



# **Framework Assessment Report**

Whistle Stop Capital

# Whistle Stop Capital

Whistle Stop Capital, LLC (Whistle Stop) is a consultancy focused on helping investors assess, and address, environmental, social and governance (ESG) topics. Whistle Stop works with its clients to identify the key areas of exposure and opportunity within investment portfolios, to build and implement engagement strategies that encourage improved corporate practices, and to incorporate appropriate metrics and benchmarks that track the positive changes catalyzed.

Whistle Stop provides services to field builders, foundations, individuals, investment advisors, endowments, and newly forming investment funds. Its allies include academic institutions, activist organizations, public pension funds, religious orders, corporate leaders, and innovators.

The lead authors of this report were Meredith Benton, Jaylen Spann, and Claire Veuthey, supported by the broader Whistle Stop team. Findings include research and analysis provided by Open MIC, Whistle Stop's project partner. Team members and their bios are available at: [whistlestop.capital/team](https://whistlestop.capital/team).

This report was prepared in support of the NetGain Partnership, a philanthropic collaboration seeking to advance the public interest in the digital age. The research provided here is part of a larger initiative, which has sought to assess the investors' role in encouraging greater accountability from technology companies to civil society. This report is not intended for public distribution.

*The content in this document is for informational purposes only. Nothing in this document should be construed as legal, tax, investment, financial, or other advice. Nothing contained in this brief constitutes a solicitation, recommendation, endorsement, or offer by Whistle Stop Capital, LLC, or any third party service provider to buy or sell any securities or other financial instruments. While Whistle Stop Capital, LLC, has exercised due care in compiling this report, it makes no warranty, express or implied, regarding the accuracy, completeness or usefulness of this information and assumes no liability with respect to the consequences of relying on this information.*

# Contents

- Key Takeaways** 1
- About this Report** 2
- Introduction: Why a Framework is Needed** 2
- What a framework does:** 4
- Section I: Steps of Framework Development** 5
  - 1. Build clarity on the “why” 5
  - 2. Consider the audience 5
  - 3. Scope the problem 6
  - 4. Review existing topic expertise 6
  - 5. Synthesize existing expertise 7
  - 6. Shift concepts into “quant-cepts” 7
  - 7. Socialize with stakeholders 8
  - 8. Test-drive the framework 8
  - 9. Integrate new knowledge 9
- Lessons from the Creation of the Framework** 9
- Principal gaps** 9
  - 1. Scope of application 10
  - 2. Research infrastructure 10
  - 3. A unifying performance metric 11
  - 4. Agreement on materiality to investors 11
  - 5. Shared understanding of best practices 11
- Opportunities** 12
  - 1. A strong interface between civil society advocates and investors 12
  - 2. Clear, meaningful performance metrics 13
  - 3. Data infrastructure 13
  - 4. A credible third-party assessor 14
  - 5. A watchdog 14
  - 6. Falling share prices 14
- Section II: The Technology Accountability Framework** 15
  - The Corporate Governance Framework** 17
  - Data Privacy Framework** 21
  - Lessons from the Use of the Framework** 25
    - 1. Company performance on overall governance framework 26
    - 2. Company performance on data privacy framework 27
- Next Steps** 29
- Appendix 1: Organizational Content Reviewed** 30

# Key Takeaways

Data frameworks and their associated infrastructure are an essential aspect of a shareholder engagement campaign. Investors need a system that allows them to compare and benchmark companies – both against their peers and relative to their own performance over time. A consistent and well-defined data set is also essential, because investors want to understand the materiality of an issue to company value. They also need to understand the relationship between stock performance and issue performance in order to act.

As we reviewed the existing landscape of thought leadership, standards, and datasets, we expected to find clear goals or concerns related to tech companies and their civil society impact. However, the tech accountability standards and frameworks we reviewed were primarily focused on conceptual policies, not tangible or quantitative practices. While consistent themes emerged, (algorithmic fairness, bias & discrimination, content moderation, disinformation, end user impact, freedom of expression, human rights, internet access and privacy) quantitative expectations were challenging to identify, even in direct conversation with thought leaders. Such quantitative metrics are precisely what equity investors find most actionable and relevant.

Given those circumstances, the NetGain Partnership advisory committee agreed to shift the focus to the development of a sample framework focused on privacy concerns. This allowed Whistle Stop to illustrate the steps needed to replicate the framework development process for other topic areas. The framework is divided into two component parts, with the portion focused on governance and oversight applicable across all issue areas. The second component part is tailored specifically towards quantifying privacy policies and practices.

The governance focus is needed, because the tech sector is ever-changing. We do not know now the key harms and concerns associated with not-yet-developed technologies. The policies, practices, responsibilities, and expertise of the individuals who lead technology companies become the most important indicators of a company's commitment to reduce current and future harms and to provide societal benefits.

The development and application of the privacy-specific framework allowed for assessment and analysis of Google, Amazon, Meta, Twitter, and Yelp. These companies were chosen in order to provide illustrative example of tech platform companies. To review and deploy the framework effectively, additional companies will need to be included in an analysis.

The research into the framework's creation identified five gaps that would impede the development of a successful finance focused tech strategy. (1) The scope of concern must be defined, (2) There are few researchers and few publications dedicated to investors' understanding of the technology sector's impact on society, (3) Unlike climate activism, where the need to reduce greenhouse gases is a clear unifying goal, technology's wide impacts mean there is no unifying metric, (4) Investors are most easily engaged on topic areas that have been deemed to be material to stock performance; this link has not yet been formally created for technology's impact on society, (5) The lack of definition of issue-specific impacts means that best practices cannot be assessed.

In response to these challenges, we recommended that the facilitation and coordination between civil society advocates and investors be prioritized. We also noted the need to develop clear performance metrics and infrastructures to research and assess tech accountability data. This linked to the need for a credible third-party assessor and corporate watchdogs. Finally, we noted that the recent drop in tech valuations in the public markets was creating a moment of opportunity; as the tech companies have fallen from their pedestals, they are now within reach.

## About this Report

This report details the process followed by Whistle Stop to create an evaluation framework to help investors understand and evaluate the technology sector's impact on society. It brings the reader through the nine steps followed and then applies the framework to a subset of the tech sector. We have compiled data and knowledge through the use of the framework applied to the practices of five companies. We also describe our insights from the framework development process.

While the findings in the previous *Landscape Report on Shareholder Engagement and Activism Strategies* and the *Moving Forward: Strategies and Recommendations* report are intended for a broader audience, this *Framework Assessment Report* is intended for a far more narrow band of already-engaged practitioners, and those who will be directly involved in determining next steps. It is not intended for public dissemination.

This report provides a detailed Technology Accountability Framework along with an assessment of the knowledge gained through the Framework development process. Discussed in the *Moving Forward* report are recommendations for the finalization and deployment of the Framework, along with strategies to increase its effectiveness.

Section I: We outline the steps needed to create the Framework and detail how we applied these to technology accountability and the knowledge that came through this process.

Section II: We present the developed Framework and apply it to five tech sector companies.

The research for this report was conducted over August and September of 2022. As an illustration of how quickly the tech sector changes, less than two months later, Twitter was taken private and is no longer a publicly traded company. The insights from its analysis remain valid, however, and so we have not removed it from this report.

## Introduction: Why a Framework is Needed

What does it take to change investors' understanding of a social issue? What is needed for them to be willing to talk to their companies and encourage improved practices or allocate capital with that issue in mind?

Equity investors (that is, investors in the stocks of public companies) are interested in the risk-adjusted returns of a corporate security. Return is based on an estimate of future cash flows generated by the company's products and services. Risk is a broader concept that encompasses reputation, shifting consumer preferences, macroeconomic stresses, political shifts, and a broad array of other factors. The investor is concerned about the relative certainty of future cash flows and the effect of risks on long-term company value. With the exception of certain faith-based and responsible investment firms, investors do not have the improvement of society or the protection of the environment as principal concerns. But environmental and social factors can affect cash flows and risk. For example, consider how the fear of reputational risk has motivated several of the leading social media companies to limit misinformation on their platforms. This is where civil society efforts to reduce societal harm by tech companies intersect with the urgency of investors to understand broad risk factors that could affect the value of their portfolios.

The *Landscape Report on Shareholder Engagement and Activism Strategies* identified the building blocks employed in past investor engagement that aimed to change corporate policies and actions as:

The success of each of these blocks rely on making a clear request of companies, and the ability to communicate and build coalitions in support of shared goals.

