**October 2021**
1st edition

Simply Secure

The New Design Congress

# The Limits to Digital Consent:

## Understanding the risks of ethical consent and data collection for underrepresented communities

Cade Diehm (The New Design Congress), Kelsey Smith (Simply Secure),
Ame Elliott (Simply Secure), Georgia Bullen (Simply Secure)

Within ethical design practices, informed user consent is a key requirement in the effort to invert the power imbalances fostered by the digital platforms that enable platform owners (organizations, governments, etc.) to build data profiles and make decisions about people. Much work has been completed by designers, activists, and aligned policymakers to translate data governance policies into plain-language and comprehensible consent. But the question remains: How well do these efforts account for the broader socio-technical power structures inherent in all personal data collection? Through a series of interviews with advocates for individuals and communities whose lives are often dramatically affected by data surveillance, this study finds that ongoing attempts to cultivate informed consent into data-driven systems likely fall short of their stated goals. The current implementations of ethical digital consent indicate that platform designers and policymakers have an insufficient understanding of systems complexity at scale, political accountability, the power dynamics inherent to organizational politics, and the second- or third-order effects of local-first data strategies. This study documents the inherent threats and risks for consent-driven digital technologies that current approaches do not address.

# INTRODUCTION

In response to the increased awareness of massive and invasive data collection on the lives of individuals and communities, platform designers and policymakers alike have sought to introduce new methods to help people better understand where their data is going.

One approach to rebalancing power in data practices is a digital consent system – a new type of user experience paradigm that communicates a platform designer's intent and obligation to the user with a focus on transparency, ethical governance, and trust. When someone enters the digital system, they are provided with a decision tree that allows them to signal their intent to grant or withhold consent to data collection. Despite a presumed common purpose, however, digital consent systems vary wildly in their execution. A common implementation is a system-level permission dialogue that is presented in the interface when a software application attempts to access a sensor, personal data, or other sensitive system[1]. These consent models are task and context driven – they interrupt a process the person using the application is trying to perform. Often, declining or withdrawing consent in these circumstances prevents the person from completing an action they are already invested in – and the user experience has commonly been exploited to increase the likelihood of a person granting consent[2]. Other consent systems, such as the European Union's General Data Protection Regulations[3], are more monolithic in nature. These implementations often legally require the platform designer to ask people to make a choice as soon as they enter an application or platform. This leaves little room for negotiation or the cultivation of a deeper understanding by the public of the implications of consent.

Current thinking around digital consent does not sufficiently address the risks inherent in individual participation in data-heavy digital platforms. Even for projects with explicit missions to empower people and their communities – such as Open Source or Federated collectively owned platforms – the potential for harm remains significant and the current paradigm does little to truly mitigate threats. Though this study provides only a partial snapshot of a complex and fast-evolving world, it reveals numerous shortcomings in the design of consent-driven digital technologies – highlighting the related threats and risks that many current approaches fail to address.

Current thinking around digital consent does not sufficiently address the risks inherent in individual participation in data-heavy digital platforms.

[1] https://www.apple.com/privacy/control/; https://developer.android.com/guide/topics/permissions/overview
[2] https://uxplanet.org/getting-to-yes-best-practices-for-ios-permissions-dialogs-9d62892142cc
[3] https://gdpr-info.eu/

# METHODOLOGY

This qualitative research study was conducted between June and August 2020. The needs-finding interviews were remote and informal, lasting 45-60 minutes and conducted via video chat. We spoke with five participants who were selected based on their experience working with underrepresented communities within the United States and United Kingdom. Participants were selected due to their professional work intersecting with underrepresented demographics and digital technology systems. Of the participants, four identified as female, one identified as male, and the selected group was racially diverse.

The composition of the participant pool was informed by the study's initial focus on disinformation and the 2020 US election. To be selected, participants were required to have on-the-ground perspective adjacent to underrepresented communities and sensitive situations, such as people and communities experiencing systemic injustice, living under oppressive regimes, or experiencing residential insecurity.

Participants were approached through a written invitation and subsequently expressed their understanding and consent to the interview process as per Simply Secure's research policies[4]. All participants received a stipend for their time.

The study was based on Socio-technical Security principles. Socio-technical Security is an emerging security research framework that "acknowledges how the interplay between actors produces emergent threats to participant communities," focusing on human relationships as the basis for a security model, rather than computing devices, software applications, or network connections[5].

