THE EMERGING MARKET IN DIGITAL TRUST

NEW OBLIGATIONS AND NEW OPPORTUNITIES FOR VENTURE CAPITAL

Prepared for the Omidyar Network

ON

OMIDYAR NETWORK
A WORLD OF POSITIVE RETURNS

September 10, 2019

Michelle De Mooy, Author
Information Trust Exchange Governing Association
(itega.org)
mdemooy@gmail.com

ITEGA

EXECUTIVE SUMMARY

A valuable new market for investors has opened up around digital trust, identity, privacy and information commerce. Global data protection regulations combined with large scale data breaches and revelations about corporate data misuse have seeded this market and prompted worldwide conversations about the role of technology and technology companies in society.

This report was prepared in conjunction with the Omidyar Network's "Race to the Top" Initiative, which is aimed at helping investors understand the risks and opportunities they face in this market. The report first analyzes trends in the data-driven marketplace, reviewing business models and technologies that have raised concerns and prompted shifts in consumer preferences and public opinion around privacy.

Through a review of relevant case studies, the report next examines successful start-ups with business models that reflect core "Race to the Top" Principles, such as fairness and inclusion, privacy and trust, transparency and accountability, and civic benefit. These companies' extraordinary growth is driven in part by their ability to differentiate themselves as trustworthy and ethical in a crowded and unprincipled marketplace.

The report concludes by arguing that the era of unimpeded use of personal data is likely over, upended in recent years by scandals, regulations, and greater public awareness and education. To become market leaders, companies and investors must embrace a new paradigm of data governance, balancing growth and revenue with gains in user trust and social good.

1. MARKET RISKS FOR DATA-DRIVEN TECHNOLOGIES

Concerns related to data-driven technologies have been raised over the last several years by researchers, advocates, companies, and policymakers. Below is a snapshot of some of these concerns, followed by an in-depth analysis of why these issues have the most potential to reduce the value of investments.

SNAPSHOT

↳Bias and discrimination in automated systems
Bias exists in the data and analysis used in technology systems, causing them to perform differently based on demographics and attributes such as ethnicity or gender. Biased systems reduce the accuracy and effectiveness--and thus the value-- of the data and the systems themselves.

↳Security and data breach
Breaches cost the average U.S. company $3.9 million. Class-action lawsuits, regulatory costs, reputational/brand hits, and loss of intellectual property contribute to the financial gut punch.

↳Privacy violation with resulting regulation costs
Examples of data misuse and privacy violations include broad sharing of personal data without user permission, enabled by easy access to data and microtargeting tools. These violations have led to increased regulation of the industry. Since going into force in May of 2018, the GDPR has resulted in 23 fines, ranging from a fine of €1,400 Euros to €183 million Euros.74 percent of small to mid-sized companies shelled out more than $100,000 (about a third spent up to $499,999) for GDPR compliance while 20 percent spent more than $1 million.

Bias and discrimination in automated systems
Researchers have identified underlying and often unintentional bias in the data and analysis used in technology systems, which causes them to perform differently based on demographics and attributes such as sexual orientation, ethnicity, and gender. Bias in facial-recognition technologies (FRTs), such as those used in Face++, are perhaps the most notorious of these systems, but social bias has been uncovered in a host of products and services, from Uber "surge" pricing to models developed for court systems, parole boards predicting the likelihood of recidivism, and for hiring and lending decisions.

The problem of bias is a profound moral and business problem for the data-driven market. Biased systems not only reinforce long-standing social prejudices, potentially reducing opportunities in the digital economy for already-marginalized communities, they also reduce the overall representation of populations, ultimately undermining the accuracy and effectiveness of the data and the systems themselves. Finding solutions that respect privacy, combat bias and improve transparency has been challenging. Efforts have included new methods for analyzing large datasets without compromising privacy, such as open-source applications of differential privacy; the creation of diverse open-source training datasets; building automated technical tools for detecting bias; and inviting a broad section of users to participate in the creation of automated systems.

