DATA&
SOCIETY

Organization Information

1. *Name of organization*

Data & Society Research Institute (DBA Data & Society)

2. *Discuss the founding and history of the organization.*

Data & Society was founded in 2014 by researcher danah boyd to advance strategies for change in how data-centric technologies are understood and governed in society. Since its founding, Data & Society has grown from seven researchers based in New York City to over 45 staff members across the United States and abroad. During that time, we have grown as an organization, built a strong board and governance structure, and brought on an experienced and values-driven senior leadership team. As an institution, **we are equally committed to research and engagement**, ensuring the impact of our findings in policy and media spheres. Our theory of change rests on the belief that quantitative evidence, though valuable and necessary, is not sufficient for understanding the social implications of data-centric technologies.

From the beginning, our work has been animated by a set of core concerns:

1. Data-centric technologies have social, cultural, and political implications that are far-reaching, unevenly distributed, and poorly understood.
2. These technologies' negative impacts disproportionately harm marginalized populations.
3. The concentration of power in the tech industry has significant implications for both democratic practice and the governance of data-centric technologies.

Over the past three years, these concerns have become central to the work of many advocacy and research organizations in our field; to policymakers at various levels of government; and to the broader public. This shift is both a result of our work (and that of many partner organizations in our network) and an opportunity to push further.

Since we were founded, understanding and securing internet privacy has been central to Data & Society's mission. Some examples of our work in this area include:

Empirical Research

- *Privacy, Security, and Digital Inequality*, which provided the first in-depth analysis of the digital privacy and security experiences of low socioeconomic status populations in the United States.
- *The Wisdom of the Captured*, which analyzed how users may be negatively impacted by the internet-mediated data collection tools which enable automated technologies to make intelligent decisions.
- *Assembling Accountability: Algorithmic Impact Assessment for the Public Interest*, which discussed privacy impact assessments and their value in assessing accountability of algorithmic systems.
- *Fairness in Precision Medicine*, which was the first report to deeply examine the potential for biased and discriminatory outcomes in the emerging field of "precision medicine."
- *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech*, which explored how consumer monitoring, audience-targeting, and automated technologies have been weaponized by political and anti-democratic actors to increase their influence.
- *Digital Identity in the Migration & Refugee Context*, which focused on how the migrant crisis was used as an excuse for pervasive biometric data tracking and collection—with no ability for these vulnerable populations to opt out.
- *The Constant Boss: Labor Under Digital Surveillance*, which looked at the changing social conditions of workplaces that pushed for worker data protection and privacy to enable workers to advocate for their rights.
- *Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care*, which discussed how workers and patient employers submit to privacy-disrespecting geolocation and biometrics as part of the changing nature of care work.
- *At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers*, which connects the rise of home doorbell cameras to a broader erosion of privacy, which in turn has undermined the working conditions and labor rights of precarious, low-wage workers.
- *Essentially Unprotected: Health Data and Surveillance of Essential Workers During the COVID-19 Pandemic*, which followed how misunderstandings of privacy regulations (and their ability to keep up with new and changing technologies) produce harm for workers.

Policy Publications

- *Response to the FTC's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*, which advocates for rulemaking to combat extractive surveillance practices that harm consumers and impede a just American technology ecosystem.
- *Democratizing AI: Principles for Meaningful Public Participation*, which offers evidence-based recommendations for integrating public participation into the AI development and implementation life cycle.
- *Algorithmic Accountability: A Primer*, which looks at the growth of harmful trends surrounding data privacy and collection, among other accountability issues.
- *Response to the White House OSTP's Request for Information on Automated Worker Surveillance and Management*, which highlighted the grave risks that automated surveillance and management tools present to workers.
- *Policy Brief* for the *Electronic Visit Verification* report listed above.
- *Policy Brief* for the *Assembling Accountability* report listed above.

3. *Describe the organization's current goals.*

We envision a future in which the values that inform the design and governance of data-centric technologies are visible and intentionally chosen with respect for human dignity and just outcomes. Governance of new technologies is often rooted in **assumptions** about how that technology *might* impact society. These assumptions often stem from extreme utopian or dystopian narratives, rather than an exploration of nuanced trade-offs. Instead, we believe it is critical to build governance around the documented **experiences** of people who live with the technology in question.

