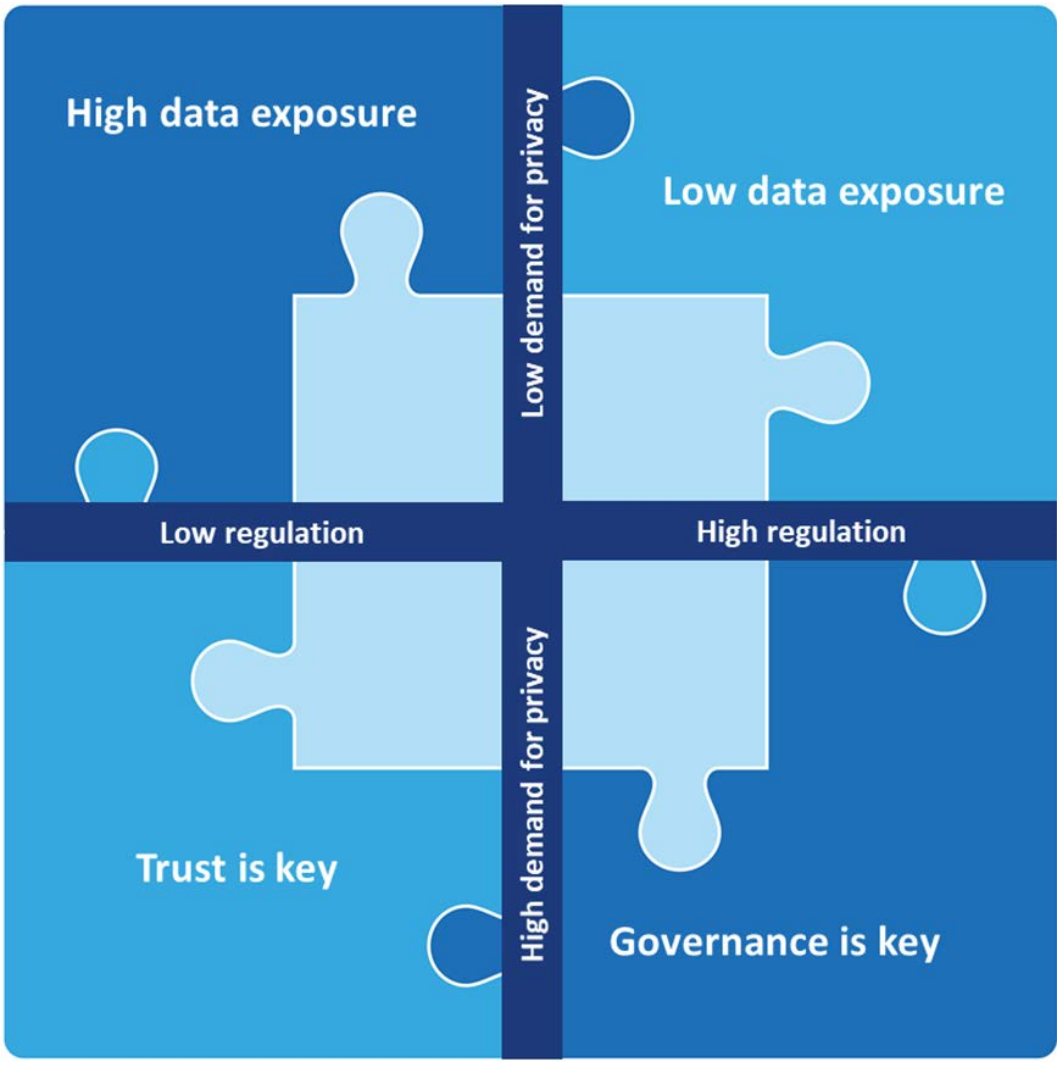
Cornerstone CAPITAL GROUP

Radically Practical Investing™

IRRC Institute

The Data Privacy Puzzle

Companies gather enormous – and growing – amounts of personal data every day. What happens if consumer attitudes or regulations change?