Interviews explored five key questions:

1. What are the benefits for both the individual/community and a data-collecting organization of data donation/accumulation?
2. Who is most at risk, and how visible are they within common consent design paradigms?
3. How does data accumulation complicate the dynamics of these communities?
4. What does consent mean for these communities and situations? Including:
    a. The socio-technical or political effects of giving/granting consent to a digital platform or organization on individuals and their community, and
    b. The socio-technical or political effects of an individual withdrawing consent from a digital platform.
5. How can risks be lessened or de-escalated?

During interviews, the following general structure was observed:

a. Participant introduction: What is your role relative to your positioning as an advocate for a community?
b. How has the accumulation of data led to dangerous examples for communities? Who is most at risk? Why?
c. What harm minimization strategies have you witnessed in response to systems of data accumulation? From the community? From advocates? From platform designers, organizations, and technology companies?
d. For you, what is the worst case scenario when it comes to data accumulation in the browser?
e. What would make you more optimistic towards data accumulation?

[4] https://simplysecure.org/blog/participant-rights
[5] https://www.usenix.org/conference/foci19/presentation/goerzen

Notably, given that the focus of the research was solely on issues of consent, this study did not address any potential information security or technical implementation issues. In addition, the statements, impressions, and understandings provided by interviewees were not independently fact-checked – but instead taken at face value in order to best represent their perceptions of the risks of ethical consent and data collection for underrepresented communities.

# PARTICIPANT PROFILES

At the beginning of each interview, participants were asked to briefly describe themselves within the context of the study's focus. Participant quotes throughout this report are paraphrased and are acknowledged to be an accurate representation of an individual participant's contribution to the report.

**Participant #1**
*"I am a criminal defense lawyer, so I review evidence collected by federal agencies. I also work with political organizations that are concerned about surveillance, infiltration, and other forms of digital security. I see both sides: people who are trying to keep data private, and people whose data is working against them. Some years ago, I started doing activist work. This intersected with my work as a public defender when people became concerned with digital security. A lot of services and products went online. There was a proliferation of digital tools."*

**Participant #2**
*"I work in a leadership role at a nonprofit advocacy organization and have worked in large tech organizations before. I work in engagement and communities. I've been interested in digital privacy issues for a decade. It's important among marginalized and diverse communities, especially pertaining to black and brown people, women, children, seniors, ethnicities, people who are Muslim, and more. Digital privacy training needs to be more available and concrete. I'm interested in the intersection of technology and human rights. I want to know how to amplify voices, and build for, not against communities. I'm involved in understanding AI, surveillance, and facial recognition. Those have the potential to suppress communities – people like me. I also speak in advocate roles. I live in the US on a visa – I have been for a number of years. I worry that my work will affect my residency."*

**Participant #3**
*"I am an activist and advocate. I work within organizational power structures to instigate for change. I often ask myself, how do I make sure the people I'm advocating for are safe and getting the resources that they need? How do I make safe space for others to come in / take power / shape governance? I consider our job, collectively, is to decolonize the US government. Within my work I ask, 'What does shifting that power look like?'"*

**Participant #4**
*"I am a person. I use the Internet. I am a community researcher, especially for black people using the Internet and understanding how tech affects the marginalized from a research perspective. I focus on communication online and in general – how to communicate safely."*

**Participant #5**
*"I work at an anti-harassment organization. We work to make online space safer for all communities. I experienced online abuse and harassment and saw gaps in addressing the issues. I also saw gaps when hearing marginalized communities. Some years ago, we started as a campaign, later becoming a movement, and now we are an established charity. We focus on women and people who are non-binary – they are most likely to be targeted. We aren't just concerned with women as a gender, we consider intersectionality as well. We do advocacy work with government and technology companies. We fight for better platforms and long-term solutions."*

# KEY FINDINGS FROM INTERVIEWS

Each of the six findings below are supported by responses from one or more of the participants. The quotes included at the end of each finding are paraphrased summaries of key discussion points and are edited for privacy and clarity. Alongside the right to withdraw at any time during the study, each participant had the opportunity to confirm that the quote attributed to them accurately represents their participation in the study.

## Finding #1: The consent model for tech is outdated.

Today's digital consent frameworks are conceptually derived from institutional or academic ethics frameworks, yet digital platforms pose unique challenges that these frameworks are not equipped nor currently designed to address. This study finds that the lack of broader societal protections – such as the frequency of data breaches[6] and corresponding lack of corporate accountability[7], or the rise of algorithmic discrimination[8] and institutional misuse of data[9] – has led to an imbalance of power that significantly impairs the ability of an individual to give meaningful consent. As a result, people are forced to consent into a system that does not foster individual autonomy. Although ethical consent systems attempt to fully inform people about their data relationship with a platform, the complexity of modern digital systems, coupled with the cascading consequences of the broader network design of each ethical platform, ensure that the goal of ethically sourced and informed consent data collection is extraordinarily unlikely.