Frameworks provide this needed infrastructure. Companies need to be assessed against their identified products, policies, and practices. Quantification in this way provides the following ability to:

- to identify leading practices
- to identify companies that exhibit leadership
- to identify companies that lag and to prioritize their engagement
- to communicate concisely to media and investors what actions are needed
- for others who are allies but not experts to become involved
- to avoid uncoordinated, one-off or “lily pad” messaging.

Data for data's sake, however, can be damaging to long-term goals. Companies must be asked for data that will be used by investors for securities selection and performance monitoring. The data requested must be linked to the strength of a company – if it is not, it will not be used by analysts. If it is not used by analysts, companies will resent that they have been asked to produce it. The data requested must be used. Turbocharged change happens when materiality can be shown, or strongly indicated, and that is only possible when there is a clearly defined set of characteristics to which attribution may be linked.

Data requested must be able to be incorporated into analysts' models and algorithms. It must be additive when they are seeking to differentiate among potential holdings and to conduct attribution. Ideally, they could build a portfolio thesis from the data set alone. We are looking for a normalized data point – that is, one that is standardized across all companies.

Essentially, when large investors, like Blackrock or State Street, integrate this data set into their securities selection process, much of the boots-on-the-ground advocacy work lightens. These investors become the messengers who tell companies that the issues matter, and that policies and practices should be improved.

When we reach this stage, public databases are taken very seriously by companies; they track these scores and measure themselves against the actions of their peers. In this way, frameworks are themselves the change agents, beyond their role as data organizers and trackers. As a framework becomes established, shifts accelerate over time as momentum builds.

**What a framework does:**

A framework rates a company’s performance relative to others in their sector and relative to the company’s own performance over time. This information is essential in helping guide companies in their own strategic approach to the issue. Securities analysts and investment portfolio managers will use frameworks to implement factor weights or screens in their portfolio, and to determine where to allocate assets.

Portfolio managers face two large challenges: understanding the extraordinarily complex system that is a corporation and explaining investment decisions to their clients. The portfolio manager cannot be a subject matter expert on every issue that affects the valuation of a company and its se-



curities. A successful framework will aid the portfolio manager in both of these tasks. The successful framework’s data points can be captured in a spreadsheet and integrated into a portfolio manager’s or securities’ analyst’s security pricing model. The analyst can then use the model to explain portfolio buy/sell/hold decisions to their clients or managers, without needing to become a deep expert on each issue area. On the other hand, if company data is presented in a way that the portfolio manager needs to expend time and effort to become an expert, it is much less likely that they will consider this information in their decision-making. Alongside analysts, the data should be crafted in a way that allows research database providers (such as MSCI, Bloomberg and Morningstar) to add the information into their service offerings.

# Section I: Steps of Framework Development

Whistle Stop has developed frameworks for other clients, and in each case we have followed the same steps and research process. It is important to note (and as will be seen below), this is not always a linear process. Knowledge developed during a later step may require revisiting earlier steps. Framework development is an iterative process.

**The nine steps in this process are:**

1. Build clarity on the “why”
2. Consider the audience
3. Scope the problem
4. Review existing topic expertise
5. Synthesize existing opportunities
6. Shift concepts into “quant-cepts”
7. Socialize with stakeholders
8. Test-drive the framework
9. Integrate new knowledge

## 1. Build clarity on the “why”

The first step is to determine what needs to be assessed, and why it is important. Is there a problem that should be ameliorated, reduced, or tracked? Are the changes being sought known, or do they need to be defined?

The mandate for the NetGain project was, within tech accountability, impact-agnostic. Rather than requesting a specific change (such as the reduction of greenhouse gasses), NetGain asked for a broad analysis of how investors might address the technology sector’s impact on society.

Within this mandate, we defined “impact on society” as the impact of a company’s products and services on society – with “society” broadly encompassing users, consumers, civil society, and other individuals, but excluding government entities. This definition also excludes companies’ impacts on their employees (and to some extent, candidates for employment), business partners, suppliers, and government entities.

## 2. Consider the audience

The next step is to identify the primary, secondary, and tertiary audiences and build the framework with them in mind. Considerations should include the depth of knowledge or interest of each audience, any existing erroneous beliefs they may have, the extent of complexity that they (or their research databases) can digest, how they will likely use the data, and the types of actions that are being sought from them.



This does not mean that other stakeholders will not use the framework, simply that they are not the target audience in its development.

For this framework, our primary audience was the disinterested securities analyst. To have an ESG issue go “mainstream” and have institutional capital participate, investors need to believe that it is worth their effort to pay attention and, then, worth their effort to act. Our goal was the minimization of the effort required for them to understand the topic area and to maximize the ease with which they could access and apply relevant data. Our secondary audience was the companies, for whom this framework will define best practices. Our tertiary audience was the media, for whom this framework will enhance comprehension of, and increase communication about, key concerns within the tech sector.

### **3. Scope the problem**

Identify the problem sought to be addressed as precisely as possible, noting the key components where change is wanted. For example, in the case of climate change, the problem is the shift in average global temperatures, but what investors and civil society can expect companies to address is their greenhouse gas emissions. Be clear about the amount of change that a company can manage and take on.

We returned to Step 3 from Step 6, having found our initial scope too broad when based on the amorphous concept of tech accountability. The framework was split into two parts: a corporate governance lens that would apply to all topic areas, and a more specific framework to address privacy-specific topics.

### **4. Review existing topic expertise**

It is imperative to enlist key experts around the topic area and to research existing materials to understand what contributes to the problem. As well, current corporate behaviors and future or potential corporate behaviors should be specified.

While it is impossible to scope out all existing and relevant publications in full, it is important to make the best efforts to learn from those who have studied the topic in depth. It is to all parties’ advantage to build on that work rather than recreate it (unless it is foundationally weak and needs to be revamped.)

If a strong framework already exists and is thoughtfully constructed, with permission of the originator, those metrics can be integrated directly. Multiple frameworks covering similar territory muddy the waters and make it harder for investors and companies to determine best practices.

Open MIC’s *ESG(+D) report* explained why investors fail to account for the risks and harms posed by tech’s impact on society, particularly in the Social and Governance realms. That report also provides an overview of the various existing frameworks, standards, and guidelines that aim to assess the sector’s societal impact.

Open MIC had mapped these existing frameworks against nine key themes: Algorithmic Fairness, Bias & Discrimination, Content Moderation, Disinformation, End User Due Diligence, Freedom of Expression, Human Rights, Internet Access, and Privacy. Building from these themes, we reviewed almost 100 Frameworks for their applicability to a quantitative framework. The full list of organizations and data sets reviewed is in Appendix 1.

## 5. Synthesize existing expertise

As appropriate, combine subtopics within a broader topic in order to avoid duplication. This should also help clearly establish logic and hierarchy: it is important to be clear about what is a root cause of any given problem, what is a symptom of this root cause, and what possible prevention and treatment options are, and not to confuse any of these. It is better to track outcomes and indicators of a program’s effectiveness than to identify each possible programmatic action.

As we reviewed the requests and expectations related to the nine issue areas, it became clear that many expectations were theoretical and at a high level, making it difficult to combine and synthesize. The research revealed a constellation of topics under the broad umbrella of societal impact. Much of the thinking around these topics is still emergent; best practice expectations for companies are far from settled. Some expectations require technical expertise beyond a lay person’s ability to assess.

Given the lack of consensus within the tech accountability space, particularly as it relates to specific actions sought at companies, alongside the constantly evolving nature of technology, we spoke with the NetGain Partnership team and decided that the best path forward is to focus on corporate governance and privacy. This shift allowed us to dedicate sufficient time to identifying existing and developing potential best practice expectations.

*Civil society does not have consistent messaging around key tech accountability criteria or expectations.*

## 6. Shift concepts into “quant-cepts”

List the desired performance indicators that would support thoughtful evaluation of company performance on the topic at hand and identify how they might either become binary yes/no questions or have numeric values assigned. For example, when seeking to understand if a company takes data privacy seriously, we considered whether or not the firm has a chief privacy officer (yes/no) and whether it has qualified staff dedicated to the issue (yes/no).

For questions where several answers are possible or a variance in quality is seen, a brief rubric of answers and scores can be applied.

We reviewed existing corporate governance and privacy frameworks, replicating their structures and current indicators as best as possible, while also integrating new concepts specific to the tech sector. The replication of existing framework structures that are known by investors, reduces some of the barriers to future implementation, because investors are already familiar with the structure and overarching approach. To the greatest extent possible, we are trying to encourage investors to take the same dance steps to a different song. In this effort, we sought to mirror, where appropriate, the structures of the CDP, the Global Reporting Initiative, the SASB Standards and Ranking Digital Rights.