Prepared by Cornerstone Capital Group for the Investor Responsibility Research Center Institute

Authors:

John Wilson *Head of Research and Corporate Governance*

Heidi Bush, CFA *Director, Global Thematic Research*

August 2018

Please see important disclosures at the end of this report

Cornerstone CAPITAL GROUP

IRRC Institute

Table of Contents

Introduction 4

What is data privacy? 6

What trends are relevant to investors? 8

- Technological: an accelerating trend 9
- Behavioral: a conflicting trend 12
- Regulatory: Divergent trends 18
- Bringing it together: increasing uncertainty 21

Future scenarios: risks and opportunities 22

- A stakeholder map 22
- Four potential operating environments 24

Data dependency and business models 28

- Exposure 28
- Consumer and Employee Trust 40
- Conclusions: trust and exposure 43

Data privacy and investment: How can investors take direct action? 46

1. Corporate governance and engagement 46
2. Investing in Data Privacy Protection 48

Introduction

Who owns consumer data? Do consumers trust companies with their data? Will consumers embrace new technologies that reveal more information about them to companies? Are companies ready to respond to changing attitudes about consumer data?

These are core questions that investors need to consider about *data privacy*, the option to shield our personal data from public view or corporate use and sale. Currently, companies have largely unfettered access to the data they gather about consumers, even as technologies make it possible to know more about consumers' online (and offline) activities. By some estimates, the number of devices connected to the internet will rise from 8 billion today to 100 billion by 2030. As devices proliferate and data-mining tools become more sophisticated, companies have increasing access to information such as our physiological traits, personal habits, location, political beliefs, lifestyle habits and purchasing behavior.

Such data may give rise to products and services that we can only imagine at present. But these potential advances come at the cost of diminished consumer privacy and the risk that our data will be used for purposes society may neither intend nor desire, such as discrimination, employee surveillance, social engineering, or unfair political influence.

Both consumer attitudes and the regulatory environment reflect deep ambivalence about the role of data in the modern economy

Both consumer attitudes and the regulatory environment reflect deep ambivalence about the role of data in the modern economy. Studies show that many consumers do not support collection of their data, but feel powerless to prevent it. Although data flows globally, the regulations that govern it are regional and inconsistent: e.g., new EU regulations strengthen consumers' control over the use of their personal data, while the US regulatory environment remains permissive.

Even as society struggles with the tradeoff between innovation and control, investors have demonstrated a keen interest in companies with strategies to monetize this growing pool of data. Companies have always sought competitive advantage through better information. The accelerating supply of personal data has raised the importance of data access and analytics to corporate performance, which in turns drives demand for even more data. At the center of this trend are the FANG[1] stocks, for whom data does not merely support their business model but lies at the core of their strategy. Most of The FANG companies did not exist 20 years ago, but now make up nearly 15% of the S&P 500, having been favored by investors in the form of valuations far outstripping the rest of the index.

Companies whose business models rely on increasing quantity and scope of consumer data are at risk if public ambivalence turns to opposition

We believe that the ambiguity of the current circumstances is unsustainable. While the exact future of data privacy is not possible to predict with confidence, investors should be concerned that companies whose business models rely on increasing quantity and scope of consumer data are at risk if the public ambivalence turns to opposition.

[1] Facebook, Amazon, Netflix, Alphabet (formerly Google).

To better understand that risk, we consider four potential operating environments that companies may face:

1. **Low demand for privacy, low regulation:** Consumer acceptance of data collection and use grows, and regulators prioritize the free flow of information over privacy. Technological innovation grows quickly, but the risk of unintended negative social consequences, such as discrimination, rises. In this scenario, companies that have high exposure to data would be best positioned to take advantage of the opportunities.

2. **Low demand for privacy, high regulation:** Overreaching regulations lead to dissatisfaction among companies and consumers, as market demands go unmet. Trust is difficult to obtain because the system lacks legitimacy. Companies with low exposure to data issues will avoid the regulatory risks associated with this scenario. New entrants will struggle to grow while managing compliance costs.