The overall goals of our work include:

- **Changing the terms of debate** by working with media and policymakers to advance human-centered and empirically grounded public discourse on technology and society issues;
- **Shifting power** by foregrounding the communities most impacted by data-centric technologies, we argue for approaches to technology design and governance that are grounded in equity and just outcomes; and
- **Shaping policy and practice** by translating research findings for policymakers with the goal of advancing rights-respecting, human-centered, and empirically grounded governance of data-centric technologies, including artificial intelligence and algorithmic systems.

Each of our projects also pursues individual goals that relate to its respective topic and intended audiences. For instance, past projects have sought to protect workers from commercial surveillance; create safe and secure online spaces for marginalized communities; and develop methodologies for assessing AI's impact on protected groups and communities to inform governance.

4. *Provide a brief description of the organization's current programs.*

Our core research programs work alongside our policy and engagement teams to ensure this research can be used to affect real-world change. Below we have provided a brief overview of each program:

Current Research Programs

- **AI on the Ground**. This program develops robust analyses of AI systems; effectively assesses their impact; and informs their future design, use, and governance. Our team recently launched the Algorithmic Impact Methods Lab (AIMLab), which brings together various partners to engage in an interdisciplinary approach to designing and piloting public interest methods for algorithmic impact assessments.
- **Labor Futures**. This program uses ethnographic research to better understand emergent disruptions in the labor force as a result of data-centric technological development, with a special focus on privacy and structural inequalities. Our team strives to center workers' concerns in research and action in order to envision just futures for labor in data-centric work environments.
- **Trustworthy Infrastructures**. This program works alongside marginalized groups to understand emerging approaches to building trust online, as well as the possibilities these practices set in motion. Rather than simply diagnosing threats and naming harms, our research aims to inform and advance effective sociotechnical solutions that reflect the knowledge and expectations of the communities that have been disproportionately harmed by the status quo.

Current Engagement Programs

- **Policy Engagement**. Our policy team works alongside our research teams to translate rigorous, empirical social science for multiple audiences and create actionable learning and policy recommendations for key targets and partners. They work closely with academic and policy research bodies; government institutions; civil and human rights advocacy groups; and community-based

organizations. Our policy work currently focuses on opportunities at the federal level, particularly with executive agencies that are directly engaged in developing and implementing new approaches to governing artificial intelligence and data security.

- **Public Technology Leadership Collaborative (PTLC).** This peer learning collective, led by Data & Society in partnership with ten academic research centers, creates knowledge communities between government decision-makers and scholars grappling with the use, study, and regulation of data-centric technologies and artificial intelligence. The PTLC offers a dynamic slate of programming—including workshops, seminars, and salons—that are intentionally informal, private, and focused on cultivating trust and sharing context. Past programming has focused on building responsible AI, fostering trust in technical systems, and incorporating public participation into the development of new technologies.
- **Media Engagement.** Our communications team builds and maintains relationships with national and global media outlets to ensure the circulation and visibility of our work. Their proactive media engagement strategy incorporates educational and convening opportunities for journalists, editors, and publishers to develop specialized knowledge in areas related to D&S research. The team also provides bespoke media training to our researchers and senior leadership to ensure they are prepared to engage with various audiences and media spaces.

5. *Has your organization ever received a prior cy pres award? If yes, please cite the applicable case(s), identify the amount(s) awarded, and describe the nature and scope of the project(s) funded.*

We have never received a prior cy pres award.

6. *Has your organization been reviewed or rated by Charity Navigator or similar entity? If yes, what are the organization's ratings?*

We have a 100% 4-star rating on Charity Navigator. This is the highest rating possible, indicating that our organization "exceeds or meets best practices and industry standards across almost all areas."

Grant Proposal

7. *Identify the organization's principal investigator or project director.*

The project director will be Executive Director Janet Haven. She will be supported by:
- Policy Director Brian Chen;
- PTLC Program Director Charley Johnson;
- AI on the Ground Program Director Jacob Metcalf; and
- Labor Futures Program Director Aiha Nguyen.

8. *Provide a summary of the plan for the program or project request. Include the issue and/or opportunity addressed, goals and objectives, activities, and timeline.*

Concern for privacy has been a critical throughline of Data & Society's work from the beginning. The current lack of federal data privacy protections, such as those proposed in the American Data Privacy and Protection Act, leaves every American vulnerable to well-documented harms caused by widespread data collection, retention, and use practices. These practices often violate norms and assumptions that individuals hold about privacy, as well as their fundamental rights and core values. We have repeatedly seen the tech industry ignore the laws that are put into place to protect consumers from invasive data collection measures, simply because they believe the value of a big data set will outweigh legal ramifications[1]. When we do see companies take steps to put privacy controls in place, these measures are often coercive (i.e., terms of service agreements) and based on the idea that each and every person will take individual responsibility for the protection of their privacy (i.e., Facebook's privacy settings dashboard). Finally, our research has shown that online privacy violations harm vulnerable and low-income populations in a distinct and often overlooked manner. While these communities clearly understand the risks and harms associated with data collection, they often lack the legal protections, tools, and strategies needed to take action to sufficiently protect themselves[2].

