protected classes are often counterintuitive or unpredictable, rendering any attempt to regulate sensitive *types* of data moot. Even seemingly innocuous data can be put to nefarious ends using open-source and readily available tools, such as predicting race based on last name and ZIP code alone.[43] For example, given the United States' history of *de facto* and *de jure* racial housing segregation (aka, "redlining"), the attribute "race" often closely correlates to zip codes, which can be predictive of outcomes in domains as wide ranging as insurance rates,[44] obstetric health,[45] access to Internet services,[46] and criminal justice[47]. Therefore, in the absence of careful assessment and governance, big data and machine learning applications in these domains can import and reinforce discriminatory outcomes.

The close correlation between seemingly innocuous and widely used data attributes and proxies for protected classes must be a key consideration for FTC rulemaking. Sensitive demographic data collected from and about consumers (and its many proxies) certainly deserve extra scrutiny and security. However, discriminatory applications of data are not harmful because they are trained on explicitly sensitive data, but because they are carelessly or intentionally put to use for discriminatory **purposes** that unfairly benefit a commercial actor. Focusing rule-making on ostensibly sensitive **types of data** (e.g., race and gender) is therefore less likely to be successful at reducing deceptive and harmful practices than focusing on **the purpose and consequences** of data uses.

To prevent harm to protected classes, *a more effective means to prevent harm would be to place restrictions and reporting requirements on* potentially harmful purposes *to which data and services are put*. In a society with deep histories of structural discrimination, many data applications risk mirroring and reinforcing those histories and violating anti-discrimination statutes. Therefore, the FTC should start with a presumption that any type of data can be used in a discriminatory fashion and create affirmative obligations for developers to demonstrate to the public that such risks have been assessed and governed. This burden of evidence should be placed on developers of systems that use consumer data in a regulated sector such as finance or law enforcement. Sectors that have significant impact on consumers' lives should be under a general obligation to assess and transparently report risks and system governance.

Data about protected classes is itself a valuable tool for understanding the extent and status of data-driven discrimination, and therefore FTC rulemaking should permit sensitive data collection and analysis for this purpose. Any effort to measure a system's propensity to discriminate against protected classes requires understanding which users are members thereof. This need might require the collection of greater quantities of granular demographic data, which in turn presents a tension between competing goals for fairness and privacy.[48] Testing for demographic unfairness can present material conflicts with privacy interests of vulnerable populations. Ideally, testing for disparate impact should not generate new data surveillance harms; likewise, it should not impose new legal liabilities to tech companies that wish to understand the impacts of their systems but do not want to hold additional, highly sensitive data about users. The FTC — and related governmental agencies focused on innovation and technology policy — should seek to promulgate best practices for navigating these conflicts, such as utilizing synthetic data or consented user focus groups. These may include the collection of demographic data for evaluation purposes alone, as well as organizational and technical means of firewalling sensitive data from other uses within a firm.

Many harms to protected classes result from disproportionate error rates for some demographic groups over others. However, FTC rulemaking is not likely to be successful at preventing harm with mandatory targets for permissible error rates (Q56). Algorithmic error is inevitable in the design and deployment of algorithmic systems;[49] there is no reasonable means of generically regulating industry error rates because appropriate error rates are highly context-driven. Instead, the challenge for the FTC is to encourage companies to only use algorithmic systems in which **the error rate is appropriate for a given use**, and to provide **transparent documentation about that error rate and the design process that was used to conditionally accept it**. A high error threshold might be tolerated in a low stakes application such as ad services, while lower error rates might be required in a higher-stakes application such as medical diagnostic services or public housing allocation.

A further element of FTC rulemaking can introduce more stringent guidelines by which companies train their systems to prevent algorithmic bias and self-report their error and accuracy rates; this requirement would allow for more context-driven decisionmaking than establishing a target error rate limit across domains (Q56, Q89, Q92). A public-facing algorithmic impact assessment or similar transparency artifact would document the **expected**

error rate and its appropriateness for a given deployment. It should also include measures for differential error rates across protected class demographic categories, especially if demographic features are used in the modeling (Q65). Other agencies may find it appropriate to establish additional domain-specific rules that the FTC is not well-suited to regulate and where the stakes are higher (e.g., CFPB may set limits for error rates in mortgage credit algorithms). In lower-stakes applications, simple public reporting — and the potential social and competitive market pressures that it could drive — would represent a significant improvement over the current landscape.

The FTC must also consider restrictions on applications of commercial surveillance, such as facial recognition, that threaten fundamental civil rights. Changes in industry practice are possibly improving disparate performance rates across some demographic categories.[50] However, the choice to frame algorithmic harms on protected classes as primarily a result of error and algorithmic bias has risks: more accurate systems alone are not sufficient to address harm to protected classes. When algorithmic systems are used in areas that have significant impact on consumers' lives like housing, loans, and hiring decisions, they remain embedded in social domains characterized by multiple intersecting legacies of discrimination. Manufacturers' claims to increasing system accuracy over time present new risks in the form of fewer precautions in the use of algorithmic systems. The FTC can play a key role in establishing safeguards for particularly risky applications of algorithmic systems; such safeguards are enumerated in part as accountability mechanisms in the following section.