People are forced to consent into a system that does not foster individual autonomy.

The complexities inherent in digital systems, the requirements for ethical informed consent, and the design practices deployed as a part of human or human-rights centred design approach are at odds with each other. Current consent models are almost always designed as a one-size-fits-all approach for the most common use cases to consider, within which trust and the lack of trust are framed only from the perspective of the platform or researcher. In practice, these concepts fail to take into account the self-assessment of individual safety and self-preservation, which are complex and contextually regionalized. Further complicating matters, consent is often deemed to have been made on behalf of others who appear in a platform indirectly or as a result of interacting with a consenting user – yet those individuals have not been given the opportunity to consent themselves. Taken together, these issues reveal a consent model out of step with the goals of informed participation, power rebalancing, and individual agency.

**Participant #2:**
*"People are well aware of what's happening. They already consented so they go further down the hole, thinking, 'I'm never going to be president, with the things in my search history, it's going to be all in the public.'*
*As people are storing and creating, holding, selling data, consent is not prioritized. The companies are asking, how do we do this under the radar? Privacy policies are long and confusing on purpose. It's fake consent: we don't realize the implications."*

*"What are the ripple effects? People think their data is theirs. They own it. We know it's not. How is it going to be used? To improve your life or not? And what about those around you?"*

**Participant #3:**
*"You can never fix the data problem unless you fix the political problem."*

*"We need data sets and we need to allow for communities to opt in. Right now it's just Google and Facebook because they have big enough data sets. But the consent model is designed for the individual. If I opt in, I am consenting on behalf of others – this is irreconcilable with the current model. This is*

6. https://haveibeenpwned.com/PwnedWebsites
7. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
8 https://ainowinstitute.org/AI_Now_2016_Report.pdf
9 https://ainowinstitute.org/litigatingalgorithms.pdf

*smaller than the social contract but bigger than the individual."*

*"I have friends who don't give me their addresses because of their personal threat models. No consent framework exists today that takes this into account."*

**Participant #4:**
*"It's the amount of times you have to ask. The lack of change logs. 'We made this better,' but no one tells us why the previous one was bad. Trust is a thing that sounds good. There's not a sensible framework that they don't have. You want to be stewards – creating the space for stewardship to be possible."*

*"There is a lack of oppositional research in these programs. [Oppositional research should be] based on multiple identities and genders. They might introduce the best tool to protect data, but it's not for someone who doesn't have a social security number for instance, so it's not usable. Lack of trust does not have to be malicious, it could be self-preserving. When it's not built for me, trust is lost."*

*"Gaining a better understanding requires an interdisciplinary approach at the start, not the middle."*

**Participant #5:**
*"I had to self-teach around data accumulation and privacy because of [my job]. It's not easy to understand. The whole topic needs to be demystified. Even the term 'data accumulation,' I get it, but having to explain it to someone else... not so easy. People don't see it as a priority."*

## Finding #2: Local-first data storage is not inherently safer for people or communities.

The collection and ownership of personal data by an organization creates a significant power imbalance[10]. In response, platform designers may turn to a "local-first" approach to data storage, in which an individual owns and controls their data in an ethical digital system. This "local is better" assumption is helpful for mitigating issues related to data abuse or company control, and is frequently proposed as a useful technique for rebalancing the power dynamic between people and organizations. Yet such a proposition does not consider its implications beyond these immediate relationships, nor how assigning data ownership to an individual can amplify power discrepancies between the individual and other non-associated parties. In particular, the "local-first" data ownership paradigm introduces vulnerability to people who might be the target of harassment from technically sophisticated antagonists[11] or prejudice from law enforcement[12].

In a centralized system, an organization can employ digital security or legal[13] expertise to fight attempts by third parties to access data beyond their interests or the interests of the consenting individual. But in a local-first data ownership system, the risks of data accumulation are placed on the individual. Accessible by targeted technical attack, search warrants, extrajudicial investigation, or theft, the local-first data storage approach (including cached data) adds vulnerability and complexity into people's lives, and has been successfully used for years to prosecute targeted individuals[14], generate narratives for state-facilitated oppression[15], and overwhelm judicial institutions.

In a local-first data ownership system, the risks of data accumulation are placed on the individual.