The issues of online privacy and data protection have become even more pressing and complex with the launch of retail generative AI systems like ChatGPT. These systems are trained on data scraped from across the internet without permission, opening a broader debate about data privacy protections and the role of individual agency within them.

[1] Lane et al. (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014).
[2] Mary Madden, *Privacy, Security, and Digital Inequality* (Data & Society, 2017).

Indeed, the Biden Administration's Blueprint for an AI Bill of Rights includes data privacy as one of five core principles for building safe and rights-respecting AI systems, arguing that Americans "should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used."[3]

And yet, current legal doctrines on privacy have ossified in the face of modern data extraction and online privacy abuse.[4] Many privacy harms are small but numerous, and they can also scale up rapidly. A breach of privacy may be an inconvenience to an individual; but when it happens to millions of people, the aggregate harm is meaningful to society. Because the law fails to recognize many privacy harms—other than those that are highly individualized and financial or physical in nature—the networked and highly distributed impacts of data technologies are often not remediable by courts.[5]

To address this, we would like to leverage Data & Society's research and engagement expertise to focus on the concept of "collective" or "networked" privacy. This will entail a framework shift—including research, narrative, and policy work—to account for communal privacy harms in data-centric and algorithmic environments. By looking at the forest, and not just the trees, we aim to demonstrate how the privacy harms wrought by AI and other algorithmic systems are experienced most acutely at the collective level—and therefore must be contested there.

We plan to address this topic by building on our already-robust work on privacy to bring a focus on collective privacy to all three of our research programs. Past research has shown that harmful data collection practices and subpar privacy regulations inflict greater harm on marginalized and disadvantaged communities[6]. By taking up collective privacy as a framework for both research and policy, the next phase of our work will focus on how unprotected internet and digital spaces abuse our privacy, how those impacts are measured, and how new approaches to governance can mitigate these harms altogether.

---

[3] "Blueprint for an AI Bill of Rights," The White House, 2022, https://www.whitehouse.gov/ostp/ai-bill-of-rights/#:~:text=Data%20Privacy,-You%20should%20be&text=Systems%20should%20not%20employ%20user,be%20appropriately%20and%20meaningfully%20given.
[4] Citron and Solove, "Privacy Harms," *Boston University Law Review 102,* no. 793 (2022).
[5] Indeed, recent research from our AIGI team has demonstrated that algorithmic harms share this challenge with privacy harms, indicating the need for new regulatory interventions that can provide recourse to people and communities injured by algorithmic systems. See Metcalf et al., "Taking Algorithms to Courts: A Relational Approach to Algorithmic Accountability," in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1450–1462 (Association for Computing Machinery, 2023), doi:10.1145/3593013.3594092.
[6] Alice E. Marwick, *The Private Is Political: Networked Privacy and Social Media,* (Yale University Press, 2023).

Goals and Objectives

The long-term goal of this focus is to explore **collective privacy as both a social concept and a usable governance framework.** Our work will help determine the gaps in our shared understanding of **internet privacy for both individuals and groups, as well as potential remedies to address harms when they occur.** In doing so, we also plan to:

- Deepen relationships with the communities most impacted by internet privacy violations to ensure we take an inclusive and participatory approach our research and engagement;
- Pursue new research topics in our core areas of concern (i.e., health, labor, platform governance, trustworthy infrastructures, vulnerable communities, and AI governance) that bring together insights on collective privacy from multiple sectors; and
- Inform government leaders and policymakers about the risks, conditions, and pitfalls of regulations surrounding privacy online, with a particular emphasis on the importance of collective privacy.

Activities

This award would allow us to greatly increase our capacity for dedicated research and engagement on internet privacy, including new research into the undertheorized area of collective privacy as well as direct collaborations with policymakers and government leaders.

Engagement Activities

Our policy engagement team, led by Brian Chen, and our Public Technology Leadership Collaborative, led by Charley Johnson, already do extensive work with government leaders and policymakers, and these connections will be very beneficial to us as we seek to move our research on collective privacy into policy impact.