We believe that the FTC must:

- Forgo efforts to ban collection of enumerated sensitive data types, in recognition of the fact that many data attributes serve as proxies for demographic categories.
- Restrict or ban the use of algorithmic systems for dangerous or discriminatory *purposes* while placing the burden of evidence on developers to demonstrate safety and fairness.
- Allow firms to collect sensitive data on demographic categories for the purpose of evaluating their systems and services.
- Introduce more stringent guidelines by which companies must train their systems to prevent algorithmic bias.
- Require companies within sectors that have significant impact on consumers' lives to report the error and accuracy rates of their systems to the public.
- Restrict applications of commercial surveillance, such as facial recognition, that threaten fundamental civil rights.

4. The FTC's regulations must create accountability mechanisms that include affirmative obligations for transparent assessment practices, paths to redress, and justice for consumers.

The FTC should use its powers under Sections 5 and 18 to prevent unfair and deceptive practices in part by creating pathways to robust accountability mechanisms: specifically, mandating public-facing documentation, impact assessments, and means to redress. Consumers cannot reasonably be expected to protect themselves from systems which they have no statutory right to inspect or demand changes of (Q5, Q6). As multiple scholars have argued, accountability for algorithmic systems requires that consumers be empowered to demand changes to deployed systems and seek redress for harm.[51] The FTC has an essential role to play in supporting the public to more effectively make these demands. **It is crucial that the FTC takes action by facilitating accountability structures through regular assessment and transparency reporting to protect consumers from unfair and deceptive practices** (Q89, Q92, Q94).

The FTC should require robust documentation of decisions made in software development lifecycles for systems that threaten consumers. Many technology firms are prepared to respond to such mandates via their investment in internal risk management teams (named variously as overseeing privacy, responsible AI, or responsible innovation) to address concerns about the aforementioned harms. Such teams have generated numerous frameworks that can serve as models for documentation requirements, such as datasheets for Datasets,[52] Model Cards,[53] and disparate impact reporting. Standards organizations and federal agencies have begun promulgating playbooks for accountable data systems, such as NIST's "AI Risk Management Framework." However, without rule-making from federal regulators, these efforts remain voluntary, scattered, and wholly unsynchronized. Even if leading technology companies wish to conduct assessments of their systems, they are often stymied by the lack of a coherent regulatory vision and reliable market conditions that incentivize industry-wide adoption.

The FTC must also require routine assessment processes during the full data and machine learning lifecycle for systems that have significant impact on consumers' lives. Assessments ought to be undertaken prior to full deployment, and ought to be updated throughout the lifecycle of a product. While it is not possible to a priori define the questions required for a given assessment, the FTC can define a framework akin to an environmental impact assessment by which experts can participate in guiding design decisions and anticipating adverse impacts. In particular, second-party, commissioned assessments hold the greatest promise for balancing the challenges of first-party assessments (conflicts of interest) and third-party (lack of access).[54] Assessment practices like these create footholds to prevent unfair and deceptive practices during the design process — prevention is preferable to seeking redress after harm is done, especially for vulnerable groups who may lose pivotal opportunities for economic, social, and political advancement. Robust guidance on assessment practices will grow increasingly critical as artificial intelligence capacity moves out of the primary technology industry (where assessments are being piloted) and into secondary sectors such as insurance, medicine, and finance.

It is essential that the FTC require both design documentation and impact assessments to be public. The public rarely has access to essential information about the assumptions, key design decisions, and performance evaluations of systems in use. There is no statutory right to view documents like these outside of legal discovery (Q6). When the public has no access to such artifacts, they fail to realize their potential as leverage for public oversight.

Indeed, previous scholarship on "legal endogeneity" finds that companies who create internal risk management and impact assessment processes (such as privacy impact assessments) operationalize them to support business as usual.[55] However, public reporting alone is not enough to prevent harm; impact assessments and other documentation are most useful when they are used by consumers, advocates, lawmakers, and law enforcement to hold developers responsible for harms. Without venues such as public hearings, administrative procedures, and courts to contest harmful practices, advocate for changes, or seek redress, public disclosure efforts are empty (Q84).

Finally, the FTC must recognize that those whose lives are affected by a given system should play a central role in its design and assessment. A growing share of scholarship argues that ongoing consultation with directly impacted people should be a required component of high impact algorithmic system design, auditing, and regulatory frameworks.[56] One form this might take is that impacted communities guide the design process and provide input on the intended purpose of a system prior to its development, with the capability to reject the development of a given system.[57] Technology developers and the FTC can draw lessons from decades of work on environmental impact assessments, which have successfully integrated input from local residents, advocates, and subject matter experts in shaping the ultimate deployment of a system. Regulators can require public input as a formal component of an assessment framework.

As the FTC contemplates rulemaking about commercial surveillance, it must foster accountability mechanisms by empowering consumers, advocates, researchers, and civil society and enrolling them in oversight. We believe that the FTC should:

- Require robust, public documentation of software development practices for systems that have significant impact on consumers' lives based on responsible data and AI frameworks in current use.
- Mandate impact assessments for systems that have significant impact on consumers' lives that include guidance for how to more responsibly develop systems toward preventing harm.
- Establish venues for consumers, advocates, and others to demand changes to systems and redress for harms.
- Include public participation from impacted communities and their advocates as a feature of requirements for technology development and assessment.