Security and data breach

Data breach is now ubiquitous for companies collecting data -- that is, most companies around the globe, including small businesses. The Ponemon Institute's 2019 report on data-breach costs found the typical cost of a breach to a U.S. company to be $3.9 million, with about one-third of that cost being incurred more than a year after the breach. The study also found that it takes most entities an average of 279 days to find and mitigate a breach.

Class-action lawsuits, regulatory costs, reputational/brand hits from the loss of consumer and investor trust, and loss of valuable intellectual property contribute to the overall financial impact of breaches. Fines authorized in the GDPR, the pending California Consumer Privacy Act (CCPA) and New York state's Stop Hacks and Improve Electronic Data Security Act and the Department of Financial Services' Cybersecurity Regulations are examples of hefty financial sanctions for lapses in data security. The sophistication of cyberattacks has raised the stakes for companies and made it more difficult to effectively defend their data stores. As costs and breaches climb, companies are investing in good data governance to reduce their risk of data breach.

Early-stage companies using sophisticated machine learning techniques to identify and reduce cyberattacks are reaching high valuations, such as Sumo Logic, which raised $100 million in funding in July 2019 and is currently valued at $1 billion. The company is part of a new crop of successful cybersecurity startups that are applying AI in the battle against malware and other security vulnerabilities.

Privacy violations with resulting regulatory costs

To a significant extent, GDPR, CCPA and other regulatory efforts are a direct result of data misuse and privacy violations at the hands of the world's largest companies. Facebook tops the list for data missteps, from a parade of large data breaches to the company's questionable forays into surveillance-oriented products and services and the Cambridge Analytica scandal. Privacy lapses have cropped up in services designed to be protective of user data, such as WhatsApp and Apple's Siri, and from industries where the privacy and security of data is subject to regulation, such as payment systems and credit cards. Health apps, which collect and use data most consumers identify as highly sensitive, have come under scrutiny for sharing user data widely and without permission.

The data-driven market has entered a new age of accountability. The enactment of the GDPR fundamentally changed how companies worldwide assess risk and reward with regard to their data holdings. Since going into force in May of 2018, EU Data Protection Authorities have issued 23 fines, ranging from a fine of €1,400 Euros for unlawful data processing by a police officer to €183 million Euros to British Airways for employing bad security practices that allowed for a data breach of 500,000 customers.

Costs to comply with the EU law have not been trivial for the private sector. A 2019 report from DataGrail found that 74 percent of small to mid-sized companies forked over more than $100,000 (about a third spent up to $499,999) for GDPR compliance with 20 percent spending more than $1 million. In the United States, calls for more transparency and responsibility for entities that misuse data have resulted in a crop of new privacy laws in the states, including the broadly scoped CCPA, destined to become a *de facto* national privacy law when it goes into effect in January 2020.

Most concerning for the data-driven industry has been the CCPA's broad definition of personal information, which covers "household" data, provisions broadly defining and restricting the sale of personal information, prohibitions on financial penalties for individuals who exercise their privacy rights, definitional uncertainty around de-identification, pseudonymization, and aggregation, and a limited private right of action for data breaches. A TrustArc survey in 2019 found that companies expect to spend anywhere from hundreds of thousands of dollars to over a million dollars on CCPA compliance - and that the majority of companies surveyed would not be ready when the law goes into effect.

A new generation of privacy-enhancing products and trust-first businesses have arisen to comply with this new regulatory environment. Browsers have created improved privacy defaults, such as Firefox's enhanced tracking protection implemented last year, while user-friendly products like InvizBox's open source privacy routers are gaining momentum with retail customers. A robust market for identity and access management -- estimated to reach $24.12 billion by 2025 -- has also grown as companies seek ways to create more trusted user experiences, secure networks, and adhering to data protection regulations.

2. SOLVING FOR THE RISKS

Innovation is key to the development of an emerging market. In the data economy, innovation around user trust will be necessary to drive growth, as companies rely more heavily on fine-grained personal data to fuel automated targeting and analysis systems, and as they navigate current and future data protection laws.