**Participant #1:**
*"With a warrant they can look at your local device. But a search warrant is just one method of collecting data for the investigation. They can get a warrant based on speculation."*

*"They use services like* Cellebrite *for extraction. The report is a map of everything: contacts, browsing history, erotic sites, deleted files, etc. These types of requests are routine, so the companies that do it are no longer a specialty. It's the push of a button. And they have so much data. My suspicion is that they are so overwhelmed with data that they just ignore the stuff that's hard. For high profile cases, there are lots of resources and they'll spend more time trying to crack a phone or digging through messy data. It's useful for us to understand how the actual process is being used by an adversary, such as the government. It's an index key word search of every file on your machine."*

*"The remote is harder to access. In some ways it's harder to get things off a remote server. But fundamentally, it's not that different. It's just harder for them to know what's there, and it's harder to control. Unless the provider is helping them out, which many do."*

**Participant #4:**
*"Risks are multiple, intersectional. What makes it risky is mitigated by other factors. What are the things that are risky for people? And design for that? There are differences between persons who are undocumented, persons in the systems but waiting for documentation, and those with undocumented relatives. But when we research we study just 'undocumented.'"*

[10] http://en.collaboratory.de/w/Power_in_the_Age_of_the_Feudal_Internet
[11] https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[12] https://ainowinstitute.org/AI_Now_2016_Report.pdf
[13] https://www.techdirt.com/articles/20130618/14341223521/google-without-ad
[14] https://www.eff.org/wp/riaa-v-people-five-years-later
[15] https://simplysecure.org/resources/techreports/NYC15-MobMsg.pdf

## Finding #3: Data creation, including the potential for data creation, is silencing.

The accelerating rate and scope of data collection, combined with increasing community awareness and savvy surrounding the dangers posed by such datasets, produces a chilling effect on those who wish to speak up and self-advocate but hesitate to do so due to the associated added risk. In a broader social context, recent examples of the chilling effect of data collection include the rise in public awareness of how behavior in social media has direct consequences for health insurance[16] or financial stability[17], as well as the rising awareness of personal data purchased by US armed forces from apps used by religious minorities[18]. Beyond the public sphere, data accumulation reduces the range of voices through the process of data deanonymization[19] – a fact that the public is becoming increasingly savvy to.

The chilling effect of data accumulation is cascading. Data accumulation perpetuates inequalities through the ripple effect of interpersonal relationships that can be inferred or measured via data. Well-known examples of this include Facebook's efforts to build shadow-profiles on individuals[20] beyond the company's ecosystem by using data accumulated from invasive collection activities of the company's user base. Ethical data collection and processing has not satisfactorily provided meaningful assurance or technical solutions to ensure that such a system will not be subject to unintended social graphing, deanonymization, or shadow profiling. Once the data is created and collected, people are unable to monitor the broader analysis process their data will be subjected to. As such, an ethical consent system remains unsuitable for those who cannot – or are unwilling to – bear the risk of being subjected to these activities.

The chilling effect of data accumulation is cascading. Data accumulation perpetuates inequalities through the ripple effect of interpersonal relationships that can be inferred or measured via data.

**Participant #1:**
*"A lot of people are more and more cognizant of their data trail. They have strategies like turning off the phone, having two phones ('protest phone'), or leaving their phone in the other room."*

**Participant #2:**
*"The new laws in the US like Muslim bans (and other communities) have targeted me. ICE [Immigration and Customs Enforcement Agency, a federal US Government agency] can have access to my social media accounts at any time. Are those programs active? It's unclear to me. But I think they have access to snoop on me and collect my data. And it's dangerous – I might push the line and they can revoke my status. If I were undocumented, that would make it so scary. [People who are undocumented] can't be vocal or stand up for themselves. That's the power that data can have."*

*"The advancement of trolls, in the early days of misinformation and harassment led to distrust in the platform (Twitter), around 2012. When that happened, the trust in the platform was jaded. You couldn't open yourself up to the*

[16] http://www.idpublications.org/wp-content/uploads/2014/09/ANALYSIS-OF-INSURANCE-UNDERWRITING-USING-SOCIAL-MEDIA-NETWORKING-DATA.pdf
[17] https://www.researchgate.net/publication/272300274_Credit_Scoring_with_Social_Network_Data
[18] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[19] https://zviewcontent.cgi?article=1016&context=hightechevents
[20] https://www.europarl.europa.eu/resources/library/media/20180524RES04208/20180524RES04208.pdf