5. The FTC must protect children and teens from the harms associated with commercial data surveillance, but also be mindful of the unique complexities of youth, young people's needs, and their place in a broader family system.

Children use online platforms and generate data. Children occupy online spaces regardless of regulations like the Child Online Privacy Protection Act (COPPA) that require parental involvement in any child under 13's use of a website that collects data. The data of children and teens, or more specifically the uses of data about and provided by children, must be treated with an even greater level of care and scrutiny than data from adults.

Children under 18 are uniquely vulnerable because of the developmental process children and adolescents go through as they grow into adults, growth that impacts their ability at younger stages to regulate their impulses and to understand, discern, and respond to things they see and choices they are asked to make. The youngest age group of adolescent children (roughly 10–13) engage in very concrete, ego-centric thinking marked by susceptibility to peer pressure and concerns. Middle adolescence (approximately 14–17) is marked by impulsivity, and the very beginning of the development of more complex thinking and the ability to project consequences of choices or actions.[58] This trajectory of cognitive, social, and emotional growth requires a different perspective and a greater duty of care for children — already evident in our state-based rules governing the age of consent for contracts, marriage, and sexual activity.[59, 60] Further complicating these age distinctions is that young people do not traverse through these developmental stages at the same rate, or at necessarily the same time, as their same-age peers. Physical development is not always in step with cognitive, social, or emotional development. This means that using the rough age boundaries to impute cognitive development (and the ability to consent or understand the implications of data collections or online choices) is, at best, inaccurate for many young people, and, at worst, actively harmful for others. For this reason, we caution the FTC about creating new age fences or categories of youth based on age or physical development. Further, age verification solutions that use multiple modes of assessment of an individual — biological age, physical age, cognitive or developmental age (Q17) — together in a layered approach will provide more accurate age verification of individuals than any of the three modes alone.

As our youngest users and consumers, minor children have the longest timeline of any of us to be haunted by the ghosts of commercial data collection and, as outlined above, its potential for discrimination and harm (Q13). For these reasons, children under 18 must be considered a particularly protected class of individuals and must have separate and greater data protections than adults.

One critical tool for protecting minors from data-related harm is that of **data minimization** — where entities are required to collect the smallest amount of data about a user necessary to provide a service or do basic research. **However, while data minimization is important, it cannot be at the expense of accurately designing products that reduce harms to specific populations of youth and adults**. Data & Society research has demonstrated that some tech companies already deploy "strategic ignorance" about the populations that use their platforms by not collecting data about users, and using this as a rationale for continuing to design inappropriate and harmful products and features for those users.[61] Data collection to enable the design and testing of products for utility and harm reduction should be allowed under any data minimization policy (Q21).

Any data policies for minors must include the ability for young people to delete, expunge, and reset the data collected about them and the algorithms fed by that data that shape the content they see. Sites like YouTube already offer consumers the ability to reset the algorithms that deliver content. This needs to be made a standard, particularly for those websites and services that are geared towards children and teens, or for accounts held by teens and minor children. There should also be an option to delete data on those services primarily targeted toward children and teens.

As the GDPR Articles 16 and 17 creates for European users, we recommend offering American youth an "eraser button" or the chance to correct, "seal" or delete their "digital permanent record" — modeled on and underpinned by the same developmental sentiments that shape how juvenile criminal offenses are handled in a US court of law.[62] Older adolescents have often reflected on their concerns about their own use and content shared online as younger adolescents, and some have even gone so far as to create new accounts in an attempt to leave behind youthful interactions and expressions. GDPR Article 17 lays out a right to removal, while Article 16 specifies the right to "rectification" of collected data. We must give youth the opportunity to truly delete the data trails that linger and the digital dossiers that accrete information about them even after they disable or delete old accounts.

The data trails that youth create through the very fact of being online do not only feed the machine of targeted advertising online, they also underpin the algorithms that decide what content a person does or does not see on many social media sites. As a part of an eraser button, the FTC should consider offering young people the chance to "reset" the algorithm and the data used to deliver content in the algorithmic recommendation systems and feeds that populate their online lives — as a part of a suite of data protections and tools for young consumers.

There are very real reasons to work towards identifying younger users in online spaces (for instance, so that a set of basic protections, including limiting or eliminating capture and retention of geolocation data, among other types of data, can be developed). However, the manner through which age is verified matters. Though COPPA has been criticized for its reliance on consent (including Verifiable Parental Consent) and "actual knowledge" for age verification, more invasive methods to verify age must be considered carefully. In particular, the risks of verifying age through biometric surveillance may outweigh the potential harms of commercial surveillance for this age group. One approach would be to create a panel reviewing age verification methods and requirements that is sensitive to actual use — and to the needs of communities, such as LGBTQ+, the undocumented, and communities of color — whose information-seeking activities may be more impacted by both the perceived and actual risks of age verification through biometric surveillance, or through other methods of verification that have been proposed by industry, such as "social vouching."[63] Since critiques of the use of AI to verify age often focus on whether the technology can assess age accurately, there is not enough attention being paid to whether age verification techniques like "video selfies" may deter important information seeking among vulnerable groups altogether. These risks must be weighed carefully. On the one hand, consent as a model is limited; parents and kids can share devices and accounts, parents are not always available to provide consent, and often, the requirement of parental consent can deter information seeking among the most vulnerable. But biometric surveillance could create an enormous repository of personal data about children and adults and the potential for that database to be misused.