These teams already have experience working with government personnel on issues relating to internet privacy, including:

- Legislative work with federal and state lawmakers to promote statutory privacy protections, including sufficient notice, guaranteed transparency, and proper accountability when people's data is collected through technology;

- Leading responses to regulatory requests from the FTC in the context of consumer protection, in which we advocate for rulemaking that would protect people's privacy from extractive data practices and commercial surveillance;
- Working with the United States Agency for International Development (USAID) to explore the harms and impacts of surveillance technologies; and
- Leading responses to regulatory requests from the White House for worker rights amid the growing implementation of algorithmic management practices, including guidance to clarify how worker surveillance and location tracking violates their privacy and jeopardizes their physical and mental health.

These teams will lead activities that translate our findings on collective privacy for policy audiences. These will include creating policy briefs and producing events and salons for government personnel to engage directly with our research and related topics.

Research Activities

Our **Labor Futures** team plans to carry out a suite of research projects related to internet and data privacy and the impact this has on workers and their workplaces. In particular, their work will address how workplaces are skirting digital privacy laws with new worker surveillance tools. This will include providing recommendations to address these loopholes in both workplace practices and in federal policy. This project will build on their past work on worker surveillance, where they documented how the changing nature of technology in the workplace (particularly biometric surveillance) is being used and abused by employers, particularly in the wake of COVID-19. Other ongoing projects will also be expanded to consider workers' collective privacy concerns, including a forthcoming event series on generative AI in the workplace and new projects focused on the intersections of labor, race, and technology.

Our **Algorithmic Impact Methods Lab (AIMLab)**, a component of our AI on the Ground program, already views privacy as a central area of investigation when looking at algorithmic impact assessments (AIAs). There are many ways algorithms create digital privacy concerns, and we believe that AIAs can simultaneously provide governance of algorithmic decision-making and safeguard our rights to privacy[7]. At present, federal assessments hold no obligation to actually engage with vulnerable communities when measuring and ameliorating "impact." We founded AIMLab to address this issue by empowering those communities to set the terms of these

[7] Kaminski and Malgieri, "Algorithmic impact assessments under the GDPR: producing multi-layered explanations," *International Data Privacy Law* 11, no. 2 (2021),125–144.

assessments. Impacted communities are often put in a dilemma that more privileged individuals do not face: trading their privacy and autonomy to algorithmic systems in order to access the most basic needs. To build AIAs that effectively serve these populations where current frameworks fail, we will use multiple case studies and different types of systems and applications to develop analytics that will help inform new methodologies for impact assessments. Aligning with the work of privacy scholar Deirdre K. Mulligan, we believe that to "make productive use of privacy's essential contestability, we [must] argue for a new approach to privacy research and practical design, focused on the development of conceptual analytics that facilitate dissecting privacy's multiple uses across multiple contexts"[8]. AIMLab's goal is to create AIA methodologies that *measure* what matters most to impacted communities, in order to facilitate their capability to *contest* how those systems deploy and operate.

Our newest research program, **Trustworthy Infrastructures**, works alongside communities most impacted by trust, safety, and privacy harms online. The fundamental goal of this research is to move towards day-to-day interactions with technology that create and sustain trust. To do so, we not only need to limit a flood of harmful attacks on privacy online, but must also look to bolster and expand existing practices and social infrastructures by putting forth new sociotechnical solutions that increase trust and protect our internet privacy. We have two upcoming projects that relate to communities who are deeply impacted by lack of privacy protections online: indigenous and black communities. The first of these projects, led by Indigenous Mestiza scholar Tiara Roxanne, looks at developing protocols of trust and safety online with Indigenous communities based in Central and South America. The second, led by Joan Mukogosi, focuses on how privacy and trust online have impacted how Black communities find and receive health care advice, particularly in the wake of COVID-19. Both these projects work directly with the communities impacted by privacy harms, and the empirical research we produce will shape the development of trustworthy digital infrastructures as well as the policies and regulations that govern them.

Publications and Events

During this period, we will produce:

- **Standalone research publications** of our findings related to the protection of internet privacy;

[8] Mulligan et al., "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy," *Philosophical Transactions of the Royal Society A* 374, (2016).

- **Policy briefs** based on our research that are designed to intervene on a specific privacy technology or regulation;
- **Public events** that bring Data & Society staff members together with invited speakers to talk about digital and collective privacy concerns;
- **Salons for government leaders** that give them a space to learn about and better understand the issues surrounding collective internet privacy; and **Relationships with media outlets and journalists** to ensure the broader public understand the implications of our research and policy work.