Trends in consumer attitudes point to key takeaways that can drive innovation.

Trust and privacy

Surveys reveal widespread trepidation among users about data privacy and security. Many believe that companies are not being transparent or responsible with their data, and many believe their data is at risk for breach. This highlights the need for companies that can offer stability and consistency in their data-governance programs. Consumers are more likely to do business with a company that they trust to protect their data and more likely to be loyal to that company over time.

- Consumer trust in businesses overall in the U.S. was down in 2019.
- Seventy-six percent of U.S. consumers said that privacy is a significant or moderate concern for them when interacting with digital brands, while 94 percent said would not do business with a company if they had concerns about their data practices. Sixty-three percent of users described data collection on smart devices as "creepy."
- Fifty-seven percent of global customers are uncomfortable with how companies use their personal or business information, while more than 40 percent of people feel they lack control over their personal data.

- Consumers worldwide also expressed discomfort being targeted online for advertising but said that they would be more willing to give consent for use of their personal data if they trust a brand.
- A 2019 Factual survey found that 53 percent of Gen Z and 51 percent of millenials were either "somewhat" or "very" concerned about data privacy. Individuals surveyed said they were most comfortable sharing personal data with entertainment sites/apps and navigation sites/apps and "utility" sites/apps.

Fear and security

Users have different expectations of privacy in different scenarios, with financial, security-related (passwords) and medical data transactions viewed as the most sensitive. Responsiveness to context and privacy social norms should be an integral part of data-stewardship programs.

- Sixty-two percent of global consumers in a Salesforce survey said they're more afraid of their data being compromised now than they were two years ago. Fifty-nine percent of consumers believe their personal information is vulnerable to a security breach.
- Eighty percent of U.S. consumers in a Deloitte study were more likely to buy products or services from a company believe are protecting their data.
- Seventy eight percent of respondents in a 2018 Ping survey would stop engaging with a brand online if it experienced a data breach and forty nine percent said they would not sign up or use an online service or app that had experienced a breach.

Ethics and social responsibility

Consumers believe that companies have an ethical responsibility to operate in the interest of the social good. Surveys indicate that when individuals are unaware of how a company is using their data, and unable to make a meaningful choice about sharing it, they view the company as ethically bankrupt and therefore untrustworthy. Purpose-driven companies receive more consumer loyalty and emotional connection. A company's ability to convey trust includes offering meaningful transparency, accountability, and ethical policies that communicate how the company's practices impact individuals and society.

- Seventy-eight percent say in a 2018 Cone/Porter/Novelli survey that companies have a responsibility to positively impact society. Seventy-seven percent feel a stronger emotional connection to purpose-driven companies over traditional companies and sixty-six percent would switch from a product they typically buy to a new product from a purpose-driven company.
- Eighty-nine percent of respondents in an IBM survey said technology companies need to be more transparent about their products. In the same IBM survey, 88 percent of consumers said the emergence of technologies like AI increases the need for clear policies about the use of personal data.
- A 2019 RSA survey found that 52 percent of consumers believe data use is ethical when a company only takes the personal information they need to deliver a service and nothing more. In the same survey, forty-eight percent thought that there are ethical ways in which a company can use personal information/data.

- 55 percent of respondents in a 2018 Brooking Institute survey thought companies should hire ethicists while 67 percent thought they should have a code of ethics. 66 percent of those surveyed also thought companies should have an AI review board and 67 percent wanted companies to mediate for AI solutions that inflict harm or damage on people.

3. CASE STUDIES: SUCCESS THROUGH GOOD DATA PRACTICES

New examples of exemplar early-stage companies working in digital trust are emerging quickly. The following includes an overview of the market's sub-sectors, then examines examples of companies that have achieved growth and success through business models that track with core "Race to the Top" Principles," a framework developed for considering the data practices of new and emerging companies in the privacy market. The case studies are first encapsulated in a chart noting the principles the company addresses, then a deeper analysis includes a description of each company, its core products/services, how it addresses the red flags discussed in Chapter 1 of this report, and current funding and valuation estimates.