3. **High demand for privacy, low regulation:** Regulators fail to effectively respond to consumer concerns about data privacy. Technological innovation accelerates, as does the risk of unintended consequences. Lack of trust in the system creates challenges for new companies and products to gain acceptance, and consumers may take steps to restrict access to data on an individual basis. Companies that achieve high trust of employees and consumers are best positioned to navigate the instability of this scenario. In this scenario, new business models may emerge to help consumers protect their own privacy. [2]

4. **High demand for privacy, high regulation:** Regulators restrict data gathering in response to consumer privacy concerns. Technological progress slows, but the system creates a high degree of trust that enables new companies and new technologies to achieve consumer acceptance with relative ease. Unintended consequences are kept to a minimum. Because no one positioning dominates this scenario, individual company management and governance to establish trust and engagement will take on particular importance.

We look at the implications of different operating environments on eight companies:

- Alphabet
- Amazon
- American Express
- AT&T
- Facebook
- MasterCard
- Twitter
- Wal-Mart

This report:

- Defines the issue of data privacy;
- Identifies key regulatory, technological and behavioral trends that will drive societal response to concerns about data privacy;
- Outlines four possible scenarios for the impact of data privacy concerns on companies;
- Examines the potential implications of uncertainties about data privacy on eight case-study companies whose business models may involve the gathering, use and possible sharing of data; and
- Concludes with a general framework for investors to monitor the impact of evolving attitudes toward data privacy on companies, plus an overview of emerging data-privacy solutions.

[2] See "Data Privacy and Investment: Investing in Privacy Protection" later in this report

What is data privacy?

Data are facts and statistics. This report considers the personal data people may create when they go online or use electronic devices that incorporate data-gathering technology. These activities create a rich pool of data about people and their activities that companies gather, collect and analyze. A study and consumer survey of 900 people in five countries, published in the May 2015 issue of the Harvard Business Review, describes three kinds of data relevant for this analysis: [3]

- *Self-reported data* are volunteered, such as when one enters an email address into a form;
- *Digital exhaust* includes the results of online activity, such as web-browsing history;
- *Profiling data* are an aggregation of other data used to predict a person's behavior, interests, or characteristics. For example, social media analysts can make reasonably accurate estimations about an individual's race, gender, income and political leanings by examining what articles the user "likes" on social media.

Mass collection of individuals' data enables many useful and entertaining services and benefits, but it may also raise concerns:

- Some types of data are sensitive, as in the cases of social security numbers and health or financial information.
- Data collection may also be *passive*, taken without the users' participation or sometimes their awareness, even if the device is not in use. An example currently in widespread use is location data created by tracking the position and movement of cellular phones, which makes possible traffic information found in Waze and other mapping apps. Collection of passive data raises concerns about the control people have over their personal information.
- Sensors and "smart" devices are increasingly monitoring people's daily lives in addition to their online activities, potentially eroding their sense of privacy.

The core issue underlying debates about data privacy is who owns the data: the individual who generated it or the company that collected it?

An overriding concern is that users have little understanding of who will gain access to this information, how it will be used, and who will benefit.

Data privacy is the ability of individuals to control what personal data are collected, who may access the data, and under what conditions. The core question underlying debates about data privacy is, who owns the data: the individual who generated it or the company that collected it?

[3] https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Current examples of measures intended to protect data privacy include:

- The option to shield data from collection built into websites and devices, such as through "private" web browsing;
- The ability to restrict who may gain access to data, for example by prohibiting the sale of data to third parties;
- The blocking of monitoring by sensors or other "passive" data gathering systems, or
- "The right to be forgotten;" the ability of users to compel search engine companies to omit old or obsolete information, especially if this information is inaccurate, from search requests.

Despite efforts to protect personal data, the amount of data being collected, disseminated and analyzed continues to grow at an exponential rate, and the use of data is increasing in both volume and in scope.