## 7. Socialize with stakeholders

Presenting an approach to experts and practitioners, gathering feedback, probing for gaps, faulty or circular logic, and any missing issues, are crucial steps to strengthening the framework, incorporating existing knowledge, and, indirectly, seeking buy-in from stakeholders in the field. Edits and additions should be made as appropriate to reflect any lessons learned or previously overlooked ideas.

Stakeholders, particularly non-profit leaders or other activists, are time and budget constrained. Requests for feedback should be focused, and, if possible, value additive or remunerated for the interviewee.

We held conversations with civil society advocates, tech policy experts, tech investors, and others, to glean areas of consensus and focus on the stakeholders who are consistently considering technology’s societal impact.

The feedback received on the framework itself improved and strengthened our approach, highlighting nuances and additional concepts that would have been missed.

If NetGain decides to move towards the next steps in this process, additional and more formal consensus building around this framework is needed. Potential next steps in this process are detailed in the *Moving Forward: Strategies and Recommendations* report.

## 8. Test-drive the framework

The success of a framework depends on its access to meaningful and usable data and the ability to build reasonable strategies to access or encourage the disclosure of this data. A framework should NOT rely on only existing datasets, because it’s rare that companies will release data voluntarily that paints them in a negative light.

Conduct research on a short list of companies, collecting data on each indicator. In so doing, determine how feasible and how insightful the framework is. Do companies disclose the information already? If so, is it readily available, or does it require significant inference? Are there major gaps in company reporting or otherwise publicly available information?

The application of the framework was tested across Alphabet, Amazon, Meta, Twitter, and Yelp. Of the data points we sought to collect, slightly over half were readily available. Should NetGain choose to activate the Framework, it will also want to develop strategies to encourage the release of this additional needed information.

## 9. Integrate new knowledge

Finally, draw from the direct application of the framework to company analysis to make appropriate changes in the framework and tease out insights.

For example, if none of the companies researched disclose any of the indicators in a subtopic, determine if the issue is emerging and companies need to be pushed towards greater disclosure, if proxies for company practice on this topic might be more easily accessible, or if the indicators are simply off the mark. On the other hand, if disclosure on another subtopic is fairly standard and consistent across the set of test companies, providing no true insights, determine if the indicators are too lax or too broad.

This final step should be repeated regularly to ensure the framework reflects evolving company practice and new regulation and remains useful in evaluating company performance.

We tightened the language and clarified a number of the indicators after the initial testing of the framework. In illustration of the circular nature of a framework development process, as we re-researched the five companies, we found that we needed to better define “impact on society.” In doing this, we returned to the first step of the process, placing clearer definitions on each of the key terms used in the Framework.

## Lessons from the Creation of the Framework

Our initial efforts attempted to corral a sprawling collection of topics of widely varying application and maturity. Some have already been subject to regulation in several jurisdictions, such as data privacy concerning children; others are emergent, technology- and/or use-case-specific, such as internet access and AI.

Our initial findings from this broad stakeholder engagement follow, starting with interlinked gaps that are both obstacles to and evidence of a still-fragmented field.

### Principal gaps

Our research identified five major gaps that impede the development of a consensus on impacts technology has on society, as well as how these impacts might be prevented, managed, and mitigated.

## The gaps identified were:

1. Scope of application
2. Research infrastructure
3. Unifying performance metric
4. Agreement on materiality to investors
5. Shared understanding of best practice

### 1. Scope of application

The now omnipresence of Web 2.0 and the dramatic growth of software more generally has resulted in technology inextricably permeating business. “Technology” can refer to the companies whose primary products and services are technology, the products and services themselves, society’s use of technology, as well as the supporting telecommunications infrastructure. The potential conflation of these different entities contributes to the field’s diffuseness, as expectations might reasonably differ for a corporate entity’s governance structure, its software’s capabilities, and its responsibility and management of user behavior, for example.

### 2. Research infrastructure

There is little publicly available research on technology’s impacts on society, nor is there much on the sector’s risk and impact management that is suitable for an investor audience.

To understand the wide range and variation of salient ESG topics affecting potential and actual portfolio companies, some institutional investors rely on ESG rating agencies to help both surface and synthesize the major ESG risks their investments face. As unpacked in Open MIC’s *ESG(+D) report*, “S” and “G” issues are likely to be the least consistently evaluated by agencies, and those agencies may even ignore emerging qualitative areas examined by this project. For a number of the indicators we identified in the framework, research infrastructure would need to be developed to determine the quality and sufficiency of the information available from companies.

Ranking Digital Rights (RDR) is a notable exception to this gap in the research landscape and was mentioned repeatedly by the stakeholders we spoke to. The organization, a nonprofit program operating as part of the policy think tank New America, focuses on freedom of expression and related privacy and governance issues in the tech sector.

An additional challenge to investor integration of the risks posed by tech companies’ societal impacts is the relatively technical nature of these issues. The depth of knowledge required to account for these risks thoughtfully is more than one could reasonably expect an investment analyst or portfolio manager to possess. As an example, one stakeholder, stating that global tech companies should publish country-specific human rights due diligence reports, acknowledged that few would

be able to assess the quality of these reports.

*There is little existing infrastructure through which tech companies are expected to disclose consistently on their impacts on society, be it qualitative or quantitative data. External researchers focused on tech accountability are also scarce.*

Ranking Digital Rights has begun this process, but the lack of larger infrastructure hampers efforts to hold tech companies accountable or even understand their impacts. This absence of an accessible body of data and analysis impedes the investor community's shared understanding and integration of the risks posed by tech's impact on society in their investment decisions and shareholder engagement work.

### **3. A unifying performance metric**

Climate advocates have been able to harness focus on a single quantitative performance metric: greenhouse gas emissions. While some see emissions alone as insufficient in understanding the impact of climate change, as well as in a company's documented performance on climate action, the metric's simplicity is part of its wide resonance with climate action advocacy, including corporations and their investors.

Tech's impact on society with regard to social and governance issues lacks such a simplifying measurement. That lack contributes to the diffusion of advocacy organizations' efforts and the confusion that investors experience when grappling with the issues.

### **4. Agreement on materiality to investors**

In a similar vein, existing research does not necessarily focus on the risks that tech's impacts on society pose to investors in companies creating or using new technologies. Once again, Ranking Digital Rights' work is a notable exception, as well as the SASB (now part of the IFRS Foundation) standards – though it's worth noting that the latter were developed through a multi-stakeholder consensus-forming and research-backed process, and it takes many years for emerging issues to qualify for inclusion in the Standards.

We do not intend to diminish the importance of examining other aspects of tech's impacts on society, but note that until the materiality of these impacts is more firmly and precisely established, it will continue to be difficult to garner investor attention and concerted action on these topics. A materiality determination exponentially increases the amount of investor interest an issue receives.

### **5. Shared understanding of best practices**

Another manifestation of the field's fragmentation was the absence of a desired end state as articulated by the civil society organizations we engaged.

Our engagements surfaced concepts that are likely to be part of emergent best practices, such as "AI explainability" and "privacy by design." But we did not observe broad consensus around governance, policy, or practice norms toward which tech companies might work.

*“There’s a growing trend for companies to have civil rights teams, who integrate unintended consequences and potential impacts on marginalized communities into the product design process.”*

— Interviewee

While some stakeholders had specific policy objectives, the absence of coordination between these groups created the sense that the desired vision of the future was unclear, and therefore the success of these advocates’ endeavors would be difficult to recognize. This lack of a shared sense of best practices hinders company focus on improvement, as well as investors’ ability to communicate their expectations to portfolio companies.

*“Civil society needs to unify its demands of companies, otherwise they risk cannibalizing each other and confusing investors who want to engage on the topic.”*

— Interviewee

Defining issue-specific objectives for tech companies to strive toward would go a long way toward drawing company attention toward the practices and outcomes that would satisfy civil society’s expectations.

## Opportunities

Support for several crucial components would aid in building the field. As is to be expected, these opportunities mirror many of the gaps identified above.

### The prioritized opportunities identified were:

1. A strong interface between civil society advocates and investors
2. Clear, meaningful performance metrics
3. Data infrastructure
4. A credible third-party assessor
5. A watchdog
6. Falling share prices

### 1. A strong interface between civil society advocates and investors

A number of industry associations already serve as liaisons for investors and ESG advocates, though none are focused on technology companies and their societal impacts. The UN-supported Principles for Responsible Investment (UN PRI), Ceres, and the Interfaith Center on Corporate Responsibility (ICCR) are the primary industry associations that play the role of this civil society and investor communication forum, but none have workstreams dedicated to the emerging issues in question here.