Market sub-sectors overview

Investments in the digital trust market have tripled since 2013, creating a platform for new businesses born from trends in policy, technology and public opinion including global data protection regulations, improved applications of AI for data analysis, and declining public support for technology companies. With stringent privacy laws coming into force in California and elsewhere in 2020, and the digital trust market is estimated to skyrocket to $158 billion by 2024. Successful firms like OneTrust, BigID, TrustArc and DataGrail offer clients data protection compliance software, ongoing technical support, and policy consulting. The private sector has proven to be thirsty for these privacy-forward business models, with valuations of some reaching the hundreds of millions to unicorn status in 2019.

The trends identified by this report have formed the overall contours of this market, with sub-sectors that are generally geared toward three categories: 1) aiding privacy professionals in their compliance efforts for their organizations; 2) helping organizations institute or update their data governance programs, including compliance with data protection laws and; 3) providing users and publishers with tools to manage digital advertising and establish or revoke consent for data usage. Some companies consolidate all of these offerings in a suite of services. Sub-sectors include:

Privacy managers

These services focus on operationalizing activities specific to a privacy program, such as reporting, auditing, and risk assessments.

Consent managers

These platforms help companies ask for, store, and manage user consents for data collection and sharing in ways that conform with global data protection laws. Consent managers sometimes also offer fulfillment of individual data rights requests, such as requests for access and deletion of accounts.

Data inventory managers
To be compliance with any number of data protection laws, companies need services like data inventory managers to help them classify, map and organize their data holdings. These services offer a bird's eye view of all the data being collected, shared, and stored across an organization.

Data breach identification and reporting
Privacy and security must be intermingled to be effective. Data breach identification is performed by analyzing activity within an organization's system and cataloging current external threats. Reporting services tell company managers when there's been suspicious activity or a breach internally or externally, and flag how and when regulators and users must be informed.

Tracking detection
Traditional uses of cookies and other online trackers have come into conflict with data protection laws. Tracking detection services scan and identify trackers found on the digital properties of publishers and other first parties. Some services also do this kind of assessment for a company's vendors, to avoid liability for vendor non-compliance under GDPR, and help first parties deliver cookie notices.

Access and controls
Organizations have to carefully monitor the entities and individuals that have access to their personal data stores for privacy, security and compliance reasons. These services provide monitoring as well as controls for managing access and report generation.

Privacy-empowered data analytics
These analytics services mine data for value without violating privacy, ethics, security or data protection laws, generally by applying methods for applying de-identification, pseudonymization and anonymization techniques. Some of these services are also beginning to offer tools that mitigate bias in datasets and corporate communications, and help explain the rationale behind outcomes of automated processing so that companies can provide this information to users.

Internal communications
These products and services provide a way for companies to use privacy-aware, secure internal communications channels.

Advertising and media management
This category of products and services covers tools that actively block advertising or provide user tools for managing data sharing and advertising, such as browsers and add-ons. Some services include tools for enterprise clients to measure engagement with content and advertising impact.

RACE TO THE TOP PRINCIPLES

Fairness and Inclusion: Create technology that is fair and non-discriminatory.

Transparency and Accountability: Be transparent about data practices and be accountable to customer expectations.

Accessibility and Openness: Open source, open standards, open APIs.

Safety and Security: Develop technology with strong technical and organizational safeguards and consider harms.

Benefit: Develop technology that benefits customers, individuals and communities, and share the rewards.

Data Integrity: Validate technology against data that is appropriate for intended stakeholders, purposes and risks.

Privacy and Trust: Minimize data and harm through privacy by design, consent, and strong anonymization measures.

Proportionality: Scale principles based on risks, adverse impact of the technology and practical capacity.

Continuity: Apply principles to transfers of technology or changes in transactional control.

Governance: Govern and manage technology through policies that adhere to purpose, scale, risks, and social impact.