Timeline

We see this work taking shape over five years, a timeframe which includes significant research and engagement periods:

Year	Project Quarter	Phase/Project
1	Q1	Hiring and Capacity Building
1	Q2	Research and Community Engagement
1	Q3	Research and Policy Engagement
1	Q4	Evaluation, Impact Stories, and Reports Research and Policy Engagement
2	Q5	Publication Release and Public Event
2	Q6	Policy Brief Release
2	Q7	Research and Community Engagement
2	Q8	Evaluation, Impact Stories, and Reports Research and Policy Engagement
3	Q9	Research and Policy Engagement
3	Q10	Publication Release and Public Event
3	Q11	Policy Brief Release

3	Q12	Evaluation, Impact Stories, and Reports Research and Policy Engagement
4	Q13	Research and Policy Engagement
4	Q14	Publication Release and Public Event
4	Q15	Policy Brief Release
4	Q16	Evaluation, Impact Stories, and Reports Research and Policy Engagement
5	Q17	Research and Policy Engagement
5	Q18	Publication Release and Public Event
5	Q19	Policy Brief Release
5	Q20	Evaluation, Impact Stories, and Reports

Ongoing activities throughout this timeline include: quarterly reporting; salons with government leaders; media placements; op-eds; travel for conferences and meetings; and responses to government requests for information as needed.

9. *Explain why the organization is approaching the issue and/or opportunity in this way.*

We consider the protection of privacy to be a social and technical concern: it's not just about sharing data, it's also about people's experiences of being watched and trusting the digital technologies they use[9]. As a result, our goals and objectives relate not only to how these companies are regulated, but also to how trust is built and sustained by the communities that use these technologies. Focusing our approach on collective trust is therefore key to building a body of research and policy action that could lead to profound change.

We have a history of using a sociotechnical perspective to inform policy debates, change, and action. Accordingly, we believe this approach is what the current privacy debate

[9] Metcalf et al., "Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery, 2021), 735–746.

needs. Rather than simply producing research and releasing it into the world, we build dedicated engagement into every research project. We engage policy, practitioners, and media communities with the goal of translation and influence, as well as engaging our peers in academia, rights-based organizations, and aligned communities to learn, collaborate, and strengthen our field to increase shared power.

Some examples of this successful engagement include:

- Our *Electronic Visit Verification* report about the abuses of privacy in care work was pivotal in our submission to the Office of Science and Technology Policy's Public and Private Sector Uses of Biometric Technologies RFI; was cited in Supreme Court of the State of New York about their digital ID practices; and was listed as a primary source by the European Parliament Research Service in their publication "AI and digital tools in workplace management and evaluation: An assessment of the EU's legal framework".
- We saw our explainer on algorithmic management in the workplace used as a foundational citation by Jennifer Abruzzo, the general counsel of the National Labor Relations Board, in her memo Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights. In this memo, Abruzzo announced that she will urge the NLRB to adopt a new framework for protecting workers from intrusive and abusive electronic monitoring and automated management practices.
- We have helped change the terms of debate around workers and automated systems. This includes the latest debates surrounding the Writer's Guild of America and the use of AI systems.
- Our AI on the Ground team has had numerous engagements with local, state and federal policy makers to inform their decisions about algorithmic impact assessments.
- Our *Digital Doorstep* report helped build new partnerships with on-the-ground advocacy groups to see real change, cited by multiple other research institutes including the Washington Center for Economic Growth, and was featured on multiple podcast interviews including *BBC Digital Planet* and *Marketplace Tech*.

10. *Identify and explain the range of funds required to effectuate the program or project request, on an aggregate and annual basis (if applicable), including how the money will be used.*

Year 1

Total Personnel costs for the first year are $889,055, which will either fully or partially cover the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), and Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000, which will cover Project Supplies & Materials (i.e. include licenses, software, publication costs), Events (i.e., venue rental and honoraria) and Travel (related to conferences, events and fieldwork).

Total costs for the first year: $1,004,055

Year 2

Total Personnel costs for the second year are $955,085, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), and Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the second year: $1,070,085

Year 3

Total Personnel costs for the third year are $983,738 which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program

Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab) Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the third year $1,098,738

Year 4

Total Personnel costs for the fourth year are $1,013,250, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $115,000 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the fourth year $1,128,250

Year 5

Total Personnel costs for the fifth year are $586,674, which will cover either fully or partially the following positions: Policy Director, Senior Policy Analyst, Program Director (Public Technology Leadership Collaborative), Senior Policy Analyst, Participatory Methods Researcher (AIMLab), Program Director (AI on the Ground), Executive Director along with Communications Support, Editorial Support, Events Support, and Finance & Operations Support.