*place. Those problems have gone on to be big problems elsewhere too."*

*"The vulnerabilities are key issues. We know some of them and we don't know some of them. We are most vulnerable when we don't know them. Like for Clearview AI: we are so vulnerable. I am in the small part of the population that knows about them. Their practices are hidden, below the radar."*

## Finding #4: Everyone – not just members of underrepresented communities – is at risk.

The current industry framing of privacy and network threats is heavily influenced by colonial bias, drawing the majority of its guidance and framing from "empirical evidence on Western-based, white, and middle-class demographics."[21] These shortcomings create blindspots that allow threats to thrive, affecting entire communities who fall outside of this narrow definition. Interviewees described the often unexplored, or downplayed, risks of data creation and collection, noting that data footprints generate vulnerability for almost everyone. Simplistic mechanisms of opt in/out consent, the challenge of understanding data collection within the context of complex systems (as described in Finding #1), and the loss of control over the collected data directly threaten marginalized communities, but also pose risks to the general public (in part because one can never fully anticipate a transition of an individual or community into a destabilized or marginalized situation). In order to mitigate the broader, society-wide risks associated with data collection and consent, participants advocated both for a deeper understanding of the institutional and colonial biases inherent in privacy studies, as well as for platform designers to develop sensitivity to this transition of users or communities into precarious or destabilized situations.[22]

Current data collection can – and almost assuredly will – be used to feed future technologies whose risks are impossible at present to understand, predict, or mitigate.

Future use of collected data is particularly problematic. Current data collection can – and almost assuredly will – be used to feed future technologies whose risks are impossible at present to understand, predict, or mitigate. Time and again, even well-intentioned or purportedly neutral datasets have produced disastrous impacts. Early facial recognition datasets, for example, were later revealed as refined tools for perpetuating racial inequities, enabling authoritarianism, and training machine learning or algorithmic governance systems[23].

**Participant #1:**
*"Keystroke logging [is the worst case scenario for data accumulation in a web browser]. In some sense, it's the increase in surface area. Activist/political perspective: crime is ideological. Site history to prove terrorism. 52,000 antifa search hits or on the harddrive. Maybe it's not even used as evidence, it's just said to a judge. Maybe it doesn't mean anything, but it adds to the narrative. They are just playing on prejudices and stereotypes and expanding on the bad guy persona."*

*"Social media posts could be used for any purpose. If someone posts a meme that says "focus" and you like it, they can say, 'you were focusing on the crime!' It's building narratives from anything in the social graph. There's nothing stopping them. They'll use anything.*
*It could be something that's not at all incriminating. Like a picture of food or friends: 'You took a selfie? So then you can't be injured or whatever.'"*

*"It could also be something related to immigration: a person wants to reunite with their deported spouse. Yet, the agent sees*

[21] https://journals.sagepub.com/doi/abs/10.1177/1527476418806092
[22] https://cdn.ttc.io/s/tacticaltech.org/smartphone-as-lifeline.pdf
[23] https://news.bloomberglaw.com/privacy-and-data-security/dating-site-profiles-capture-prompts-privacy-violation-lawsuit

*pictures of that person going out, having fun. Then they say, 'Oh, you don't want to reunite with your spouse? You're going out and having drinks?' That can be used against you. It's difficult to say you have no associations – everyone is connected. Those connections are enforced by the data out here."*

**Participant #2:**
*"It's obvious, we are going to find out that a lot more people are at risk than we thought. With facial recognition, AI, etc., and the inequities in the black and brown communities. Data collected on them is used against them. For immigrants, undocumented immigrants, and visa holders, so much of their data can be called up."*

*"For women, it's doxxing and women are suffering. Communities, genders, ethnicities ... Ethnicities being torn apart online."*

**Participant #4:**
*"Once data collection became a business people didn't know how to stop it. Data is more important than the product. At the same time, when people advise you to get off Facebook, I think 'where would you like to migrate the millions of people who use Facebook as the internet? And you insult them at the same time?' I don't actively use Facebook, but I am not going to delete my account. I have family members around the world. That is the platform that they can use. My great aunt is not going to figure out another platform."*

**Participant #5:**
*"Everyone is at risk. There is a knowledge gap online. There is a lack of understanding how platforms work, digital citizenship. It's across the board. Men don't realize the way they use the platform could perpetuate harm. It's making the situation worse with violence against women. This is completely under-researched and the social biases are apparent. Allyship is important for tech justice. Not just making the platform safer, but for other people to know what's going on."*

## Finding #5:
## Ethical platform designers must consider themselves as the potential bad actor.

While those who demand design justice and ethical platform development are well-intentioned in their pursuit of empowering people and communities, the reality is many recent dangerous technological advances started out just as well-intentioned before resulting in systemic abuse or worse. Institutional change beyond the control of a platform designer, and sometimes occurring far after a user base has given consent, can easily lead to the introduction of situations ripe for exploitation. It simply is not possible for even the best-intentioned designer to accurately foresee changes in partnerships or leadership through which carelessness or ulterior motives may poison a platform's original values.