Corporations and advertisers that wish to continue to collect data about consumers, including minors, argue that giving notice of data collection practices and asking for consent for collection provides a reasonable response to concerns about consumer data collection and surveillance. Even for adults, there is little evidence that requests for consent are appropriate protections from data collection. And minors are not even legally allowed to provide consent. This leaves mechanisms for notification and consent that are either easily bypassed or which foist parents into a situation that creates great friction. The friction of parental consent can not only deter a minor's legitimate access, it can also prevent companies from providing services in the first place. We can see this with COPPA's convoluted Safe Harbor requirements and its contribution to "platform deserts" for children ages 5–12.

Parents are not the answer to child privacy and data protection. Rather than yet again placing the full weight of responsibility for protecting children on the backs of parents, we need to move away from an exclusively individual focus and provide some basic floors — similar to those established in the UK's Age Appropriate Design Code including restrictions on geolocation data[64] or the use of "nudge techniques" pushing children to disclose or share more personal information[65] — to protect minors from data collection (Q19). Right now, collecting this data and selling it, and then using it to track and manipulate children and families, is too easy. We need rules to make this data collection truly costly, so companies will choose not to do it, rather than putting the onus on the parent or child user to manage it across multiple and numerous platforms.

As the FTC contemplates rulemaking about consumer data practices, it must consider minor children as a unique protected class that requires some basic data protections. We believe that the FTC must require:

- Transparency from corporations in all parts of the consumer data ecosystem about their data practices.
- Data minimization with carve outs for data collected for harm prevention research, and robust, painful enforcement of data minimization and retention rules, especially for minors.
- An "eraser button" for children's data and reset buttons for algorithms driven by these data.
- Age verification to be a robust, layered process, and not just based on biological age.
- Create basic parameters of protection for minor accounts, rather than placing the entire burden of child data protection on the shoulders of overwhelmed parents.
- Do not depend on parents to manage the data surveillance and consent regimes for youth.

6. The FTC's regulations must protect workers, who are particularly vulnerable to commercial surveillance, and be attentive to the myriad ways that surveillance is used to control them.

In investigating the harms to workers, the FTC must foreground the fact that their status renders them into "captive populations" for whom data collection practices are imposed by employers; as a result, standards around consent should be considered differently from other types of consumers (Q79).[66] Workers as a category are particularly vulnerable to commercial surveillance because employers have broad rights over workers to surveil, control, and wield power and information asymmetries that favor employers' interests.[67] Few workplace-specific privacy protections exist to limit their scope. Moreover, companies' business models increasingly misclassify their workforces as independent contractors in order to exclude them from standard labor protections and benefits, leaving the low-wage workforce with even fewer avenues for recourse against unfair or deceptive practices.[68] The FTC should continue to include independent contractors in its definition of workers, and should consider how digital platform companies are both at the forefront of experimenting with new surveillance practices and at the same time are evading legal accountability as employers.[69]

A key issue is that workers' consent to data collection is difficult or impossible to meaningfully obtain because the imposition of data-driven technologies are often required as part of the employment contract or are embedded into the labor process (Q74). The use of digital platforms to manage workers has made it easier for companies to frequently change privacy policies, and workers may only be informed through a lengthy user agreement that they are pressured to immediately accept in order to clock in to work. However, policies to grant workers more choice to opt-out of data collection (Q80) may be insufficient to address aggregate harms to workers and may come with penalties on workers who decline to provide their data. For instance, as part of employer-mandated health insurance programs, some employers have introduced wellness-tracking apps that track workers' physical movements as well as require them to submit sensitive information about their diets, smoking habits, and family medical histories. Although use of such apps are often opt-out, employees who refuse are typically required to pay higher premiums and other increased costs to their health insurance.[70] In Europe, the GDPR addresses this issue by stating that an employer cannot claim an employee's consent as legal basis for data collection; if the employee will suffer negative consequences by refusing, then it is not considered freely given.[71] While efforts to implement notice and consent from workers may provide some transparency on data collection and use, they ultimately place responsibility on individual workers and assume informed consent is easy and sufficient (Q76). However, workers may experience the same harmful or deceptive practices regardless of whether or not they have chosen to opt-out because broader workplace management decisions are often informed by aggregate rather than individual worker data.[72]