A more comprehensive inclusion of stakeholders in those discussions – namely, civil society and subject-matter experts, as well as large, influential asset managers such as Blackrock and State

Street – would support regular communication between these parties, helping to accelerate investor understanding and action. This extension would contribute to a much-needed conversation around what investors should expect from their technology investments.

*“All coordination between stakeholders is nascent. It’s difficult to explain the issues to stakeholders, and then agree on the creation of a shareholder resolution.”*

— Interviewee

*“We need to ensure the impact of investors is significant. What’s missing is more intentional communication between the NGOs that would be filing lawsuits and those like ours that would be filing [shareholder] resolutions.”*

— Interviewee

## 2. Clear, meaningful performance metrics

The lack of consensus around a short list of ESG performance metrics muddies both advocates and investors’ focus in understanding and action. Transparency reports disclosing government requests for user information and companies’ responses offer a good start in the realm of data privacy, but address only a fraction of the larger topic.

Agreement around a few key metrics would simplify advocates’ message in garnering investor buy-in and focusing their analysis and resulting requests of relevant technology portfolio companies.

*“Having a human rights policy doesn’t always impact a company’s actions.”*

— Interviewee

## 3. Data infrastructure

Currently, insufficient data collection and assessment infrastructure exists. Outside of Ranking Digital Rights, which is focused on a subset of tech accountability issues and 22 companies, there was little infrastructure found to identify, collect, and assess tech accountability-related data. This dearth of infrastructure applies to the identification and assessment of company-released reporting, as well as the independent research that would need to be conducted.

For example, if a company issues a human rights impact assessment, the quality and sufficiency of that reporting – both in terms of data released and the programs described – would require a high level of topic-area expertise. It would also require assessment from a country-specific lens. This level of knowledge-building and staffing during the earlier stages of this program would need to be foundation-funded. As the utility of the data becomes more clear to companies and investors, it may transition to being partially or fully funded by other income streams.

Researchers and research infrastructure is also needed for the collection and assessment of



company performance beyond a company’s own reporting. Companies rarely volunteer data which presents their actions poorly or might lead to legal or brand risk. As such, research infrastructure is needed to verify claims that corporate policies have resulted in well-implemented and effective programs and that harms have not occurred.

*“ We need to be able to look beyond rhetoric and PR. Policies are insufficient.”*

— Interviewee

#### **4. A credible third-party assessor**

A credible, impartial evaluator of company performance would allow for the emergence of a shared industry benchmark, resulting in a “race to the top” as companies see the effects of their efforts and are rewarded for improvements – or pilloried for any regressions.

*“ An incomplete impact assessment is difficult to assess because of the unknown unknowns. It’s impossible to know how much was excluded from the report.”*

— Interviewee

In the climate action realm, the CDP has played this role, growing from a data-collecting nonprofit to the central repository of company performance and comparative data, and of important geographical and industry analyses. The CDP serves as a hub, providing visibility for companies that lead the private sector as well as for those that are just getting started. The organization offers a supportive onramp and roadmap to direct corporations on their climate journey. CDP celebrates leaders and generally shies away from direct criticism of laggards, but has continued to raise the bar in terms of corporate climate action. An analogous body for the tech sector would assist both investors and corporations in evaluating their ranking relative to peers on the dynamic topics covered by tech’s societal impact.

#### **5. A watchdog**

On the topic of corporate money in politics, organizations such as OpenSecrets and the Center for Political Accountability keep companies accountable for their direct and indirect political spending and the transparency they provide. In other areas, such as CEO compensation, racial justice and toxic substances in consumer goods, *As You Sow’s* deep expertise and company relationships help mobilize investors to engage their portfolio companies. These nonprofits’ work sheds light on companies whose actions (or inaction) are particularly egregious, and support investor engagements on topics that may be regulated or technical.

The watchdog role, which sustains scrutiny on areas that companies do not want to discuss, is essential in pushing forward a more nuanced public understanding of corporate behavior.

## 6. Falling share prices

While it may seem counterintuitive, the recent crash in the share prices of the leading tech companies provides an opening for pressuring these companies through investor action. The tech sector has been the darling of equity investors for many years. Shareholders believed that they could do no wrong and shied away from criticizing the companies, preferring to sit back and enjoy the share price ride. “Why rock the boat?” had been the investor mindset until recently.

Now, share prices are falling and the entire sector is under the investor microscope. For example, this year, Meta’s share price dropped nearly 70% (as of 11/21/22), and Elon Musk’s management approach during his takeover of Twitter has been widely panned. Investors are wondering what signs of distress they missed and how to avoid similar disasters in the future. This means they are more willing to look deeply into the governance practices of these companies and to be more critical.

This has a parallel in the crash of the oil and gas sector several years ago. Oil and gas had been one of the most profitable sectors for many years, then fell dramatically in 2015-2016 and plateaued after that. This opened up the sector to greater scrutiny by investors who were encouraged to start asking questions about how the industry would deal with the challenge of climate change. While these companies have rallied recently, investor pressure has not relented. Thus, the current travails of the companies in the tech sector may present an opening for critics and advocates to find common cause with the investor community.

## Section II: The Technology Accountability Framework

Given the objective of creating a usable, practical framework for investors to understand and evaluate tech’s impacts on society, Whistle Stop focused on creating a **governance-centered** framework to emphasize the high-level oversight of the issue. This approach offers a number of advantages:

- It provides an overarching view of company management of emerging risks and impacts. It’s particularly appropriate for dynamic topics such as those under consideration here, where next year’s issue is unknowable.
- It allows for more relevant comparisons between companies, because it is less dependent on a specific business model or technology.
- It capitalizes on the fact that corporate governance is already central to investment decisions, and is therefore more familiar and accessible to a securities analyst.
- Starting with the governance of emerging issues, where best practices are still taking shape and likely to evolve, has been a well-trodden path to harness and catalyze investor engagement. This is illustrated in Whistle Stop Capital’s report *Landscape Report on Shareholder Engagement and Activism Strategies*.

There are, however, topic-specific considerations that a broad governance framework might miss. To remedy this, we also created a secondary framework to assess a relatively mature topic, as an illustration of the specific controls a company might have to manage and mitigate risks. After

considering the full range of issues, we selected one where regulation<sup>1</sup>, civil society, and companies have started to establish policies and practices: data privacy, and the related topic of data security.

Informed by the civil society and investor stakeholder engagements mentioned above, as well as a careful review of existing standards and frameworks, we synthesized relevant sub-topics into two frameworks. Their joint use was designed to result in an assessment with the following characteristics when applied to large, publicly listed technology companies:

- thorough coverage of the major relevant privacy topics
- reflective of current-day best practices and also indicative of areas where more data and research might be needed
- practical, i.e., not so detailed or extensive that a generalist investor would find it too onerous to utilize.

Please note that this only applies to data privacy and security, and not to tech’s impact on society more broadly. It is intended as an illustration of how investors might create other, complementary scores for tech companies when assessing other topics such as AI explainability, access, etc.

This framework is subject to a few important limitations: first, we expect these combined frameworks to be useful in assessing large, public, and well-scrutinized companies’ management of their impacts on society. These assessments rely entirely on publicly available information. Private companies or those with poor disclosures on these still largely unregulated topics will prove much more difficult to evaluate with the tools outlined below.

*“What is the core of the business model? Is it for advertisers, is it for the analysis of personal data? Will it lead to the development of awful algorithms?”*

— Interviewee

Second, there are crucial considerations based on a company’s business model. For example, as concerns data privacy, investors should consider whether data brokers can ever be considered “responsible” investments or reasonable engagement targets. Tobacco offers a helpful analogy, as their business model relies on producing and selling goods that are inherently damaging. Similarly, data brokers collect and aggregate data from disparate sources and sell manufactured consumer profiles that may turn out to be shockingly intrusive. Data privacy and security are not risks to be managed but rather obstacles to building their products and services. As with traditional “sin” stocks, a concerned investor may determine that they are not adequate engagement targets as the shareholder might be effectively asking the company to withdraw from its core business.

A good framework will be forward-looking, aware of and utilizing the data it has now, but also recognizing that companies don’t volunteer information that might put them in a bad light unless they are pressed by investors or regulators. Knowing they will be asked, however, can jumpstart or speed

---

<sup>1</sup> Several notable markets regulate consumer data use and privacy, such as the EU GDPR, the UK Age Appropriate Design Code, the California Consumer Privacy Act, and the California Age-Appropriate Design Code Act.

up programs, to avoid publicly lagging peers. An important part of catalyzing change is creating the incentive structures to improve programs, alongside the ability to recognize and commend improvements once they have been made.