NEW COMPANIES AND PRINCIPLES THEY ADDRESS

Company name	Fairness and Inclusion	Transparency and Accountability	Accessibility and Openness	Safety and Security	Civic Benefit	Data Integrity	Privacy and Trust
Text.io	✓						
Kyndi		✓					
Element AI			✓				
Cohesity				✓			
CrowdStrike				✓			
Brave					✓		
Freckle IOT and Killi app					✓		
AnyClip						✓	

BigID							✔
Wickr							✔
DuckDuckGo							✔
OneTrust							✔

Text.io
Text.io helps companies improve diversity by using AI to analyze job postings and provide a“bias” score and language suggestions. The company’s automated language and tone detection uses natural language processing and data mining to identify words and phrases that are statistically likely to attract one type of applicant, such as a man or woman, over another.

Kyndi
Kyndi provides explainable AI solutions. Kyndi’s approach to ethical AI is to create a system that “reads” unstructured data rather than data that is shaped and formed through algorithms created by people, an act that can inadvertently imbue bias and makes outcomes that are nearly impossible to explain.

Element AI
Element AI builds AI-powered enterprise software products. The company has created open-source systems and fostered communities of like-minded developers to build frameworks based on ethics and responsibility.

Cohesity
Cohesity empowers companies to back up, manage, store, and tease out insights from their data and apps. The company helps secure data to stop data breaches.

CrowdStrike
CrowdStrike applies cloud-based analytics and AI to provide a single view of real-time state of security threats, enabling organizations to speed up triage, prioritization and incident response. CrowdStrike’s Threat Graph provides real-time analysis of data from endpoint events across a global crowdsourcing community.

Brave
Brave Software focuses on increasing browsing speed and safety for users, while growing ad revenue share for content creators. Brave browser blocks all trackers and third-party cookies by default and the system allows publishers to get revenue at no cost, just for the content they create.

Freckle IOT and Killi.io
Freckle IOT delivers a privacy-compliant data and independent media measurement for brands and platforms to better understand the impact that their media has on driving a consumer into a location. Killi is an app that allows consumers to download, opt-in and take control of their data from companies that are currently using it and monetizing it.

AnyClip
AnyClip is an AI-based video content data and monetization platform. AnyClip provides metadata for videos in real-time so that videos on social media and other websites are instantly categorizable.AnyClip helps publishers and brands maintain the integrity of their digital environments and their content. When targeting content for users, the company does not collect personal data.

BigID
BigID develops software that helps companies understand and organize data they collect and process to satisfy privacy regulations. Core enterprise products include data inventory and mapping, and automated privacy, security and individual rights management. The company has an app store for privacy, security, and data governance capabilities such as data rights fulfillment, third-party data monitoring, and data risk.

Wickr
Wickr is a secure instant-messaging application and platform offering end-to-end encryption and content-expiring messages. Wickr’s platform allows users to securely share text and files, and use secure audio and video conferencing on mobile and desktop platforms.

Duck-Duck Go
Duck-Duck Go is a privacy-focused search engine that protects users from search leakage by default and reroutes clicks so that websites won’t know the search terms that were used. The company also uses encryption for users and displays encrypted versions of websites in search results. DuckDuckGo only collects anonymous product information and works with affiliate sites that don’t require user personal data.

OneTrust
OneTrust makes a data protection compliance platform that includes features like data mapping and consent management. Its Privacy Management Software, can be cloud-hosted or on-site and manages client data practices, from security and risk management to monitoring data collection and compliance across different jurisdictions (an important value for companies navigating the GDPR and the forthcoming CCPA). OneTrust also has a consent and preferences tool that allows users to determine how their data will be handled (or not) on different sites.

