OMIDYAR NETWORK™

July 2019

Race to the Top: A Coalition Building a New Paradigm for Identity Data

Data is at the heart of the digital revolution and has created immense economic and social value. And it will continue to play a vital role in solving the biggest problems of our time and fueling economic growth. As such, data is critical to us as individuals, technologists, investors, and entrepreneurs interested in a healthy society of empowered people.

The companies we invest in as VCs are at the center of the data economy. Competitive dynamics, and the drive toward growth, are driving some parts of the sector toward ever-more intrusive forms and amounts of data collection. Two risks emerge from this dynamic. As time goes on and our data changes hands, the way it is used can stray from our original preferences, violating our privacy. As a result, we have seen a series of systematic failures across the industry, including security breaches, privacy violations, bias and a lack of transparency.

As consumers have become more aware, there preferences have changed very clearly and quickly.

- In March of this year 58% of respondents to an Axios survey agreed with the following statement: "The privacy threat is a crisis, and we need to force companies to change." This was up from 51% in 2018.
- Axios also asked for a response to the following: "Online services are essential, and we all have to accept some risk." The share agreeing with this statement dropped from 46% to 38%.
- This extends beyond privacy.
- 58% of Americans feel that computer programs will always reflect some level of human bias (Pew)
- According to HSBC, more people would trust flipping a coin than getting mortgage advice through machine learning.
- A recent paper estimated that over 130 bills have been introduced at various levels of government in the US alone. Thus, not only do current practices contribute to the tech backlash, the regulatory response also creates immense risk for businesses and for investors.

If today's data practices are causing people to feel disempowered and eroding their trust, then we have now entered a downward spiral – *a race to the bottom* – in which the competitive dynamics of the industry are increasingly at odds with the interests of individuals. This downward spiral cannot persist without eventually reaching a failure point at which customer engagement, trust, traction, and commercial viability becomes irreversibly damaged. The VC industry, in the view of some, has contributed to the problem by prioritizing growth over trust. Our view is that the VC industry can play a key play role in being part of the The VC industry can be part of the solution, along with technologists, lawyers, regulators, and CEOs.

A group of investors, technologists, and thought leaders have come together to replace this dynamic with a *Race to the Top* – a new business paradigm for the use of personal data that prioritizes the trust of individual consumers of our products and services. To build trust, the group prioritizes the safety and agency of consumers and individuals in products and services.

The group, which has had an initial convening in May and several calls, is working toward:

- a common set of principles to guide investment decisions that build trust and to help investees (please see working draft below);
- tools for supporting investment decisions at each stage of the VC life cycle;
- tools for the companies we invest in, to ensure that their products are aligned with committed values and contribute to a *Race to the Top.*

To be used by VCs, these principles and tools must be co-developed by VCs and informed by industry experts. There are currently 13 VCs and 5 thought leadership organizations participating in the coalition. Participating Organizations: Omidyar Network, International Finance Corporation, National VC Association, Internet Trust Exch. Gov. Association (ITEGA), PTB Ventures, Pick Axes & Shovels, Harvard Kennedy School, DBL Ventures, West Wave Capital, Anthemis Capital, Glasswing Ventures, Structure Capital, Flourish Ventures, Firefly Ventures, Georgian Partners, QED Ventures, Greater than X, MIT Media Lab.

Omidyar Network is supporting the coalition by commissioning background studies to identify and strengthen the commercial case for a new paradigm. The papers will address the following issues:

- Detailed analysis of consumer preferences regarding privacy, safety and security of information technology products. To what extent have consumer preferences changed, and will this result in a material shift in growth from products that are perceived to create risks and harms and toward those that are perceived to be more aligned with privacy and safety?
- Analysis of the emerging policy and regulatory framework at the Federal and State level concerning privacy and product safety. What are the downside risks and liabilities facing both enterprises and VCs who do not shift to more privacy-enhancing business models? What are the business practices that will be incentivized or disincentivized by the emerging policy and regulatory framework?
- What are examples of firms, enterprises and business models that represent a Race to the Top?

The next convening of this group will be on September 13, 2019 at Mozilla HQ at Mountain View. We seek to hear presentations on these issues, finalize the principles and move forward on development of tools and approaches for VCs.

Magdi M. Amin, Investment Partner, Omidyar Network Mamin@Omidyar.com
Gordon Myers, Chief Counsel, IFC. Gmyers@ifc.org
Abiah Weaver, Director, Strategic Marketing & Communication, Omidyar Network Aweaver@Omidyar.com