A related but separate issue is *data security*, or cybersecurity, which is the protection of collected data from unauthorized or inappropriate uses. For purposes of this report, "data privacy" applies to the use of data in ways that are lawful and with the implicit or explicit consent of the individuals that generate the data. The separate issue of *data security* is beyond the scope of this report. However, the increased ability of companies to collect massive amounts of personal data increases the potential impact of a data security breach. In effect, data privacy status strongly influences how valuable is a cache of information to an unauthorized user.

What trends are relevant to investors?

We explore each trend in more detail with the goal of providing investors further insight into the potential evolution of data privacy as an investment issue

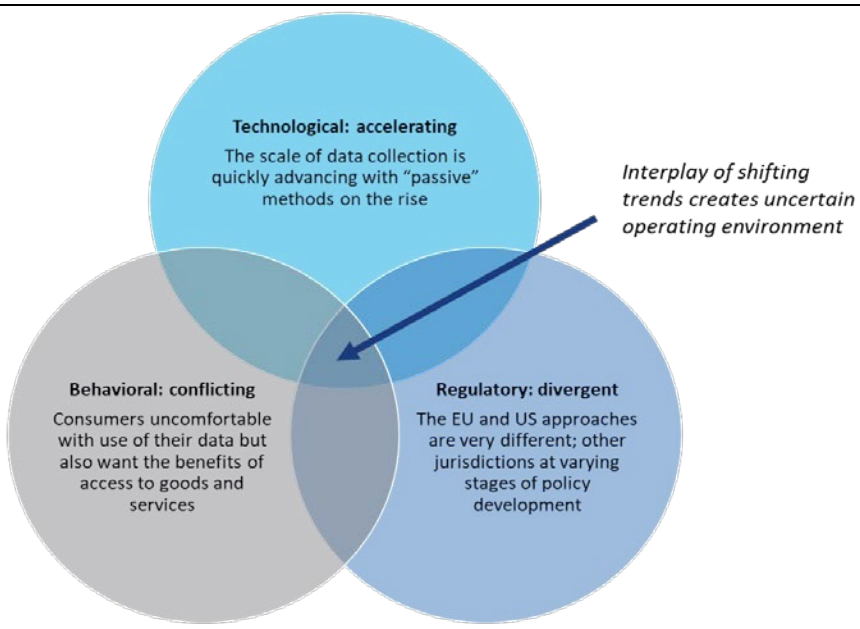
Companies have faced few barriers to gathering and employing user data for business purposes. If society, through regulation or consumer resistance, eventually places limits on corporate access to data, the growth expectations of data-driven companies could be severely impacted.

Several emerging trends are raising the issue of data privacy as a strategic and operational concern for companies and investors in the medium term. Our framework categorizes each trend into one of three factors:

- **Technological:** Technological development is increasing the volume of data being gathered and the capability of companies to analyze the data for useful purposes.
- **Behavioral:** Consumers freely use services they know (or should know) are gathering their data but feel ambivalent about doing so.
- **Regulatory:** Regulatory regimes currently are adopting diverse approaches to data privacy, with the EU adopting a consumer rights approach that limits the use of data, while the US has a more permissive set of rules that facilitates the free flow of data.

How these trends intersect is likely to have broad implications for both consumers and companies. However, the conflicting nature of behavioral and regulatory trends makes definitive predictions questionable. We explore each trend in more detail with the goal of providing investors further insight into the potential evolution of data privacy as an investment issue.

Figure 1: Intersecting trends in data proliferation and management



Source: Cornerstone Capital Group
Note: passive technology collection encompasses sensors, the "internet of thing" (IoT), and artificial intelligence products, such as Amazon's Alexa, that constantly monitor consumers through face and voice recognition.

Technological: an accelerating trend

The data explosion has been under way for many years. According to a report by Seagate and IDC, the "Digital Universe" (i.e., all the data in the world) grew from 0.13 zettabytes in 2005 to 16 zettabytes[4] (1 trillion gigabytes) in 2016, a 12,300% increase.[5] The report predicts that the digital universe will grow to 163 zettabytes by 2025, or another 1000% increase.