Both directly and indirectly, participants criticized the mistaken optimistic assumption that institutional cultures that govern collected data either share or will maintain the political and social values held by a team of platform designers. For digital consent, the belief in the institution is often paired with design ethics, preventing platform designers and policymakers from deeply interrogating the impact of their work[24]. Institutional alignment is difficult to measure, and training in digital ethics can often fall short of expected or desired organizational cultural change[25].

When building a digital consent system, the potential for weaponized design[26] should be examined by the team responsible for implementing the consent system. This could take the form of a conceptual and governance intervention through both participatory design with community members and critical engagement with practitioners familiar with Socio-technical Security and threat modelling practices (e.g., the Trike security framework[27]) to ensure that a digital consent system is not implicated in a designed system that harms users while performing *exactly* as designed.

Participants criticized the mistaken optimistic assumption that institutional cultures that govern collected data either share or will maintain the political and social values held by a team of platform designers.

**Participant #2:**
*"Talented tech-savvy people are getting all data about a woman, and using it in ways that can be deadly."*

*"We are eager to build tools without thinking of the implications. Once we are done with Covid, what happens to the data and technology, will people still use it? Once data and technologies are out there, it's out there for good. There's no going back. People create things and say, 'I never imagined it would be used for this.' The trickle effects are scalable. Scary things like the Facebook scroll that destroyed the attention span of the population. It was never intended that way. We are using these technologies in ways we never imagined. There aren't enough people and guards to set up for limitations and understanding how to protect those people."*

**Participant #1:**
*"There is a conflict with the business model of companies. It's antithetical to how they make*

[24] https://tv.undersco.re/videos/watch/f769b6e4-d992-4a73-bac1-b05ee6116368
[25] https://people.engr.ncsu.edu/ermurph3/papers/fse18nier.pdf
[26] https://newdesigncongress.org/en/pub/on-weaponised-design
[27] https://www.octotrike.org/

*money. Google's business is the collecting, forming, and selling model. Google is just an example, there are a million others. That's the game. It's irreconcilable. We have to acknowledge that exists. It's hard to deal with and grapple with. Being aware of that is going to be useful for a minimization analysis. It's not just what you think you're doing that's being collected. It's not just you doing bad things that can be used against you. It's everything. Where you were, where you weren't. Your phone was turned off, turned on. Anything."*

**Participant #3:**
*"Bad stewardship of data is a huge problem. It doesn't matter how you address this in the moment, without solving for data protection, the political context or motivations will change. You can be sure of that. You can encrypt or otherwise try to protect it, but it is too tempting to use datasets beyond their intended purpose. Power shapes the usability of data, not just the data itself."*

*"What companies do internally matters when they are trying to engage with underrepresented communities. Why should these communities trust these governance models when they can't govern themselves with community responsibility?"*

**Participant #4:**
*"Researchers do not respect people enough. I've learned that over the past decade. Research does not look like the actual spaces. The research community should be apologizing. [The labels] 'Alt-left' and 'alt-right' are offensive. It leads to 'cancel culture' and anti-vaccine beliefs. You do not have black researchers, researchers of color, multiple generations of the Asian diaspora. Has any researcher talked to actual users? What about popular research methods for research with younger people? How are you going to do this work if the generation has not passed the age of majority? How are you doing it so that it is good and kind? I don't think it's responsible. Every study should be opt-in, regulated. At this point, there may be 16 different centers, all doing the same research."*
*"I often hear about efforts to incorporate differential representation – yet everyone needs a PhD to enter. The thought is that research is not worthy unless you have a PhD. How will your methods be for people who don't have high school diplomas?"*

**Participant #5:**
*"The mainstream tech companies are like life and death for some people. They use tech for their sexual expression so they have to be careful depending on their situation. They cannot accept dangerous data accumulation – there are massive repercussions. That's where the alternative tech comes in. My worry is, big tech will buy them all out. What is going to happen in five years' time? Like Fitbit? There is no incentive for tech companies to do the right thing. We need a regulator."*

## Finding #6
## Participants are overwhelmed by both the potential for harm and the indifference of decision-makers.

Underlying all participant interviews was a recurring theme. They – along with the communities they represent – are intimidated by past and current issues, and paralyzed by the scale and potential of harm, as well as the real or perceived institutional resistance by technology companies and legislators to tackle these problems. Participants repeatedly expressed skepticism over the successful creation of a new platform capable of true ethical data collection and custodianship – even one operated by a recognizable stakeholder with a reputation of advocating on behalf of individuals and communities.