# The Corporate Governance Framework

The Corporate Governance Framework is composed of 77 indicators organized into 9 sections: Policy commitment, Governance and management oversight, Risk and opportunity identification, Internal implementation, External relationships, Assessment, Accountability, Transparency, and Relationship to shareholders.

## THE CORPORATE GOVERNANCE FRAMEWORK

### → Policy commitment

#### ▶ Precautionary Principle

- Does the company state that it employs the precautionary principle,<sup>2</sup> or equivalent?
- Are there public examples of the company's use of the precautionary principle, such as:
  - taking preventive action in the face of uncertainty?
  - shifting the burden of proof to the proponents of an activity?
  - exploring a wide range of alternatives to possibly harmful actions?
  - increasing public participation in decision-making?

#### ▶ Culture

- Has the company made statements around its commitment to civil society?
- Are these statements mirrored by the executive team in public communications?

### → Governance and management oversight

#### ▶ Board oversight

- Does the company state that the Board of directors exercises formal oversight over the company's impact on society?
- Does the company disclose the process followed by the Board to exercise its oversight over the company's impact on civil society?
- Does the board review performance measures related to the company's impact on civil society at each Board meeting?
- Does at least one fourth of the board participate in a committee related to the company's impact on civil society?

#### ▶ Executive level oversight

- Does an executive-level committee or officer oversee how company policies and practices impact civil society?
- Does the company disclose the process followed by the executive-level employee(s) to exercise this oversight?
- Are expectations for this role clearly defined and made public?

---

2 The Precautionary Principle is the idea that a harm does not need to be irrefutably proven before action is taken to avoid it.

- Is executive remuneration linked to the achievement of goals related to civil society impact?
- ▶ **Board level competency**
  - Does the company state that the board has civil society expertise?
  - Does the board define this civil society expertise and its origins?
- ▶ **Executive level competency**
  - Does the company state that the executive level has civil society expertise?
  - Does the company define this executive level civil society expertise and its origins?

## → Risk and opportunity identification

- ▶ **Risks and opportunities**
  - Does the company have a process for identifying, assessing, and responding to civil society-related risks and opportunities?
  - Is the risk management team independent, appropriately qualified and sufficiently resourced?
  - Does the risk identification team have clear and sufficient channels for the escalation of concerns?
  - Do external stakeholders have clear and sufficient channels for the escalation of concerns?
- ▶ **Product use**
  - Is a process established for identifying , assessing and mitigating risks associated with direct product use, both intended and unintended?
  - Is a process established for identifying , assessing and mitigating risks associated with indirect product use, both intended and unintended?

## → Internal implementation

- ▶ **Dedicated staffing**
  - Does the company clearly disclose that it has internal staff experts in understanding its impact on civil society?
  - Do internal staff have appropriate expertise for the civil society issues most likely to face the company?
  - Are measures of the effectiveness of the internal team clearly defined?
  - Does the internal team report to the executive level?
  - Does the internal team have direct access to the board?
  - Is the internal team sufficiently resourced?
- ▶ **Employee involvement**
  - Does the company clearly disclose that it provides employee training on civil society issues?
  - Are employees incentivized to encourage alignment with civil society goals?
- ▶ **Employee empowerment**
  - Do employees have a protected mechanism to communicate with each other and external stakeholders around civil society issues?
  - Do employees have an anonymous mechanism to elevate concerns to the board?
  - Does the company state that it does not use concealment clauses?

## → External relationships

### ▶ Expertise

- Does the company participate in organizations or events intended to increase its ability to understand and address civil society concerns?
- Does the company provide financial support to organizations or events intended to build out the ecosystem of organizations addressing civil society concerns?

### ▶ Empowerment

- Does the company have a clear mechanism for stakeholders to request remedy and to appeal decisions?
- Are consumers able to determine the scope of their interactions with the company's technologies?
- Does the company maintain a third party managed whistleblower program for employees and other stakeholders to report concerns?

### ▶ Public policy involvement

- Does the company report on its political involvement in alignment with the CPA-Zicklin Index?
- Does the company report on how its political giving aligns with its publicly stated values?
- Does the company provide supporting data to show that it is monitoring and modifying its political involvement as needed to remain in support of its publicly stated values?

## → Assessment

### ▶ Metrics

- Has the company set measures and metrics to assess its societal impact?
- Are metrics to assess societal impact set with guidance and feedback from experts?
- Has the company evaluated the impact of removing or modifying a service, given civil society concerns?
- Does the company's assessment and review process have an accessible and trustworthy forum to provide anonymous feedback?
- Does the company make clear how it assesses the effectiveness of its civil society assessment program (e.g., what indicators or metrics, if any)?

### ▶ Process

- Does the company conduct country-specific assessments?
- Does the company conduct scenario analyses related to its civil society impact?
- Does the company consider indirect as well as direct civil society impacts?

### ▶ Target setting

- Has the company set targets relative to its policies and programs?
- Did the setting of these targets involve internal and external stakeholders?
- Do targets address short and long-term goals?

## → Accountability

### ▶ Committee oversight

- Does the company have an independent, committee comprised of civil society experts to review its societal impact?
- Does that committee have the appropriate level of expertise?

- Is the committee independently governed and remunerated?
  - Does the committee have the ability to prevent the development of, or end the use of, products or services which are concerning?
- ▶ **Changed practices**
- Are there examples of the company having ceased or significantly modified a project or product due to its initial negative societal impact?
  - Has the company undertaken mitigation efforts related to a harmful product or service?
  - Does the company change programs or policies when it fails to meet its civil society-related targets?

## → **Transparency**

- ▶ **Public reporting**
- Does the company report publicly on its civil society programs?
  - Does the company report the outcomes of its civil society assessments?
  - Does the company openly discuss challenges and lessons learned?
  - Does the company report at least once a year?
- ▶ **Data verification**
- Is the company's reporting audited by an independent third party?
- ▶ **Disclosure**
- Are individuals made aware of the ways the company revenue is reliant on an individual's engagement with the company's products or services?
  - Does the company share with end users what data it collects and how it is used?

## → **Relationship to shareholders**

- ▶ **Board structure**
- Are the board chair and CEO roles held by different people?
  - Is the board Chair an independent board member?
  - Are less than 15% of shares held by the board or executive officers?
  - Is the board more than 75% independent?
- ▶ **Responsiveness**
- Has the company been responsive to shareholder resolutions that received more than 40% of investors' support?
  - Are stakeholders able to contact the board directly?
  - If the company has multiple share classes, are voting rights consistent across shares?

# Data Privacy Framework

The topic-specific Data Privacy Framework is composed of 70 indicators organized into seven sections, primarily mirroring the broader governance framework structure: Policy commitment, Governance and management oversight, Risk and opportunity identification, Internal implementation, Assessment, Accountability, and Transparency. The internal implementation section is the most extensive, as it covers the indicators we would seek as specific evidence of the company's implementation of data privacy.

## THE DATA PRIVACY FRAMEWORK

### → Policy Commitment

- ▶ Precautionary Principle
  - Does the company have a policy stating that its use of private user data is proportional to business need?
- ▶ Culture
  - Has the company made statements around its commitment to data privacy?
  - Has the company described its business model for the use of user data?

### → Governance and management oversight

- ▶ Board level competency
  - Does the company state that the Board has expertise on data privacy and security?
  - Does the board define this data privacy and security expertise and its origins?
- ▶ Executive level competency
  - Does the company state that the executive level has data privacy and security expertise?
  - Does the company define this executive level data privacy and security expertise and its origins?

### → Risk and opportunity identification

- ▶ Risks and opportunities
  - Does the company have a process for identifying, assessing, and responding to user data privacy-related risks or opportunities?
- ▶ Sector-specific risks
  - Does the company collect, access, or manage or otherwise handle sensitive personal data, such as financial data or health data?
- ▶ Demographic-specific risks
  - Does the company collect, access, or manage or otherwise handle the private data of vulnerable people, e.g. children, people with disabilities, domestic violence victims, etc.?
- ▶ Geography-specific risks



- Does the company collect, access, or manage or otherwise handle private data in locations where access to that data may put people at risk?

## ➔ Internal implementation

### ▶ Dedicated staffing

- Does the company have a chief privacy officer, chief security officer, or equivalent?
- Does the company have a privacy and security or privacy and security-related staff committee?
- Is at least one member of the board regularly briefed, or provide oversight of, the privacy and security committee?

### ▶ Employee involvement

- Does the company clearly disclose that it provides employee training on data privacy and security issues?
- Are employees incentivized to encourage alignment with data privacy and security goals?

