RED FLAGS CATEGORY

Organizational Governance, Policies and Practices

Ford Foundation

6

RED FLAG

The governing body and the team behind the project are homogeneous in demographic, background, and expertise; the team is structured in such a way that the knowledge or decision-making power is concentrated within a small group of individuals.

AT A GLANCE

- The lack of diversity in demographics and backgrounds among the team members may result in a disconnect between the team and the community they are attempting to serve.
- The concentration of knowledge and decision-making power within a small group of individuals can result in a bottleneck effect and an increased chance of biased viewpoints.
- To identify this red flag ask about team member experience, organizational structure, expertise and demographics of board and advisors, diversity and hiring practices.

If the governing body or team that is creating the product comes from a uniform and dominant group (such as being uniformly white, male, and/or young) and is attempting to solve a problem in a community who has been historically excluded, then there is a major mismatch between the team and people who will use and/or be affected by the product.

Sometimes, no team members have or are connected with direct/lived experience with the communities or problems being targeted (e.g., policing in BIPOC communities or individuals impacted by the carceral system, or experience with people with disabilities).

Alternatively, the team may lack the necessary expertise (technical, issue-based) and/or sensitivity surrounding the issues and sociopolitical context. This consideration also applies to the organization's governing bodies, including the board of directors and advisors. Given the gender and racial gaps in the technology sector,[1] the diversity and inclusion in those projects should be a subject of further scrutiny.

A red flag also occurs when all the knowledge or decision-making power is concentrated in a small group of individuals. This may be unsustainable from a product development perspective because there may be a bottleneck effect. If an organization is understaffed they may struggle to support the community they are supposed to be serving, even with the best intentions. Additionally, when decisions are made by a small group of individuals, there may be an increased chance of biased viewpoints.

EXAMPLE

A city government partners with a local anti-human trafficking nonprofit and a major technology company to organize a "tech for good" hackathon for identifying and breaking human trafficking patterns. After the hackathon, one of the participating groups decides to expand its proposed project and start a nonprofit. The founding members are exclusively former tech workers, all white and majority male. From early on, because of their lack of expertise and connections to the advocacy space, they face multiple issues, ranging from a lack of knowledge about culture and language to not being able to develop a trustworthy relationship with relevant advocacy groups among survivors, domestic workers, and sex workers.

[1] Molla, Rani, and Renee. Lightner. "Diversity in Tech," 2016, https://graphics.wsj.com/diversity-in-tech-companies/

Questions to Identify this Red Flag

Do any of your team members have direct/lived experience with the community(ies) or issue being addressed? How did you put your team together?

Can you tell us about your organizational chart/structure? Who do you categorize as technical/policy/advocacy experts on your team and how do you define expertise?

Can you tell us about the expertise and demographics of your board of directors and/or advisors?

Why is diversity important for your organization?

Can you tell us about your hiring practices and the steps you have taken to ensure that you have built a diverse team?

What policies have to change to make the tech solution truly viable? Are you supporting the advocates pushing for these policies?

RESOURCES

- A primer on Agile development in the public sector
- The U.S. Government Accountability Office's Agile Assessment Guide

7

RED FLAG

There is insufficient disclosure about the project's privacy policy, terms of service, and algorithmic use policies (if applicable). Furthermore, there is no process for obtaining meaningful informed consent from communities.

AT A GLANCE

- Informed consent is often not obtained from communities, and the consent process is often limited to generic terms of service and privacy policies written in inaccessible jargon.
- To identify this red flag ask about privacy policies, the process for obtaining informed consent, and how the vendor manages situations where consent is not knowingly given.

The first step for vendors to show their commitment to beneficiaries' fundamental rights is to disclose their policies around data usage, privacy, terms of service, and algorithmic use, among others. Transparency enables the demand for accountability – which may diminish in public-private partnership projects.

In addition, not being able to obtain informed consent is one of the main pitfalls of any data-driven project. Often, the process for obtaining informed consent is restricted to providing generic terms of services. Those documents are often written using inaccessible, lengthy, and legal jargon. Other issues include deceptive design practices (e.g., obfuscating or hiding website cookies settings) and a lack of alternatives if a person refuses to use or be a subject of those tools. In addition, technologies that are used by public agencies are often used on people without their knowledge (e.g., smart city projects, sharing databases between multiple public agencies and law enforcement).