Working Draft Principles: Race to the Top

Principle	Elaboration
1. Benefit	Technology should provide customers, individuals and communities with access to products, services and capabilities that benefit them. Data creates immense economic value. Businesses should share a fair and meaningful part of this economic value with individuals.
2. Fairness and Inclusion	Technology should be applied in a fair and non-discriminatory manner. Businesses should ensure that no group of individuals are systematically denied access to their data or associated rights. Technology should be developed in a manner that assures outcomes reflecting the requirements of individuals and communities expected to use or benefit from the innovation. Companies should use best efforts to avoid bias, discrimination, or adverse effects.
3. Transparency & Accountability	Businesses should be transparent about their data practices and hold themselves accountable to their customers' expectations. ● Proactive disclosures: Companies should regularly inform individuals about the data it collects, how it uses it and the potential harms. ● Purpose limitation. Data use should be limited to the purposes for which the consent of individuals was obtained. Technology providers are accountable for performance and foreseeable ethical implications of their technologies. • Corporate Burden of Proof: In any dispute related to data, companies should shoulder the 'burden of proof', i.e. they should demonstrate that the use of data was legitimate and ethical. Technology providers should ensure access to effective redress mechanisms for affected individuals/communities. Accordingly, affected individuals, communities and stakeholders should be provided with access to relevant information sufficient to assure public understanding of the risks, opportunities and impacts of the technology proposed. ● Auditability: Companies should introduce mechanisms (e.g., data logs) that allow flows of personal data to be traceable and auditable. Companies should introduce mechanisms to enable auditability of decision systems over their life cycle.

	Technology providers and any technology developed shall comply with applicable law and should respect human rights by minimizing or mitigating impacts of their technologies on human rights.
4. Accessibility & Openness	Companies should be open about their products, business models and policies, and explain them in clear terms to users. ● Open source: Companies should use existing peer-reviewed open source software, whenever available ● Open standards: Companies should use open standards that collect and process data in a transparent way ● Open APIs: Companies should make any personal information they hold available through open APIs, subject to a strong ID verification mechanisms.
5. Safety & Security	User data should be protected from misuse or disclosure to unauthorized potentially malign third parties. Companies should systematically consider potential unintended harms resulting from the misuse of their products and services. ● Companies should make use of the Ethical OS or similar tools to identify potential risks and harms due to unintended use. Businesses should take a holistic approach to product safety and cyber risk-management that includes available best practices. Technology should be developed, delivered and used in line with the industry's best practices for safety and security. ● Stress testing: Companies should continuously and actively test their software to ensure that safety features are well implemented. ● Simplicity: companies should avoid complex solutions and take the most straightforward path to achieving software solutions. ● The claimed outcomes of the technology should be validated by training and confirmation against scenarios and datasets appropriate to the purpose, risks, stakeholders, and implementation scale. Companies should make efforts to educate users on data security good practices.
6. Data Integrity	The claimed principles, norms and outcomes of the technology should be validated by training and confirmation against scenarios and datasets appropriate to the envisioned purpose, risks stakeholders, and implementation scale.

7. Privacy and Trust	Personal data should be treated with the utmost care, and give customers control and oversight over how their data is collected, stored, and used. The wishes of customers with respect to how personal data is used should be proactively sought and respected. ● Privacy by default. The default settings for choices to should be those that minimize data flows. Any additional data flows should be by opt-in consent. • End-to-end encryption: Companies should encrypt all data stored in the platform (data in place) and transferred (data in transit) on their platform as well as any partner with whom they exchange data. ● Strong authentication: Companies should apply authentication frameworks commensurate with the level and magnitude of risk that would result from the unauthorized access to personal data, services or platforms ● De-identification: Companies should, as far as possible, de-identify personal information they store ● Meaningful choice: As far as possible, access to services should not be contingent on sharing of information.
8. Proportionality	Application of these Principles should be scaled to risks and adverse impacts of the technology, and in the case of early stage technology providers, as appropriate, to their practical capacity.
9. Continuity	Any transfer of the technology, including any licensing or joint venture arrangement, or any change in control of transaction, should be made with due regard for continued application of these Principles.
10. Governance	Technology providers should maintain governance and management systems appropriate to the purpose, scale and potential impacts of the technology, including policies, procedures, business processes and organizational capacity to assure reasonable control over such impacts. Technology providers should seek to avoid, minimize or mitigate potential risks and impacts, including environmental, social, governance and privacy ones.

Draft Framework for VC Toolkit

Stage	Description and Relevant Principles	Tools	Progression Framework (what minimal and maximum performance looks like)	References and Resources
Fund Thesis	In support of the new data economy Based upon risk and opportunity Tied to Principles			https://georgianpartners.com/investment-thesis-areas/trust/ Rebuilding trust in financial services Nathan Kinch ODI Data Ethics Canvas
Sourcing				
Screening		Checklists of principles Questions to ask Questionnaire Document Review Monitoring Tool Quantify Risks and Opportunities		
Diligence		Measurable Indicators Policies Practices Function · Ex: Privacy Mechanisms for informed consent Auditability of data use Data Access Protocols (Tools to Build) · Ex: Fairness Data for Purpose % of data Data balance vs. objectives		https://georgianpartners.com/principles-of-trust/

Term Sheet		· Hiring Cyber Risk Officer · Excluded Applications (Dual Use) · Negotiated contribution from company to improve effort		
Legal Closing				
Board Seat		· Board Diversity · Team Diversity · Data Policy Review · Board Review of Risk o Legal Templates o Good Data Practices o Other templates · Compliance Check · Terms Check · KPIs around Privacy		Accion Data protection template
Monitoring				
Portfolio Review				