Moreover, a larger amount of this expanded digital universe will be important to people's lives. The report forecasts a rise in percentage of data that is *critical* — important to the continuity of people's daily lives — from 10-20%, and a larger increase, from 2-10%, in the proportion that is *hyper-critical*, or having immediate impact on health and well-being .[6] Finally, users' interactions with connected devices and applications will increase exponentially, from fewer than 100 per day in 2010 to nearly 5000 in 2025[7]. Many of these interactions will be invisible to users.

This trend is made possible by three overlapping technological developments:

1. The Internet of Things,
2. Machine Learning, and
3. Sensors & Smart Environments

Figure 2: Total amount of global data

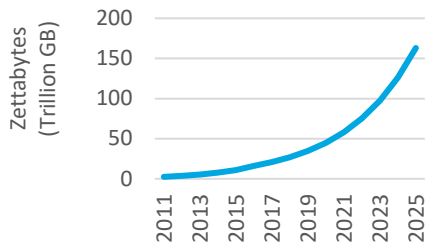


Figure 3: Interactions per connected person, per day

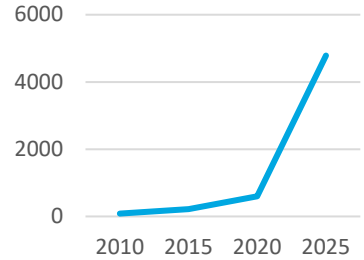
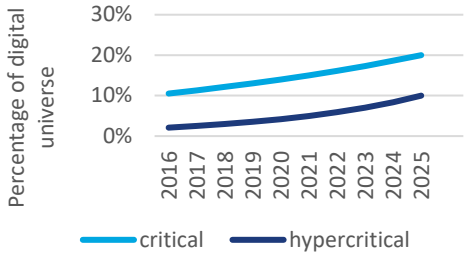


Figure 4: The growing importance of data



Source: Seagate/IDC; Cornerstone Capital

There are about 8 billion connected devices now; there will be tens of billions of connected devices by 2020 and over 100b by 2030

The Internet of Things

The internet allows people to share information with others instantaneously across great distances. The Internet of Things (IoT) enables inanimate objects to communicate in the same way. For example, mapping apps use the IoT to identify traffic jams by monitoring how fast GPS-connected smartphones are moving along a stretch of road; medical devices monitor patient compliance with prescribed use of the device and communicate results to healthcare providers.

Every interaction creates some data, and the amount of data produced will grow with the number of functioning devices and their increasing sophistication. Although estimates vary, there are

[4] https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf
[5] https://www.emc.com/collateral/about/news/idc-emc-digital-universe-2011-infographic.pdf
[6] https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf
[7] IBID

about eight billion connected devices now; the consensus is that there will be tens of billions of connected devices by 2020 and over 100 billion by 2030[8]. Because of network effects, the number of connected devices implies exponential growth in the amount of data, covering every aspect of home and work life, on- and off-line.

Machine learning and Artificial Intelligence

Artificial Intelligence (AI) is how computers solve problems and carry out tasks for which they were not specifically programmed. The goal of AI is to create computers that can determine for themselves the best way to achieve their objectives.

From a stream to a flood of data

These technologies will accelerate the flow of data. First, they will create greater demand for data, since their usefulness improves as data availability grows. Second, they will increase the supply of data. Moreover, sensors, IoT, Machine learning and smart environments will change the nature of available data:

- More of the available data will be gained through *passive* means – without the participation or sometimes the awareness of the individual being monitored;
- Sensors will increase the gathering of data in the *physical, off-line* world, rather than the online world characteristic of most data being captured today; and
- Machine learning will use the increased volume of data to conduct more and more accurate *profiling* of users, inferring the likely behavior or characteristics of a person from available data about them.