### ▶ Data collection

- Do the company's security and privacy practices change depending on 'level' of privacy of data collected (e.g. personally identifiable information (PII), protected health information (PHI), personal data, sensitive personal data...)?
- Is user data collected only with consent, or with an alternative legal basis?
- Does the company seek to minimize the amount of private data it collects?
- Do users have the option to request a copy of the data that is collected across various products and services?

### ▶ Data management

- Do users have the right and ability to alter and delete their data permanently from company systems ("right to be forgotten")?

### ▶ Data use

- Has the company set limitations on primary data use?
- Does the company provide or ensure customer/data user (if different from user, e.g. an employer or advertiser) training on appropriate usage of private data?
- Does the company conduct Know Your Customer (KYC) or other due diligence on customers?
- Has the company set limitations on its product use by certain customer types, e.g. government, law enforcement, defense or intelligence companies, data brokers, etc?
- Do users have the right and ability to control how their information is used, particularly for advertising purposes or AI development purposes?
- Has the company built in usage limitations on secondary data uses?
- Has the company set conditions and/or limitations on secondary data uses by its customers, for example in its product terms of service or other legal provisions?
- If so, do these conditions and/or limitations on secondary data uses cover the combination of data from several sources, e.g. several of its products?
- Does the company employ heightened thresholds for data usage for vulnerable groups, e.g. children or human rights defenders living under authoritarian regimes?

### ▶ Data storage

- Does the company retain private user data? (1 if it does not do so)
- If it does retain data, does it disclose the time period during which it retains this data?

- Does the company disclose its storage practices of private user data?
- If so, do its data storage practices include any of the following best practices: encryption, anonymization, or aggregation?

▶ **Data distribution**

- Does the company sell, rent, or otherwise provide private user data to third parties? (1 if it does not do so)
- Does the company rely on a robust framework for the conditions under which it provides user data in response to law enforcement requests?
- Does the company employ heightened thresholds for data distribution for vulnerable groups, e.g. children, people with disabilities, women in states that have limited reproductive freedoms, dissidents, journalists, human rights defenders in authoritarian regimes?
- Does the company require its suppliers to uphold the same privacy standards as those to which it holds itself?
- Does the company require its business partners (e.g. mobile apps) to uphold the same privacy standards as those to which it holds itself?

▶ **Product design, development and deployment**

- Does the company rely on “privacy by default/ by design” principles in product design, development, and/or testing?
- Does the company limit employee and other privileged access to user data to those with a strict “business need to know”?
- Does the company’s product include the ability to disable or shut down (a “kill switch”) its technology in the event of a known violation or misuse of the product?
- Does the company monitor whether its privacy management processes are sufficient post-deployment?

▶ **Data security**

- Does the company follow best practice data privacy principles as laid out in the AICPA’s Privacy Management Framework<sup>3</sup>?
- Does the company follow best practice data privacy and security technology to ensure it is following the PMF principles, e.g. end-to-end encryption, two-factor authentication, etc?
- Does the company have SOC 2 certification (Type 2) and/or HIPAA audit?
- Does the company have best-practice protocols to address all cases of data leaks, breaches, hacks, or theft, ex post, as outlined by the FTC?<sup>4</sup>
- Does the company regularly test its own data security processes to ensure they are effective and sufficient?
- Does the company monitor whether its data security processes are sufficient post-deployment?
- Does the company track and monitor legislative developments and regulations related to privacy and data security?
- Has the company avoided data leaks, breaches, hacks, or theft?
- Are end users given the right to opt out of certain types of data usage?

➔ **Assessment**

▶ **Metrics**

- Has the company set measures and metrics to assess the strength and effectiveness of

---

3 <https://us.aicpa.org/interestareas/informationtechnology/privacy-management-framework>

4 <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>

its data security systems?

## → **Accountability**

### ▶ **Violations**

- Has the company avoided General Data Protection Regulation (GDPR) violations or fines?

### ▶ **Existing framework alignment**

- Is the company compliant with:
  - GDPR guidelines?
  - EU-US and Swiss-US Privacy Shield frameworks?
  - Digital Advertising Alliance's Self-Regulatory Principles for Online Behavioral Advertising?

## → **Transparency**

### ▶ **Public reporting**

- Does the company publish a transparency report?
- If so, does the report include the number of law enforcement requests for data it received?
- If so, does the company report on its response to each?
- If so, does the company report on its process to determine whether the provision of user data to the government was warranted?
- Does the company report on how often the board is briefed on privacy and security issues?
- Does the company report the number of users whose information is used for secondary purposes?
- Does the company disclose the total amount of monetary losses as a result of legal proceedings associated with user privacy?
- Does the company disclose a list of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring? (if applicable)
- Does the company disclose:
  - the number of data breaches it has encountered?
  - the percentage involving personally identifiable information (PII)?
  - the number of users affected?
- Does the company disclose how information handling practices at each stage of the information "lifecycle" (i.e., collection, usage, retention, processing, disclosure, and destruction of information) may affect individuals' privacy information?

# Lessons from the Use of the Framework

We applied this framework to a sample of five tech platforms: Alphabet, Amazon, Meta, Twitter, and Yelp. This small universe of companies shouldn't be considered representative of all tech companies, but these large, public (or formerly public) firms have been scrutinized by users, regulators, and civil society alike for their impacts on society. The indicators were each equally weighted; other analysts may choose to place greater weight on certain topics or subtopics. We also set each indicator towards a positive outcome. That is, in each binary 1/0 allocation, a "1" indicates a positive practice.

The framework yields significant insights around company preparedness to strategically manage rising tech accountability issues, as well as current oversight of privacy concerns.

Even though we would expect these companies to be some of the most forthcoming, we must remember that, given the nascent nature of this framework, they have not yet been asked to report on a number of these indicators. This said, their disclosures exhibited significant gaps, as well as some encouraging signs, which we delve into below.

Note that we did not seek to weight sections or indicators, though if one were particularly interested in certain sections or felt that certain indicators were particularly important, changing weightings would be a simple way to emphasize them in the resulting company scores. For example, this is how the CPA's Zicklin Index is structured. Given this, we have not determined what, for instance, a "passing" score would be on our two frameworks.

Note about Twitter: this analysis was based on information released by Twitter before it was taken private by Elon Musk. There is no way to know if the company will continue with the same level of disclosure going forward. Thus the company's ratings should be understood as an historical analysis rather than a characterization of how the company currently operates.

**Table 1: Overall Framework Scores**

	Alphabet	Amazon	Meta Platforms	Yelp	Twitter
Governance	31%	30%	39%	16%	35%
Privacy	51%	40%	44%	16%	42%
<b>Total</b>	<b>41%</b>	<b>35%</b>	<b>41%</b>	<b>16%</b>	<b>38%</b>

# 1. Company performance on overall governance framework

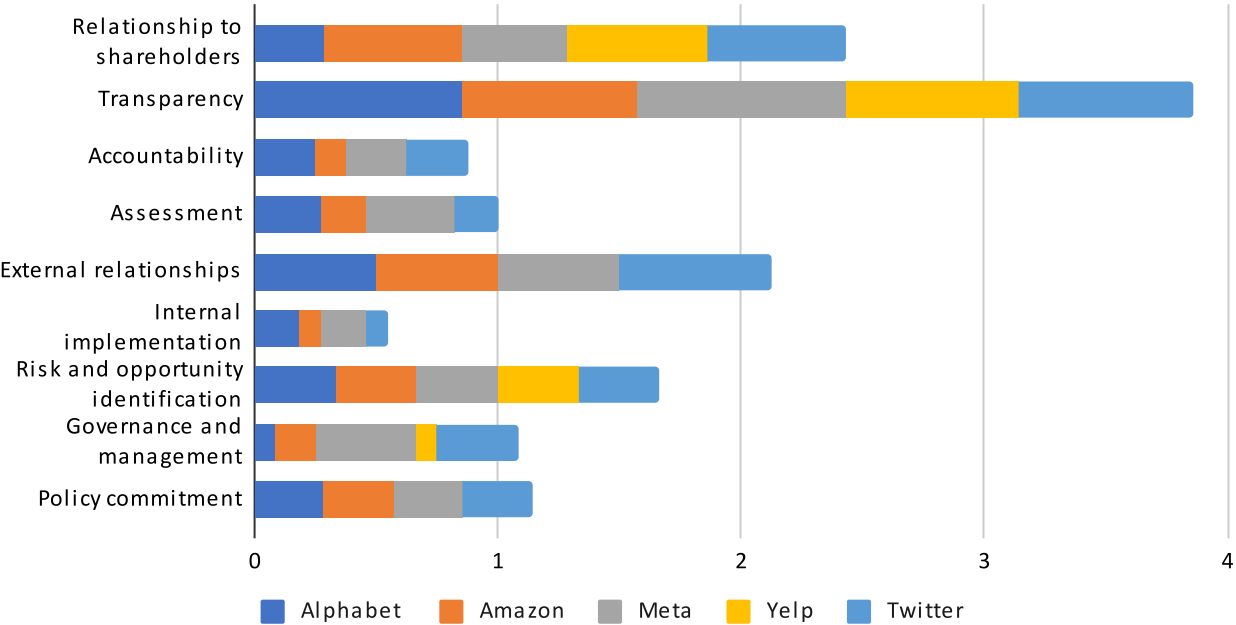
As a percentage of total available points, these test companies’ practices were notably strongest when it came to Transparency. They scored the lowest possible relative points when it came to Internal Implementation, Accountability and Assessment.