**Participant #1:**
*"Accumulation of data is a nightmare. It makes everything so difficult. For me, it makes it impossible to know the full scope of the evidence. The massive amounts of data makes it difficult to form a defense. I don't know what they're using against you. Before, you could assume they didn't have evidence, now it's flipped, you have to assume that they have evidence. Most lawyers don't have tools or time. There's a huge processing power imbalance, combined with ignorance and fear. The prospect of putting that in front of a jury, it's a rough game. They are over-collecting data. The government can't deal with it all. And it helps them more – all presumptions are in their favor. It completely overwhelms the defense; it's like looking for needles in a haystack. The more they collect, the less I can do my job. They are not required to tell you what they want to use. I have a duty to look through all the data. Hardly anyone has the capacity to do this work. They'll use anything to convict."*

**Participant #2:**
*"I'm timid to suggest benefits of data donation. Overall it depends on regulations and policies. I know not all companies are awful. If there are regulations and if organizations are stipulated, it has the potential for greatness. But I see too much harm."*

**Participant #3:**
*"When I participate in health research, my immediate fear is legal protections and techniques for anonymizing data. I worry about insurance companies – how anonymized is anonymization? My health profile is very unique. I want to believe in the power of data research. I am a short-term pessimist, long-term optimist."*

**Participant #4:**
*"There is a difference between the need for systemic change and constantly reinventing and making things that don't work. That is where intersectional intervention from the start and clear communication comes in. Safety moderation, for example, is now a gig [unpaid community moderation]. Email is another example, where you are overwhelmed by administering your inbox. You have to spend your time making sure you are unsubscribed."*

Participants repeatedly expressed skepticism over the successful creation of a new platform capable of true ethical data collection and custodianship.

*"People are gearing up – trying to figure out what will and what will not work. So much is on the fly, in the moment. The problem is not that it's reactive. Advocates often yell for help, but don't get listened to, don't get what they need to help mitigate. Help from technology vendors is often paternalistic."*

**Participant #5:**
*"Because violence against women is a*

*continuum. It started offline, continued online. Facebook started as a way to rate women. With the murder of George Floyd, people just started thinking 'maybe we should be stop being so white and so male.' Twitter Voice was introduced recently, and women could have told you how it could be used against them. Although the team who managed it was black, when you ask if the team was diverse? You get crickets. That is the problem."*

# Conclusion

This study engaged five participants as community representatives from the United States and the United Kingdom to produce qualitative research examining the efforts to produce digital consent systems that seek to rebalance power between people and communities, and data-collecting organizations. These interviews were combined with a review of the historical and current issues related to data collection in an effort to critically examine whether digitally-facilitated consent actually represents an individual's informed understanding of the implication of that consent – both for themselves, their own personal relationships, and their wider communities. This study concludes that efforts to refine digital consent with these objectives in mind have not succeeded.

Data accumulation has great power over a person's agency, their relationships, and the communities within which they operate. The associated harms are therefore pervasive and reach almost every human being. Current and proposed implementations of platform-facilitated data collection employ a trust-promotion or informed consent model, where people make a decision about the trustworthiness of a platform and consent to that platform accessing or generating data about them. Digital consent is derived from decades-old evolutions in participant advocacy in social and health sciences,[28] and it is often combined with dominant human-centered design paradigms – such as designing for obviousness via simple language and frictionless interfaces – to provide coherent interfaces when asking for consent.[29] Ethical digital consent further builds upon these

This study concludes that efforts to refine digital consent have not succeeded.

While consent models serve the humanities well, they are unsuitable for technology design.

[28] https://kantarainitiative.org/confluence/download/attachments/101811330/MEF-whitepaper-understanding-digital-consent.pdf?api=v2, https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview

Practitioners must examine the systemic shortcomings of digital consent and commit to an ongoing iteration of consent and data governance within platforms. Platform designers and policymakers must not assume that collection is safe, and in turn must design data storage systems accordingly.

practices, employing frameworks such as the Design Justice Network's Network Principles[30] or Society-centered design[31] in an attempt to negotiate and rebalance power within digital systems. Yet while these consent models serve the humanities well, they are unsuitable for technology design.