While ultimately it is public agencies' responsibility to ensure the public's interest in consent, transparency, and oversight mechanisms in every stage of contracting, it is the vendors' responsibility to provide accessible information, design interfaces for obtaining informed consent, develop policies and make them publicly available, be transparent about their third-party relationships, and set boundaries for data co-ownership with public agencies.

EXAMPLE

As part of their "Green City, Smart City" initiative, a city decides to fully switch to paperless subway tickets. They have a contract with a company to develop an app. The city is also interested in integrating all other ticket-based transportation services including parking tickets and traffic tickets. It will provide APIs so other developers can use the city data and propose new digital services. During the sign-up, users must accept lengthy terms of service agreements. However, they are not fully aware of how their transportation data is used, what other data is collected, with whom the data is shared, and what consequences this might have.

Questions to Identify this Red Flag

Ask the potential grantee/vendor to provide privacy policies, terms of services, algorithmic use policies, developer policies, etc. Ask about the process of coming up with those policies and whether the policies are publicly available, and if not, why? Moreover, how understandable are these policies for the layman?

What does “informed consent" from communities mean to you? Describe your process for obtaining informed consent mainly from users of your product.

How can you collaborate with public agencies to obtain informed consent? What options do beneficiaries have if they decide not to use or be a subject of using your tool?

How do you manage a situation where you later learn that a subject did not knowingly consent to data collection or sharing?

RESOURCES

- Ranking Digital Rights Corporate Accountability Index: privacy, freedom of expression, and governance indicators
- Smart City PDX, On the road for the Surveillance Technologies Policy

8

RED FLAG

There is no formal process for conducting a human rights or algorithmic impact assessment and/or a mechanism to track, report, and remediate harms.

AT A GLANCE

- Potential grantees should regularly evaluate their products' and policies' impact on society, with processes in place to report and address any potential harm.
- They should have a strategy for receiving reports and remedying potential harms.
- To identify this red flag ask about the frequency and methodology of impact assessments.

It is important for vendors to conduct impact assessments to understand the direct and indirect societal harms of their project, especially on underrepresented and underresourced communities.

Impact assessments can be done internally or with the help of independent external experts. Funders should require potential grantees to report on their impact assessment methods and their findings. Funders can also connect their (prospective) grantees to experts who can help with conducting and developing impact assessment processes – not as a one-time assessment but rather as a continuous one.

In addition, vendors should have a strategy (e.g., feedback channel, functioning email addresses, "Contact" or "Report Issues" online forms on their own or government's website) to receive reports about the potential and actual societal harms of their products from beneficiaries and third-party advocates/researchers. Being transparent about those harms and having a strategy to redress harms is a must.

EXAMPLE

City A is a "sanctuary city." Undocumented immigrants can purchase e-tickets with less fear of government surveillance and consequences such as arbitrary detention and repatriation. A year later, the same company which built the e-ticketing service wins a bid to develop similar services for City B. City B has a very strict policy on immigration and is not a sanctuary city for undocumented immigrants. Without conducting a thorough human rights impact assessment on design choices, app features, data collection, and data sharing practices, undocumented immigrants (in both City A and B) may be at risk of surveillance, violation of their rights to freedom of movement, and potentially even detention and repatriation.

Questions to Identify this Red Flag

What unintended negative consequences are possible as a result of this product? Are you willing to abandon the product if the negative consequences are too great?

Do you conduct any types of impact assessment? If yes, do you publish impact reports in a manner/format that is widely accessible?

What mechanism do you offer to prevent, mitigate, and remediate harm?

Do you provide any feedback channel for receiving reports about any harm as a result of your product design and deployment?

Do you ask for indemnification in your contract? What are you liable for if you do cause harm?

RESOURCES

- Digital Rights Check
- The Santa Clara Principles On Transparency and Accountability in Content Moderation
- United Nations Guiding Principles on Business and Human rights (UNGPs) B-Tech Project

A list of risk assessment and documentation tool:

- https://github.com/users/royapakzad/projects/3
- Data Protection Impact Assessment template
- Assembling Accountability: Algorithmic Impact Assessment for the Public Interest

9

RED FLAG

There is not enough knowledge about technology standards and regulations that apply to vendors' practices.