Direct Project costs are $112,198 which will cover Project Supplies & Materials (i.e., include licenses, software, publication costs), Events (i.e., venue rental and honoraria), and Travel (related to conferences, events and fieldwork).

Total costs for the fifth and final year $698,872

Total Personnel costs are $4,427,802. Total Direct Project costs are $572,198 for a total of $5,000,000 across 5 years.

11. *Will the money be used to continue an existing project or create a new project?*

This money will be used to sustain and increase the capacity of our current programs, as well as to fund new research projects within those programs. It will not be used to start a new, dedicated program.

12. *What target population will your organization's project benefit?*

These activities will respond to broad and pressing internet privacy concerns that impact the general public, while also maintaining a particular focus on collective privacy as it relates to low-income and precarious workers and other vulnerable communities. These projects will benefit these groups by directly including them in the research process, designing governance approaches grounded in participatory methods[10], and engaging government leaders on our research findings in ways that foreground these groups.

Evaluation

13. *Will your organization agree to provide a report to the Court and the parties every six months informing the Court and the parties of how any portion of the Settlement Fund allocated to it has been used and how remaining funds will be used?*

We agree to provide a report to the Court and the parties every six months; this report will detail how the funds have been (and will be used to support this work). We routinely provide narrative and financial reports of our programs to other funders, so our team certainly has the experience needed to ensure this is carried out every six months.

14. *Describe how your organization will evaluate the success of the grant on enhancing or promoting the protection of internet privacy.*

[10] Michele Gilman, *Democratizing AI: Principles for Meaningful Participation* (Data & Society, 2023).

We build a series of impact measures and evaluation periods into the timeline of every project we take on. This work is led by Ania Calderon, our managing director, alongside our strategy and engagement team, who bring significant experience in setting impact measures, tracking our impact, and evaluating the results of our work.

Our impact and evaluation model for projects has six core components. They are:

1. **Learning questions**. Each year, our projects and programs develop two timely learning questions that help us assess the kind of impact we are making. For this project, we will develop these learning questions related to internet privacy in consultation with the associated research programs. They will focus on asking questions of impact that bring us closer to our long-term goal of the protection of internet privacy.
2. **Project retrospectives**. We regularly hold project retrospectives as part of our research pipeline, often in conjunction with the launch of a report or major publication. These retrospectives are used to reflect on each project's intended purpose: how it promotes the protection of internet privacy; what successes we saw in the process; and the biggest factors that contributed to change and impact.
3. **Quarterly program progress**. Each quarter, we take stock of—and report on—program progress and share this information with the organization as a whole. These updates reflect on the outputs we've been successful in producing, review our key learning questions and assumptions, and explain how we will move this work forward in the future.
4. **Learning Labs**. Our strategy and engagement team hosts biannual org-wide learning labs. These sessions bring us together as a group to share insights, connect learnings across programs and project retrospectives, review the impact we are having, and discuss how we might use these insights to inform future decisions. For this project, Learning Labs will give us an opportunity to review our long- and medium-term goals related to internet privacy alongside the work of the entire organization.
5. **Impact stories and annual reports**. Where appropriate, we publish our outcomes and progress as impact stories. These stories are narrative tools for communicating the processes and outcomes of our work to various stakeholders. They connect the dots across our various projects and organizational initiatives, showcasing common themes and learnings that elucidate how our work is reflecting the values and strategy of the organization as a whole. Since our work on internet privacy will be done across all of our research programs, impact stories will be an essential tool for bringing each component together to create a comprehensive portrait of our work and its impact.**Board Oversight.** Data &

Society's board of directors maintains oversight over all of our work through regular reporting on organizational goals and strategy, as well as scrutinous financial oversight. They also provide important support and guidance that shapes how we evaluate and track the overall impact and success of our projects.

15. *Does your organization intend to use the results of the project in any publications, conference papers, and presentations?*

We intend to produce outward-facing reports, articles, papers, and presentations as part of this project. We have a long history of producing and publishing reports in-house through our website, as well as having papers and articles accepted into journals and media outlets. Our researchers are also regularly invited to present at conferences, events, and institutions around the world. These include the Mozilla Festival; AI and Tech Summit; ACM Conference on Fairness, Accountability, and Transparency (FAccT); Association of Internet Researchers Conference; and Trust and Safety Research Conference.