Meta and Twitter (pre-takeover) had the highest overall scores. This should not be interpreted as a commendation of these companies, simply a relative assessment. All companies were lacking in 60% of the Governance Framework’s desired actions.

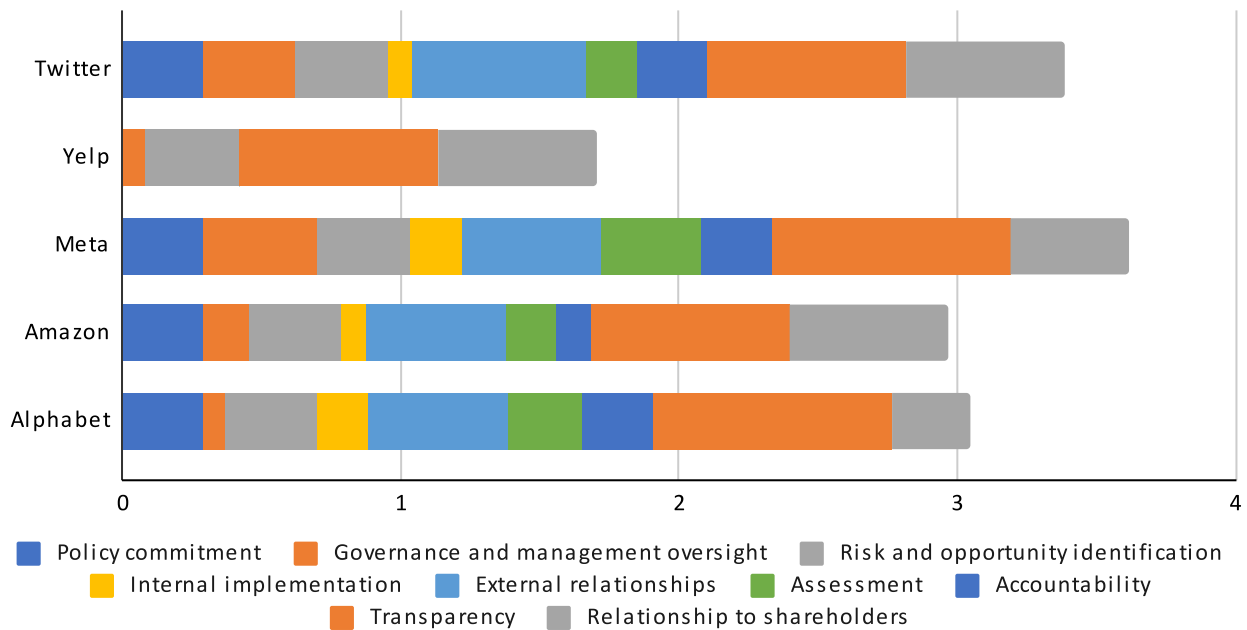
**Table 2: Governance Topic Scores**

	Alphabet	Amazon	Meta	Yelp	Twitter
<b>Policy Commitment</b>	29%	29%	29%	0%	29%
<b>Governance and Management Oversight</b>	8%	17%	42%	8%	33%
<b>Risk and Opportunity Identification</b>	33%	33%	33%	33%	33%
<b>Internal Implementation</b>	18%	9%	18%	0%	9%
<b>External Relationships</b>	50%	50%	50%	0%	63%
<b>Assessment</b>	27%	18%	36%	0%	18%
<b>Accountability</b>	25%	13%	25%	0%	25%
<b>Transparency</b>	86%	71%	86%	71%	71%
<b>Relationship to Shareholders</b>	29%	57%	43%	57%	57%

**Governance, Topic Performance**



## Governance, Company Performance



## 2. Company performance on data privacy framework

Within the topic-specific framework, while most of the companies’ total scores were similar (Yelp was anomalous) there was significant variance in company performance by topic area. It is important to note that the Internal Implementation topic area held 41 indicators, while the “Assessment” indicator held only one. Therefore, each topic area does not hold the same level of granularity and nuance in the information it provides.

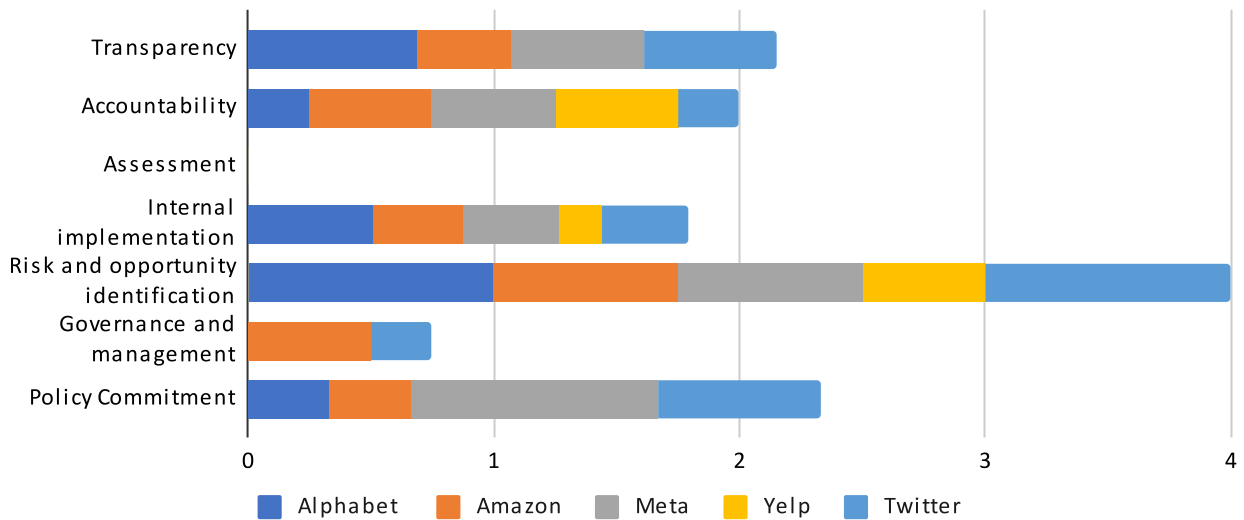
Within Internal Implementation, the most robust and nuanced topic area, Alphabet outperformed, with a positive score at just over half of the indicators. It lagged behind Amazon in its Governance and Management Oversight score, however, and Meta in its Policy Commitment.

Accountability here assesses company adherence to existing regulations, as well as any media coverage of violations of those regulations; companies’ relatively high scores here show that when faced with specific rules, they are able to rein in their practices to avoid breaking the law. None of the companies earned a positive mark for their assessment practices, as, concerningly, none of them had “set measures and metrics to assess the strength and effectiveness of its data security systems.”