AT A GLANCE

- Vendors may have incomplete knowledge of local, state, and federal regulations relevant to their practices.
- Lack of engagement with technology standards and regulations can result in "one-size-fits-all" project design.
- To identify this red flag ask about the impact of relevant regulations and an organization's stance on them.

In some cases, vendors may possess insufficient or incomplete knowledge about local, state, and federal regulations that are applicable to their practices. Similar to Red Flag 3 (on "band-aid" fixes), this shows a lack of engagement with policy and advocacy space. This may also result in a "one-size-fits-all" approach to project design. In addition, being knowledgeable about technology standards (e.g., standards published by national bodies such as NIST, professional codes published by the ACM or IEEE), and best practices helps their products to be reliable.

EXAMPLE

An electronic medical records company is not familiar with local medical privacy regulations. The company complies with federal regulations but has not developed infrastructure to handle evolving local privacy regulations. In particular, parts of the software assume that certain data is available, when in reality the data is only accessible in certain states.

Questions to Identify this Red Flag

What are the key regulations/laws/regulatory proposals that apply to this project?

How does [applicable regulation/regulatory proposal] affect this project?

What is your position on [applicable regulation/regulatory proposal]? This question depends on funders' knowledge about the regulatory space. For instance, you can ask about the Community Control Over Police Surveillance (CCOPS) Model Bill, or the Algorithmic Justice and Online Platform Transparency Act.

Is changing [applicable regulation] something you commit resources to? Is your service part of a larger set of goals?

RESOURCES

- Federal & California ai legislation database from the CITRIS Policy Lab
- Privacy: California Consumer Privacy Act (CCPA), Illinois Biometric Information Privacy Act.
- Local Surveillance Oversight Ordinances
- Federal Fair Housing Act
- NIST's Face Recognition Vendor Test (FRVT)
- IEEE P7000TM Standard
- Making Smart Decisions About Surveillance

10

RED FLAG

Based on the vendor's current policies, there are not enough safeguards for preventing harm during organizational restructuring, spin-offs, merges, or dissolution.

AT A GLANCE

- Vendors should have clear policies in place to prevent harm during organizational restructuring, spin-offs, mergers, or dissolution.
- They should have a data ownership policy that stays robust during major organizational changes, backed up with dedicated resources and a written policy.
- To identify this red flag ask about the safeguards potential grantees have in place for these hypothetical scenarios, such as impact assessments and data ownership policies.

Often, "tech for good" projects start as experiments. For instance, a city decides to pilot a new welfare distribution platform. However, there is no clarity about the consequences of program failure or what happens if the city decides not to continue working with the vendor. Funders should ask potential grantees about the safeguards they have in place during these hypothetical scenarios.

In addition, vendors should have a data ownership policy from the start: Who owns the data after potential major restructuring such as mergers and spin-offs? They should guarantee that their policies for harm prevention and mitigation stay robust during situations such as major organizational changes e.g., changing top executives, changing business models or creating a spin-off nonprofit from for-profit vendors or vice versa, entering a new market, and being acquired by or merged with other companies. This should be backed up with dedicated resources, such as teams or individuals, who are committed to the program's maintenance, or having a written policy for sunsetting a program that includes a policy for deleting user data.

EXAMPLE

A nonprofit that maintains a suicide hotline shared its beneficiaries' anonymized and unidentifiable information with its spin-off organization. The for-profit company provides audio-based emotion recognition services. Both the for-profit and nonprofit organizations share the same CEO. Privacy activists and mental health advocacy groups raise concerns about this data sharing relationship. They believe extracting commercial value from people's most sensitive and vulnerable conversations is unethical. There is a resulting lack of trust in such services despite being backed and promoted by government public health agencies.

Questions to Identify this Red Flag

Do you have any written policy to show that you will be conducting impact assessments if your organization goes through major changes (spin-off, changes in business model, acquisition, dissolution)? What's your data ownership policy during these major changes?

Did you pilot this project anywhere? If yes:

- Did you have an exit interview with users when the pilot ended?
- What safeguards did you have in place to protect users' data?

RESOURCES

- Crisis Text Line, from my perspective