Case studies

P1 FAIRNESS AND INCLUSION
Market risk: Bias and discriminiation in automated systems

Company name: Text.io
Market sub-sector: Privacy-empowered data analytics
Description: Improving diversity in the workforce is a core value at many companies but there aren't a lot of practical tools for implementing it, particularly combating unconscious bias that can creep into the hiring process. Text.io analyzes a company's job postings, as they are being written or edited and before they are posted, using artificial intelligence. The scan highlights particular words that could help or hinder a search for diverse candidates, makes suggestions for edits, and provides a "bias" score.
How the company addresses market risk: Text.io tackles the problem of unconscious bias in the hiring process by feeding its predictive engine data from job postings around the world and comparing it with real-world hiring outcomes. The company's automated language and tone detection uses natural language processing and data mining to identify words and phrases that are statistically likely to attract one type of applicant, such as a man rather than a woman. The company released Text.io Flow in April 2019, a product that assists in writing effective text (i.e. emails) through automated suggestions.
Funding: Text.io raised nearly $30 million since its founding in 2014 from investors such as Bloomberg Beta, Scale Venture Partners and Emergence Capital. Its customers include Cisco, IBM, Twitter, McDonald's, Dropbox and CVS.
Current valuation: $115 million

P2 TRANSPARENCY AND ACCOUNTABILITY
Market risk: Bias and discriminiation in automated systems

Company name: Kyndi
Market sub-sector: Privacy-empowered data analytics
Description: Kyndi provides explainable AI solutions for clients including those in the U.S. government, and in finance, healthcare, IT, and infrastructure.
How the company addresses market risk: Kyndi's approach to ethical AI is to create a system that "reads" unstructured data rather than one that spits out results of algorithms created by people, which can inadvertently imbue bias and makes outcomes that are nearly impossible to explain. An AI system that "reads" presents outputs, as opposed to a system that amplifies human inputs without meaningful transparency into how it arrives at conclusions. This allows companies to evaluate whether their ethics and values align with the outputs and determine how to proceed, and to communicate and explain the results of AI decision-making to users.
Funding: Kyndi received $20 million in Series B funding in July of 2019 from Intel Capital, UL Ventures, PivotNorth Capital, and other investors.
Current valuation: $30 million

P3 ACCESSIBILITY AND OPENNESS
Market risk: Privacy violation with resulting regulation costs

Company name: Element AI
Market sub-sector: Privacy-empowered data analytics
Description: Element AI builds AI-powered enterprise software products.
How the company addresses market risk: Element AI has created open-source systems and fostered communities of like-minded developers to build frameworks based on ethics and responsibility. Their products target enterprise decision-making but the company also makes AI that work for people across several industries. Information gleaned through Element AI's tools are shared across tools and industries by the company, so that systems made for an insurance underwriter to automate document processing, for example, can be used for banks processing loans or in other industries. The company exercises data minimization techniques in its AI, using "small data" to make products through the use of synthetic data.
Funding: Element AI has raised $107 million in funding from investors Data Collective, Intel Capital, Microsoft Ventures, and Tencent Holdings. In 2019, the Candian Government invested $5 million in the company.
Current valuation: $1 billion

P4 SAFETY AND SECURITY
Market risk: Data breach, Privacy violation with resulting regulation costs

Company name: Cohesity
Market sub-sectors: Data inventory managers, Data breach identification and reporting
Description: Cohesity empowers companies to back up, manage, store, and tease out insights from their data and apps. Cohesity's Anti-Ransomware Solution works to prevent, detect, and respond to ransomware attacks, among the biggest security threats companies face today. In March 2019, Cohesity launched an application marketplace for its secondary storage systems that offer a way to run third-party apps on storage devices themselves.
How the company addresses market risk: Cohesity helps companies implement secure data governance programs that are effective at stopping data breaches. The app marketplace the company launched in 2019 created a secure platform for data stores, so that apps are brought to data rather than the other way around.
Funding: Cohesity has raised more than $400 million from investors such as Sequoia Capital, and Cisco Investments, including a Series D round of $250 million from SoftBank Vision Fund.
Current valuation: $1 billion

Company name: CrowdStrike
Market sub-sector: Data breach identification and reporting
Description: CrowdStrike applies cloud-based analytics and AI to identify real-time threats, enabling organizations to speed up triage, prioritization and incident response. The company's Falcon platform detects attacks and provides five-second visibility across all current and past endpoint activity. CrowdStrike's Threat Graph provides real-time analysis of data from endpoint events across the global crowdsourcing community, allowing detection and prevention of attacks based on patented behavioral pattern recognition technology.