The challenges to obtaining meaningful consent in the worker context also bear directly on the FTC ANPR's concerns about transparency in the collection, use, and retention of consumer data (Q43). The goals of worker surveillance have expanded from conventional practices of evaluating labor processes or worker performance to trying to make predictions about workers' future behaviors, their emotional states and mental health, their social interactions, and their financial status. A recent industry survey found that, since 2018, more than 550 tech products have emerged that collect, aggregate, and analyze data about workers across every aspect of employment, from hiring and beyond.[73] These largely unregulated third-party companies amass data from myriad sources, including biometrics, customer reviews, credit scores and financials, both on-and off-the-job behavioral data, and more.[74] Workers have little transparency or input into what counts as good, accurate information or whether assessments about them are fair. For example, racial and gender biases, as well as discrimination against people with disabilities, have all been documented across automated decision-making in hiring, management, and performance evaluation.[75] However, the harms workers face go well beyond issues of bias and discrimination, but give employers significant power to target, control, and manipulate workers in ways that damage their physical, emotional, and financial well-being. Companies can deceptively leverage data to engage in wage theft and wage suppression,[76] pressure workers to risk safety to meet high productivity benchmarks, target financially insecure workers for predatory payday loans,[77] and suppress labor organizing.[78] In defining unfair and deceptive practices, the FTC must prioritize investigating forms of surveillance that explicitly target vulnerable categories of workers, particularly low-wage workers who have less bargaining power and job mobility. Importantly, efforts to merely empower individual workers with more access to their own data are insufficient. Regulatory efforts must instead prioritize developing standards for how and why data is collected and used to make decisions about workers.

We ask the FTC to:

- Recognize that workers are unlike consumers in that they do not have even an ostensible choice over the extent to which they are subjected to commercial surveillance.
- Focus on investigating harms experienced by low-wage workers and others who have fewer means to contest additional pressures and penalties introduced by workplace surveillance. This entails holding both employers and third party developers accountable for how technologies are designed and deployed.
- Ensure that assessments of automated decision-making systems include appraisal of whether such systems abide by current workplace protection laws.
- Restrict or ban the use of automated decision-making tools in some aspects of the hiring process, given their demonstrated record of bias and discrimination.

In conclusion, we thank you for grappling with commercial surveillance and data security practices that threaten consumers and prevent a just and fruitful American technology ecosystem. Pursuing rulemaking on commercial surveillance and data security practices is crucial for this end. Any potential regulations must require transparency tools, accountability mechanisms, and rules that deftly and fervently protect the many ways discrimination and coercion arise. We look forward to supporting the FTC in this effort.

Sincerely,

Serena Oduro, Policy Analyst

Sareeta Amrute, Principal Researcher/Program Director

Jenna Burrell, Director of Research

Robyn Caplan, Senior Researcher

Amanda Lenhart, Program Director

Alexandra Mateescu, Researcher

Jacob Metcalf, Program Director

Meg Young, Participatory Methods Research Fellow

Endnotes

[1] https://www.theatlantic.com/technology/archive/2016/10/incessant-consumer-surveillance-is-leaking-into-physical-stores/504821/.

[2] Useem, Jerry, "How online shopping makes suckers of us all," *The Atlantic*, May 2017. https://www.theatlantic.com/magazine/archive/2017/05/how-online-shopping-makes-suckers-of-us-all/521448/.

[3] Powles, Julia, and Hal Hodson. "Google DeepMind and healthcare in an age of algorithms." Health and technology 7, no. 4 (2017): 351-367.; Gregory Barber and Megan Molteni, "Google Is Slurping Up Health Data—and It Looks Totally Legal," *Wired*, November 11, 2019. https://www.wired.com/story/google-is-slurping-up-health-dataand-it-looks-totally-legal/ ; Lovell, Tammy, "Google and DeepMind face legal claim for unauthorised use of NHS medical records" *Healthcare IT News*, May 17, 2022. https://www.healthcareitnews.com/news/emea/google-and-deepmind-face-legal-claim-unauthorised-use-nhs-medical-records/.

[4] Kantor, Jodi, Arya Sundaram, "The Rise of the Worker Productivity Score," *The New York Times*, August 14, 2022. https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html/.

[5] Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*, December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html/.

[6] Waldman, Ari Ezra. "Cognitive biases, dark patterns, and the 'privacy paradox'." *Current Opinion in Psychology* 31 (2020): 105–109; Narayanan, Arvind, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. "Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces." *Queue* 18, no. 2 (2020): 67–92.

[7] Gillespie, Tarleton. Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press, 2018.

[8] Lambrecht, Anja, and Catherine Tucker. "Algorithmic bias? An empirical study of apparent gender-based discrimination in the display of STEM career ads." *Management science* 65, no. 7 (2019): 2966–2981.

[9] Finkel, Eli J., Paul W. Eastwick, Benjamin R. Karney, Harry T. Reis, and Susan Sprecher. "Online dating: A critical analysis from the perspective of psychological science." *Psychological Science in the Public Interest* 13, no. 1 (2012): 3–66.

[10] McCluskey, Megan, "How Addictive Social Media Algorithms Could Finally Face a Reckoning in 2022," *Time Magazine*, January 4, 2022. https://time.com/6127981/addictive-algorithms-2022-facebook-instagram/.

[11] Calo, Ryan, Chris Coward, Emma S. Spiro, Kate Starbird, and Jevin D. West. "How do you solve a problem like misinformation?." *Science Advances* 7, no. 50.

[12] Ravel, Ann. "A new kind of voter suppression in modern elections." *U. Mem. L. Rev.* 49 (2018): 1019.

[13] Starbird, Kate. "Disinformation's spread: bots, trolls and all of us." Nature 571, no. 7766 (2019): 449–450; Woolley, Samuel C. "Bots and computational propaganda: Automation for communication and control." Social media and democracy. The state of the field, prospects for reform (2020): 89–110.