In general, today's popular digital consent paradigms fail to address the issues identified by the participants in this study. The gaps between the goals of digital consent implementation and the reality of outcomes for communities and individuals were described by both the interviewees as well as the study's literature review. Each participant expressed resentment or frustration towards institutions, driven by specific regionalized examples of harm caused by digital systems. Common to each participant's experience was that material risks or poor outcomes experienced by participants or the communities they represent are amplified by digital platforms, and that digital consent failed to account for these realities. In some cases, participant resentment was driven by what they considered to be willful ignorance of the ramifications of data accumulation by those who design these systems and the platforms and pathways for bringing people into these systems. In others, resentment was drawn from direct experience of institutional marginalization in either a professional or personal context. Many communities that our participants either identify with or have advocated for have been subject to intergenerational institutional violence and rightly continue to combine these historical impacts with contemporary experiences in formulating their own models for self-preservation and safety.

Going forward, practitioners must examine the systemic shortcomings of digital consent and commit to an ongoing iteration of consent and data governance within platforms. Platform designers and policymakers must not assume that collection is safe, and in turn must design

[29] Krug, Steven. Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability, New Riders, 2014.
[30] https://designjustice.org/read-the-principles
[31] https://societycentered.design/

data storage systems accordingly. This includes on-device local storage. A common assumption inherent to designed systems of consent and data accumulation/ownership is that the organization the designer represents maintains the same values around privacy and trust, and that these values will be maintained indefinitely (or at least as long as the data remains useful). Yet in practice the political framework for those in custodial control of datasets can change drastically and quickly – posing a risk to all whose data was collected.

Regarding organizational change, data governance often fails to anticipate second- and third-order effects, such as abuse or harm facilitated by a partner organization and assisted by seemingly unrelated collected data, or institutional racism drawn from conclusions within a collected data set. These detrimental effects can also stem from a data breach or other action taken by someone outside the collecting institution. They all must be accounted for.

Yet regardless of designer intent, the public is gaining a better understanding of the consequences of the often false assumption of aligned values between designer and institution, as well as the unintended effects of dataset abuse during organizational or societal political shifts. This expansion of knowledge brings an increasing expectation of accountability on behalf of data custodians. For platform designers, meeting these heightened expectations requires careful assessment of local-first and centralized data governance models. Considerations should also be taken to research and develop mitigation strategies for problems of data accumulation within the person's device and beyond, including custodial ownership of the larger dataset over time.

Whether seeking to deploy private analytics or develop partnerships for ethnographic research, platform-based personal data collection and analysis comes with a high degree of fast-moving risk. Platform designers must therefore develop a set of sensitive and direct plans for navigating unexpected scenarios in which they or an associated organization with platform access suffer a public collapse of social trust. Notably, these scenarios will likely unfold outside of the platform designer's control, restricting their ability at that time to deploy crisis management strategies or modify their system for informed consent. But that does not mean that they cannot be designed for. And they should. That's why a platform designer who positions themself as an advocate for internet privacy and self-determination must utilize an expanded systems approach to consent, take on a broader understanding of the risks of data accumulation, and be unafraid to employ a combined design/communication strategy that not only acknowledges but embraces the likelihood of digital threats in order to mitigate them and obtain consent.

# ABOUT

This study was supported by Reset, an initiative engaged in programmatic work on technology and democracy. Reset seeks to change the way the internet enables the spread of news and information so that it serves the public good over corporate and political interests – ensuring tech companies once again work for democracy rather than against it.

The research behind this study was conducted, in part, to help support and inform consent work related to Mozilla Rally.

The New Design Congress

**The New Design Congress** is a Berlin-based research organization that recognizes all infrastructure as expressions of power, and sees interfaces and technologies as social, economic, political and ecological accelerants. The organization is a fiscally sponsored project of Simply Secure.

Simply Secure

**Simply Secure** is a women-led nonprofit working to transform the current design paradigm in tech by centering the needs of people as the guiding principle. Through educational programs, resource building, and open research partnerships, we are decentralizing the power of digital design by increasing the number of people who can perform the essential tasks that shape our collective online future. We envision a world where everyone – particularly the most systematically underserved – has the knowledge, network, and digital tools needed to enrich their lives.


1st Edition, September 2021

newdesigncongress.org
simplysecure.org