How the company addresses market risk: The company's Threat Graph data model - similar to the graph models developed by Google and Facebook - collects and analyzes large volumes of security-related data and gives companies easy-to-use tools to quickly mitigate threats and deploy security responses.
Funding: CrowdStrike received $481 million in funding over six rounds, the last being a Series E round in July of 2018, from Accel, General Atlantic and IVP (Institutional Venture Partners).
Current valuation: After it's IPO in June 2019, between $6.6 billion and $6.8 billion

P5 BENEFIT
Market risk: Privacy violation with resulting regulation costs

Company name: Brave
Market sub-sectors: Advertising and media management, Tracking detection
Description: Brave Software focuses on increasing browsing speed and safety for users, while growing ad revenue share for content creators. Brave's browser blocks invasive tracking and targeting advertising and rewards users with Basic Attention Tokens (BAT) for choosing to view advertising and allows them to anonymously donate tokens to publishers to pay for content. Built using Chromium open-source code, Brave recently rolled out early-stage cryptocurrency wallets for Ethereum tokens and for BATs.
How the company addresses market risk: The Brave browser blocks all trackers and third-party cookies by default, and users can easily control what they want to block and what they don't, whether it's cookies or social media logins. The BAT-based micropayments system allows publishers - like news outlets - to regain revenue for content they create.
Funding: Brave has raised a total of $42 million in funding since 2015, with $35 million coming during its Initial Coin Offering in July 2017. Investors include Digital Finance Group and Foundation Capital.
Current valuation: $133 million

Company name: Freckle IOT and mobile app Killi.io
Market sub-sector: Advertising and media management
Description: Freckle IOT delivers privacy-compliant data and independent media measurement for brands and platforms. Killi is an app that allows consumers to download, opt-in and control data that companies are using and monetizing. Killi allows consumers to sell their data (passively or via surveys) and receive cash payments.
How the company addresses market risk: Freckle applies privacy-forward techniques to gather real-time first-party data while complying with GDPR and other privacy standards. Its mobile app, Killi, was developed to give consumers a way to trade personal information with brands in exchange for compensation. To do this, Killi enables smart contracts between users and brands who are looking to purchase user data. The app allows users to delete their data at any time and only shares and sells permissioned user data. The company also embraces 'purpose specification," or only collecting data needed, by creating a loop so that the more data customers share, they more money they earn.
Funding: $514 million in two rounds of funding from private investors, with the most recent investment of $91,000 occurring in 2018.
Current valuation: $514 million

P6 DATA INTEGRITY
Market risk: Privacy violation with resulting regulation costs

Company name: AnyClip
Sub-sector: Advertising and media management
Description: AnyClip is an AI-based video content data and monetization platform. AnyClip's Luminous AI analysis tool helps publishers, content owners and brands to analyze the contents of a video clip, frame by frame. When used as targeting criteria in advertising campaigns, this analysis helps brands to avoid aligning with "unsafe" video content and reach audiences that are consuming more relevant video content.
How the company addresses market risk: AnyClip gives publishers and brands tools to avoid posting fraudulent video content by analyzing metadata for videos in real-time. This method also provides a way for companies to better categorize their datasets and narrow their content targeting, reducing database disorganization and the amount of data collected and stored overall.
Funding: AnyClip has raised $24 million in funding from Limelight Networks, Jerusalem Venture Partners, GTI Capital, and other investors.
Current valuation: Between $84 - $126 million

P7 PRIVACY AND TRUST
Market risk: Privacy violation with resulting regulation costs