[14] Papakyriakopoulos, Orestis, Christelle Tessono, Arvind Narayanan, and Mihir Kshirsagar. "How Algorithms Shape the Distribution of Political Advertising: Case Studies of Facebook, Google, and TikTok." https://arxiv.org/abs/2206.04720 (2022).

[15] Haenschen, Katherine, and Jordan Wolf. "Disclaiming responsibility: How platforms deadlocked the Federal Election Commission's efforts to regulate digital political advertising." *Telecommunications Policy* 43, no. 8 (2019): 101824.

[16] Khan, Lina. "Amazon's antitrust paradox." *Yale Law Journa*l 126 (2017).

[17] Bhuhiyan, Johana, "How can US law enforcement agencies access your data? Let's count the ways," *The Guardian*, April 4, 2022. https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta; Bhuiyan, Johana, "Facebook gave police their private data. Now, this duo face abortion charges," *The Guardian*, August 10, 2022. https://www.theguardian.com/us-news/2022/aug/10/facebook-user-data-abortion-nebraska-police/.

[18] Valkenburg, Patti M., Adrian Meier, and Ine Beyens. "Social media use and its impact on adolescent mental health: An umbrella review of the evidence." *Current Opinion in Psychology* 44 (2022): 58–68.

[19] Bloch, Stefano. "Aversive racism and community-instigated policing: The spatial politics of Nextdoor." *Environment and Planning C: Politics and Space* 40, no. 1 (2022): 260–278.

[20] https://themarkup.org/the-breakdown/2020/08/25/does-facebook-still-sell-discriminatory-ads ; https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known/.

[21] https://petsymposium.org/popets/2015/popets-2015-0007.php/.

[22] Ravel, Ann. "A new kind of voter suppression in modern elections." *U. Mem. L. Rev.* 49 (2018): 1019.

[23] Ali, Muhammad, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, and Aaron Rieke. "Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes." *Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (2019): 1–30.

[24] Buolamwini, Joy, and Timnit Gebru. "Gender shades: Intersectional accuracy disparities in commercial gender classification." In *Conference on Fairness, Accountability and Transparency*, pp. 77–91. PMLR, 2018.

[25] Hill, Kashmir, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, December 29, 2020.

[26] Sweeney, Latanya. "Discrimination in online ad delivery: Google ads, black names and white names, racial discrimination, and click advertising." *Queue* 11, no. 3 (2013): 10–29.

[27] Obermeyer, et al. 2019. "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations. *Science* 366(6464): 447–453.

[28] Fox Kahn, Albert 2020. "Listening Beyond the Bars" https://www.stopspying.org/listening-beyond-the-bars/.

[29] Annany, Mike. 2022. "Seeing Like an Algorithmic Error: What are Algorithmic Mistakes, Why Do They Matter, How Might They Be Public Problems?" *Yale J.L and Tech*, vol. 24.

[30] https://www.theguardian.com/us-news/2021/jul/28/digital-surveillance-caregivers-artificial-intelligence/; https://datasociety.net/library/electronic-visit-verification-the-weight-of-surveillance-and-the-fracturing-of-care/.

[31] https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html/.

[32] "Facebook Hosted Surge of Misinformation and Insurrection Threats in Months Leading Up to Jan. 6 Attack, Records Show," ProPublica, January 4, 2020. https://www.propublica.org/article/facebook-hosted-surge-of-misinformation-and-insurrection-threats-in-months-leading-up-to-jan-6-attack-records-show https://www.propublica.org/article/facebook-hosted-surge-of-misinformation-and-insurrection-threats-in-months-leading-up-to-jan-6-attack-records-show/.

[33] Feathers, Todd, Simon Fondrie-Teitler, Angie Waller, Surya Mattu, "Facebook Is Receiving Sensitive Medical Information from Hospital Websites" The Markup, June 16, 2022. https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites/.

[34] Christian, Sandvig, and Algorithms Automation. "Politics| When the Algorithm Itself is a Racist: Diagnosing Ethical Harm in the Basic Components of Software." *International Journal of Communication* 10: 19.

[35] Hao, Karen, "The Facebook whistleblower says its algorithms are dangerous. Here's why," *MIT Technology Review*, October 5, 2021. https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/.

[36] Bobrowsky, M. Facebook Disables Access for NYU Research Into Political-Ad Targeting. WSJ. https://www.wsj.com/articles/facebook-cuts-off-access-for-nyu-research-into-political-ad-targeting-11628052204.

[37] Isaac, M. Meta Agrees to Alter Ad Technology in Settlement With U.S. *The New York Times* (2022). https://www.nytimes.com/2022/06/21/technology/meta-ad-targeting-settlement.html.

[38] Shen, H., DeVos, A., Eslami, M. & Holstein, K. Everyday algorithm auditing: Understanding the power of everyday users in surfacing harmful algorithmic behaviors. *Proc. ACM Hum.-Comput. Interact.* 5, 1–29 (2021).

[39] Mozilla Foundation. New Mozilla Tool Enlists Users to Determine if YouTube's Algorithmic Controls Actually Work. Mozilla Foundation. https://foundation.mozilla.org/en/blog/new-mozilla-tool-enlists-users-to-determine-if-youtubes-algorithmic-controls-actually-work/ (2021).