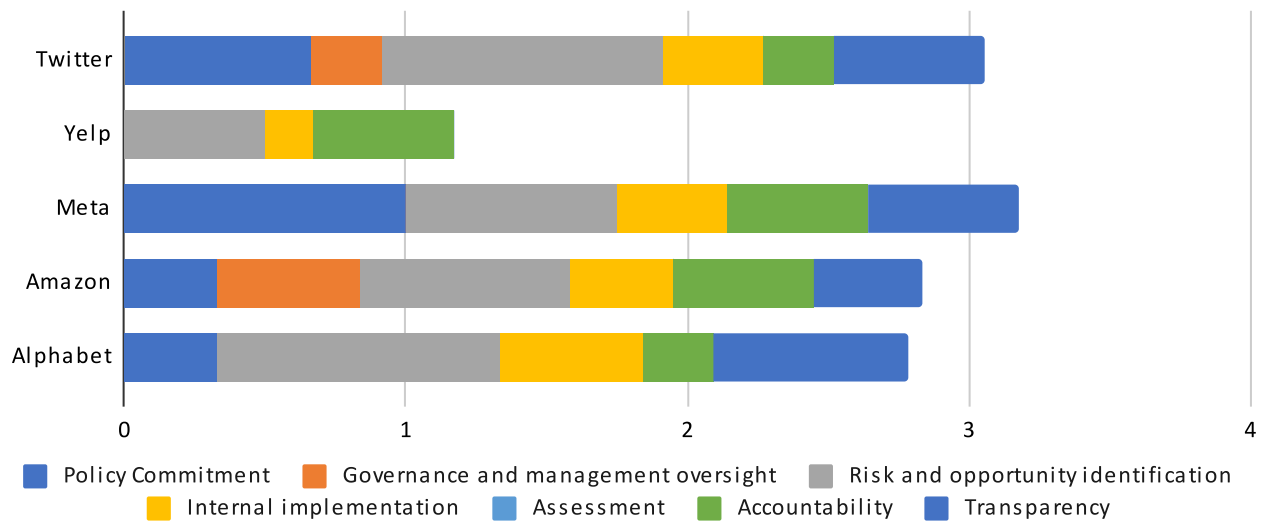
**Table 3: Privacy Specific Framework Scores**

	Alphabet	Amazon	Meta	Yelp	Twitter
<b>Policy Commitment</b>	33%	33%	100%	0%	67%
<b>Governance and Management oversight</b>	0%	50%	0%	0%	25%
<b>Risk and Opportunity Identification</b>	100%	75%	75%	50%	100%
<b>Internal Implementation</b>	51%	37%	39%	17%	35%
<b>Assessment</b>	0%	0%	0%	0%	0%
<b>Accountability</b>	25%	50%	50%	50%	25%
<b>Transparency</b>	69%	38%	54%	0%	54%

**Privacy, Topic Performance**



**Privacy, Company Performance**



Before the Framework can be formally launched, a more in-depth and wider-reaching stakeholder engagement process must be followed. This allows for additions, edits and corrections from key knowledge hold-ers on the topic area of concern. The Frameworks above would, at this point, more akin to halfway risen dough than a loaf of bread. A number of steps remain before the research above would be considered sufficiently vetted to share with a broader community of investors or to use as a base from which companies might be engaged.

## Next Steps

The above Framework was developed as a learning and research tool on the state of current tech accountability expectations and as an illustration to the NetGain Partnership the actions needed in order to develop a meaningful framework on a tech accountability issue area.

Should the NetGain Partnership decide to move into the next phase with the Framework, a number of additional steps would be needed. These are detailed in the *Moving Forward* report.

## Appendix 1: Organizational Content Reviewed

The tech accountability expectations of each of the following organizations were reviewed in order to identify consistent themes and expectations for corporate behavior.

<b>Standard/dataset</b>	<b>Creator</b>
10 Principles for Ethical AI	UNI Global Union
Accountability and Transparency	Cigref, Syntec Numerique
AI and Human Rights Report	All Tech Is Human



<b>Standard/dataset</b>	<b>Creator</b>
AI Ethics Principles & Guidelines	Dubai
AI in the UK: Ready, willing and able?	United Kingdom
AI System Ethics Self- Assessment Tool	Dubai
AI-RFX Procurement Framework	Institute for Ethical AI & Machine Learning
Algorithmic Equity Toolkit	ACLU
Algorithmic Impact Assessment	Canada
All Tech is Human Report	All Tech is Human
Analysis of Ethical Issues Report	Tech Ethos
Analysis of International and EU law and policy	Tech Ethos
Artificial Intelligence Impact Assessment	ECP
Asilomar AI Principles	Future of Life Institute
Auditing Black-box Models for Indirect Influence	algofairness
B-Tech Project	UN OHCHR
Civil Rights Table Principles	Civil Rights Table
Code of Practice on Disinformation	European Union
Companion to the Model AI Governance Framework – Implementation and Self-Assessment Guide for Organizations	Singapore,World Economic Forum
Confronting Bias: BSA's Framework to Build Trust in AI	BSA   The Software Alliance
Content Governance Metrics (forthcoming)	SASB
Data Ethics Impact Assessment	Data Ethics
Data for Children Collaborative Ethical Assessment	UNICEF
deon Ethics Checklist	Driven Data
Digital Catapult Ethics Framework	Machine Intelligence Garage
Digital Decisions Tool	Center for Democracy & Technology
Digital Inclusion Benchmark	World Benchmarking Alliance
EqualAI Framework & Checklist	EqualAI
Ethical Application of Artificial Intelligence Framework	American Council for Technology-Industry Advisory Council
Ethical Framework for a Good Society	AI4People
Ethical Guidelines	Japanese Society for AI
Ethically Aligned Design	IEEE Global Initiative
EthicalOS Toolkit	Institute for the Future,Omidyar Network
Ethics & Algorithms Toolkit	GovEx,City and County of San Francisco,Harvard DataSmart,Data Community DC
Ethics and algorithmic processes for decision making and decision support	Algorithm Watch
Ethics for Sustainable AI Adoption	Association of Chartered Certified Accountants

<b>Standard/dataset</b>	<b>Creator</b>
Ethics Guidelines for Trustworthy AI	European Commission
EthicsGrade Ratings Database	EthicsGrade
Fair Information Practice Principles	OECD
Foresight into AI Ethics	Open Roboethics Institute
Global Network Initiative Principles	Global Network Initiative
Governing Artificial Intelligence: Upholding Human Rights & Dignity	Data & Society
Guidance on Human Rights Impact Assessment of Digital Activities	Danish Institute for Human Rights
Guidance on Implementing the UNGPs for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities	United States
Guidelines for the Ethical Development of AI and Big Data Systems: An Ethics by Design approach	SHERPA
Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data	OECD
Handbook on Non-Discriminating Algorithms	Netherlands,Tilburg University
Human Rights and Technology Final Report	Australian Human Rights Commission
ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights	Shift Project,Institute for Human Rights and Business
IEEE Algorithmic Bias Considerations	IEEE Standards Association
IEEE Ontological Standard for Ethically Driven Robotics and Automation Systems	IEEE Standards Association
IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being	IEEE Standards Association
IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children	IEEE Standards Association
IEEE Standard for Data Privacy Process	IEEE Standards Association
IEEE Standard for Transparent Employer Data Governance	IEEE Standards Association
Internet Media & Services Sustainability Accounting Standard (forthcoming)	SASB
Investigate	American Friends Service Committee
Investor Toolkit on Human Rights	Investor Alliance for Human Rights: An initiative of ICCR
Investors' Expectations on Responsible Artificial Intelligence and Data Governance	Federated Hermes
ISO/IEC 27001 Information Security Management	International Standards Organization
ISO/IEC JTC 1/SC 42: Artificial intelligence	International Standards Organization
Model Artificial Intelligence Governance Framework	Singapore
Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors	Heartland Initiative,Access Now,Business & Human Rights Resource Centre

<b>Standard/dataset</b>	<b>Creator</b>
OECD AI Principles	OECD
Organisation Best Practice	Foundation for Best Practices in Machine Learning
Principles for Accountable Algorithms and a Social Impact Statement for Algorithms	FAT/ML
Principles to Promote Fairness, Ethics, Privacy Management Framework	Singapore American Institute of CPAs
Project ExplAIIn	United Kingdom, Alan Turing Institute
Rabat Plan of Action & Threshold Test	UN OHCHR
Ranking Digital Rights Index	Ranking Digital Rights
Report on freedom of expression, states, and the private sector in the digital age	UN OHCHR
Salient Issue Briefing: Conflict & Security	Investor Alliance for Human Rights
Salient Issue Briefing: Discrimination	Investor Alliance for Human Rights
Salient Issue Briefing: Freedom of Expression	Investor Alliance for Human Rights
Salient Issue Briefing: Political Participation	Investor Alliance for Human Rights
Salient Issue Briefing: Privacy & Data Protection	Investor Alliance for Human Rights
Surveillance and human rights	UN OHCHR
Tech Giants and Human Rights: Investor Expectations	Danish Institute for Human Rights, Swedish Council on Ethics
Technical Best Practice	??
Tenets of the Partnership on AI	Partnership on AI
The Box: A Tool for Operating AI Principles	AI Ethics Lab
The Montreal Declaration	Universite de Montreal
The Responsible Machine Learning Principles	Institute for Ethical AI & Machine Learning
Toolkit for Centering Racial Equity Within Data Integration	Actionable Intelligence for Social Policy
UnBias Fairness Toolkit	Proboscis
Universal Guidelines for Artificial Intelligence	The Public Voice
Web Content Accessibility Guidelines	G3ict