Company name: BigID
Market sub-sectors: Privacy management, Consent management, Data inventory management, Tracking detection
Description: BigID develops software that helps companies understand and organize data they collect and process to satisfy privacy regulations. Core enterprise products include data inventory and mapping, and automated privacy, security and individual rights management.
How the company addresses market risk: BigID’s AI tools enable companies to comply with global data privacy regulations such as the GDPR. Most recently, the company launched an app to augment privacy, security, and data governance capabilities including data rights fulfillment, third-party data monitoring, consent management, and data risk.
Funding: BigID has raised a total of $96.1M in funding over 5 rounds. In September 2019, the company raised $50 million in Series C through Bessemer Venture Partners, SAP.io Fund, Comcast Ventures, and Salesforce Ventures are the most recent investors.
Current valuation: Between $100 - $500 million

Company name: Wickr
Market sub-sector: Internal communications management
Description: Wickr is a secure instant-messaging application and platform offering end-to-end encryption and content-expiring messages.
How the company addresses market risk: Wickr’s platform allows users to securely share text and files, as well as hold secure audio and video conferencing on mobile and desktop platforms. Both sender and receiver must have the app to communicate and only the receiver is able to decrypt messages once they are sent. The company does not hold any decryption keys.

Funding: Wickr has raised $73 million in funding from Singtel Innov8, Wargaming, and others.
Current valuation: Between $136 million - $204 million

Company name: Duck-Duck Go
Market sub-sector: Advertising and media management
Description: Duck-Duck Go is a privacy-focused search engine. The company also does education-based campaigns concerning the privacy of search engines and the company has developed a privacy app that blocks scripts from tracking visitors.
How the company addresses market risk: DuckDuckGo protects users from search data leakage by default and reroutes clicks so that websites won't see user search terms. The company also uses encryption for users and displays encrypted versions of websites in search results. DuckDuckGo only collects anonymous product information and works with affiliate sites that don't require user personal data. DuckDuckGo gives users the option of using POST requests as well, which stop data leaks by preventing user searches from appearing in the browser.
Funding: Profitable since 2014, DuckDuckGo hit 40 million searches per day in May 2019 and has been growing at an annualized 60% a year in search volume for the past ten years. Duck-Duck Go raised $10 million from OMERS Ventures in 2018.
Current valuation: $160 million

Company name: OneTrust
Market sub-sectors: Privacy management, Consent management, Tracking detection
Description: OneTrust offers companies a data protection compliance platform that includes features like data mapping and consent management. It plans to expand its products to vendor management and verification.
How the company addresses market risk: The company's core product is its Privacy Management Software, which can cloud or on-site hosted. The product manages data practices, from security and risk management to monitoring data collection and compliance across different jurisdictions. OneTrust also has a consent and preferences tool that allows users to determine how their data will be handled (or not) on different sites.
Funding: OneTrust attained unicorn status in July 2019 after a Series A of $200 million from Insight Partners.
Current Valuation: $1.3 billion

4. CONCLUSION

The era of unimpeded use of personal data is over, upended in recent years by scandals, regulations, and greater public awareness and education. As the public learns more about the commercial value assigned to their data, and the ways data can be used to benefit or harm them and society at large, they have begun to demand more accountability and seek a return of this value. Investors should see these shifts as a call to innovation in an industry known best for its disruptiveness and ingenuity.

To navigate these market changes, and future-proof their investments, investors need tools that:

- Measure how data practices impact the bottom line for companies, both positively and negatively.

- Develop measurements evaluating how practices improve or weaken consumer trust and social benefit.
- Support early stage companies that use strong privacy and identity practices and help position them as market leaders.
- Create a framework for accountability and transparency around data practices that will ultimately shape the market.

The downward slide in global attitudes about data-drive technologies, and forthcoming data protection regulations, support the value of this emerging market in digital trust. As this report makes clear, and the case studies detail, companies that build a foundation of ethical values that inform compliance activities, product design and key decision-making can successfully generate revenue, grow consumer trust, and foster social good; they are poised to or already have become market leaders. Companies that, on the other hand, consume data blindly without regard for these seismic shifts in the market and in consumer attitudes, have greater risk of rising costs, reduced returns, and declining user confidence. When imbued into products and viewed through the lens of shared values, concepts like ethics and privacy are incubators for innovation and sustainability.