[40] Hegelich, S. Facebook needs to share more with researchers. *Nature* 579, 473–473 (2020).

[41] Engler, Alex, "Tech cannot be governed without access to its data," The Brookings Institution, September 10, 2020. https://www.brookings.edu/blog/techtank/2020/09/10/tech-cannot-be-governed-without-access-to-its-data/.

[42] Mhasawade, Vishwali, Yuan Zhao, and Rumi Chunara. "Machine learning and algorithmic fairness in public and population health." *Nature Machine Intelligence* 3, no. 8 (2021): 659–666; Corbett-Davies, Sam, and Sharad Goel. "The measure and mismeasure of fairness: A critical review of fair machine learning." arXiv preprint arXiv:1808.00023 (2018); Schumann, Candice, Xuezhi Wang, Alex Beutel, Jilin Chen, Hai Qian, and Ed H. Chi. "Transfer of machine learning fairness across domains." arXiv preprint arXiv:1906.09688 (2019); Barocas, Solon, Moritz Hardt, and Arvind Narayanan. "Fairness in machine learning." *Nips tutorial* 1 (2017): 2; Obermeyer, Z., Powers, B., Vogeli, C. & Mullainathan, S. Dissecting racial bias in an algorithm used to manage the health of populations. *Science* 366, 447–453 (2019); Green, B., 2018. "Fair" risk assessments: A precarious approach for criminal justice reform. In *5th Workshop on Fairness, Accountability, and Transparency in Machine Learning* (pp. 1–5).

[43] Flatow, I. How Imperfect Data Leads Us Astray. Science Friday. https://www.sciencefriday.com/segments/imperfect-data/ (2021); Elliott, M., Fremont, A., Morrison, P., Pantoja, P. & Lurie, N. A New Method for Estimating Race/Ethnicity and Associated Disparities Where Administrative Records Lack Self-Reported Race/Ethnicity. Health Serv Res 43, 1722–1736 (2008); Naunheim, T. Surgeo. (2022). https://github.com/theonaunheim/surgeo/blob/717a0a0367a189d0197eafc919d8332ccaefd8ea/docs/source/index.rst/.

[44] Lin, Xiao, Mark J. Browne, and Annette Hofmann. "Race discrimination in the adjudication of claims: Evidence from earthquake insurance." *Journal of Risk and Insurance* (2022).

[45] Hollenbach, Stefanie J., Loralei L. Thornburg, J. Christopher Glantz, and Elaine Hill. "Associations between historically redlined districts and racial disparities in current obstetric outcomes." JAMA network open 4, no. 9 (2021): e2126707-e2126707.

[46] Mossberger, Karen, Caroline J. Tolbert, and Michele Gilbert. "Race, place, and information technology." *Urban Affairs Review* 41, no. 5 (2006): 583–620.

[47] Arnold, David, Will Dobbie, and Crystal S. Yang. "Racial bias in bail decisions." *The Quarterly Journal of Economics* 133, no. 4 (2018): 1885–1932.

[48] Dwork, Cynthia, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Richard Zemel. "Fairness through awareness." In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pp. 214–226. 2012.

[49] Cooper, A. F., Moss, E., Laufer, B. & Nissenbaum, H. Accountability in an Algorithmic Society: Relationality, Responsibility, and Robustness in Machine Learning. In *2022 ACM Conference on Fairness, Accountability, and Transparency* 864–876 (ACM, 2022). doi:10.1145/3531146.3533150.

[50] Face Recognition Vendor Test (FRVT) Ongoing. National Institute of Standards and Technology. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing. Retrieved 4 October 2022.; Buolamwini, J. & Gebru, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on Fairness, Accountability and Transparency* 77–91 (PMLR, 2018); Raji, I. D. & Buolamwini, J. Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* 429–435 (ACM, 2019). doi:10.1145/3306618.3314244; Raji, Inioluwa Deborah, and Genevieve Fried. "About face: A survey of facial recognition evaluation." arXiv preprint arXiv:2102.00813 (2021).

[51] Bernhardt, Annette, Lisa Kresge, and Reem Suleiman. "Data and Algorithms at Work: The Case for Worker Technology Rights." San Francisco: UC Berkeley Labor Center. https://laborcenter.berkeley.edu/data-algorithms-at-work(2021); Metcalf, Jacob, Emanuel Moss, Ranjit Singh, Emnet Tafese, and Elizabeth Anne Watkins. "A relationship and not a thing: A relational approach to algorithmic accountability and assessment documentation." arXiv preprint arXiv:2203.01455(2022); Crawford, Kate, and Jason Schultz. "Big data and due process: Toward a framework to redress predictive privacy harms." BCL Rev. 55 (2014): 93.

[52] Gebru, Timnit, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé Iii, and Kate Crawford. "Datasheets for datasets." *Communications of the ACM* 64, no. 12 (2021): 86–92.

[53] Mitchell, Margaret, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru. "Model cards for model reporting." In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, pp. 220–229. 2019.

[54] Metcalf, J. Witnessing Algorithms at Work: Toward a Typology of Audits. *Points*. https://points.datasociety.net/witnessing-algorithms-at-work-toward-a-typology-of-audits-efd224678b49 (2022).

[55] Waldman, Ari Ezra. Industry unbound: The inside story of privacy, data, and corporate Power. Cambridge University Press, 2021; Edelman, Lauren B., and Shauhin A. Talesh. "To comply or not to comply—That isn't the question: How organizations construct the meaning of compliance." Explaining compliance: Business responses to regulation (2011): 103–122.

[56] Metcalf, Jacob, Emanuel Moss, Ranjit Singh, Emnet Tafese, and Elizabeth Anne Watkins. "A relationship and not a thing: A relational approach to algorithmic accountability and assessment documentation." arXiv preprint arXiv:2203.01455(2022); Krafft, P. M., Meg Young, Michael Katell, Jennifer E. Lee, Shankar Narayan, Micah Epstein, Dharma Dailey et al. "An action-oriented AI policy toolkit for technology audits by community advocates and activists." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pp. 772–781. 2021; Costanza-Chock, Sasha. "Design justice, AI, and escape from the matrix of domination." (2018); Hampton, Lelia Marie. "Black feminist musings on algorithmic oppression." arXiv preprint arXiv:2101.09869 (2021).

[57] Lee, Jennifer, Meg Young, P. M. Krafft, and Michael A. Katell. "Power and technology: who gets to make the decisions?." Interactions 28, no. 1 (2020): 38–46.

[58] Allen, Brittany and Waterman, Helen. (2019) "Stages of Adolescence," Healthy Children [website], American Academy of Pediatrics. https://www.healthychildren.org/English/ages-stages/teen/Pages/Stages-of-Adolescence.aspx/.

[59] Legal Age, https://www.law.cornell.edu/wex/legal_age/.

[60] US Department of Health and Human Services, (2004) "Statutory Rape: A Guide To State Laws and Reporting Requirements." https://aspe.hhs.gov/reports/statutory-rape-guide-state-laws-reporting-requirements-1/.

[61] Lenhart, Amanda and Owens, Kellie. (2021) "The Unseen Teen: The Challenges of Building Healthy Tech for Young People," Data & Society Research Institute. February 2021. https://datasociety.net/library/the-unseen-teen/.

[62] "Juvenile Justice," (nd) Youth.gov, Interagency Working Group on Youth Programs, US Government. https://youth.gov/youth-topics/juvenile-justice/.

[63] https://www.forbes.com/sites/petersuciu/2022/07/01/meta-testing-new-age-verification-tools--experts-explain-why-they-wont-work/?sh=4a643bb02e3e/.

[64] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/.

[65] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/13-nudge-techniques/.

[66] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019, p. 397.

[67] Annette Bernardt, Reem Suleiman, and Lisa Kresge. "Data and Algorithms at Work: The Case for Worker Technology Rights," UC Berkeley Labor Center, November 2021. https://laborcenter.berkeley.edu/data-algorithms-at-work/.

[68] Smith, Rebecca, and Maya Pinto, "Rewriting the Rules: Gig Companies' Drive for Labor Deregulation," In Beyond the Algorithm: Qualitative Insights for Gig Work Regulation, ed. Deepa Das Acevedo. (Cambridge: Cambridge University Press, 2020), 189–207; Brian Callaci, "Puppet Entrepreneurship: Technology and Control in Franchised Industries," Data & Society Research Institute, January 2021. https://datasociety.net/library/puppet-entrepreneurship/.

[69] https://datasociety.net/library/at-the-digital-doorstep/.

[70] Bort, Julie. "This Company Saved A Lot Of Money By Tracking Their Employees With Fitbits," *Business Insider*, November 22, 2018. https://www.businessinsider.com/company-saved-money-with-fitbits-2014-7/.

[71] "GDPR: Consent," https://gdpr-info.eu/issues/consent/.

[72] Aiha Nguyen. "The Constant Boss: Labor under Digital Surveillance." Data & Society Research Institute, May 2021. https://datasociety.net/library/the-constant-boss/.

[73] Bossware and Employment Tech Database, Coworker.org. https://home.coworker.org/worktech/.

[74] Miller, Michelle, and Sam Adler-Bell. "The Datafication of Employment," The Century Foundation, https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/.

[75] Brown, Lydia X. Z., Ridhi Shetty & Michelle Richardson, "Algorithm-driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination?," Center for Democracy & Technology, December 2020. https://cdt.org/insights/report-algorithm-driven-hiring-tools-innovative-recruitment-or-expedited-disability-discrimination/.

[76] Federal Trade Commission, "Amazon To Pay $61.7 Million to Settle FTC Charges It Withheld Some Customer Tips from Amazon Flex Drivers," February 2, 2021. https://www.ftc.gov/news-events/news/press-releases/2021/02/amazon-pay-617-million-settle-ftc-charges-it-withheld-some-customer-tips-amazon-flex-drivers.

[77] Caitlin Harrington, "Workers Are Trading Staggering Amounts of Data for 'Payday Loans'," *Wired*, March 23, 2022. https://www.wired.com/story/payday-loan-data/.

[78] Palmer, Annie. "How Amazon keeps a close eye on employee activism to head off unions," *CNBC*, October 24, 2020. https://www.cnbc.com/2020/10/24/how-amazon-prevents-unions-by-surveilling-employee-activism.html/.