Today, the state of the art in AI involves "machine learning." Traditionally, computers completed tasks by following specific and detailed rules and instructions that were programmed in by humans. With machine learning, computers learn to recognize patterns in large amounts of data with no (or minimal) rules or instructions. A computer can learn to recognize dogs simply by viewing hundreds or thousands of pictures of dogs, without having been fed any information about what a dog is.

Machine learning is a tool to allow computers to perform tasks too complicated for humans to create instructions for, such as recognizing voices, faces and facial expressions, identifying musical styles, and learning different languages. Machine learning began in the 1950s, but only recently has the growth in computing performance and available data enabled machine learning to achieve broad scientific and commercial use. [9]

For instance, Amazon's digital assistant Alexa uses machine learning to understand human speech and provide recommendations for individual users. Amazon is expanding Alexa's uses and launching a version of the tool for businesses[10], which will both increase Amazon's access to data and improve the digital assistant's performance. The accuracy of artificial intelligence is directly related to the amount of relevant data available to analyze. As artificial intelligence improves, users are more likely to increase dependence on it, thereby creating more data, in an ever-expanding spiral of data creation.

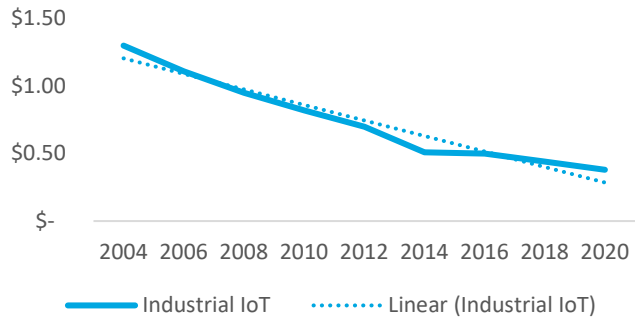
[8] http://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11; https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says; https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/
[9] http://www.mlplatform.nl/what-is-machine-learning/
[10] https://www.technologyreview.com/the-download/610503/amazon-wants-to-put-alexa-in-the-workplace/

Sensors And Smart Environments

Combining machine learning, the IoT, and sensors — devices that monitor events and changes in the physical environment — makes it possible to transform homes, offices, stores and transportation into s*mart environments*. Smart environments use digital technology to automate certain repetitive functions and allow individuals more control over the environment. Ongoing declines in sensor costs allows increasing scope and scale of smart environment applications.

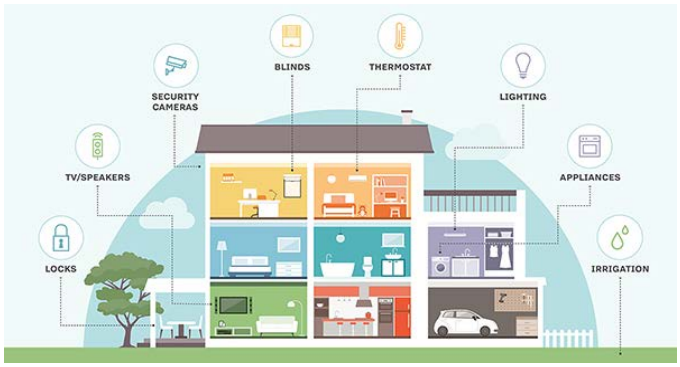
Smart homes already manage temperature levels for maximum comfort and energy efficiency. In future, smart environments at in-patient health care facilities will improve patient monitoring and treatment, for example by adjusting the patient's diet automatically according to their health needs. In industrial settings, smart technology will provide a continuous stream of data to managers to coordinate operations across the supply chain efficiently and safely. Smart stores track what a customer purchases and associates it with a debit account, without any checkout procedure. Smart mobility, in the form of shared, autonomous vehicles, has the potential to transform not just how people travel, but also how they work and where they live.

Figure 5: Cost of IoT sensors



Source: IoTOne, 2016; Cornerstone Capital Group

Figure 6: Smart home diagrams

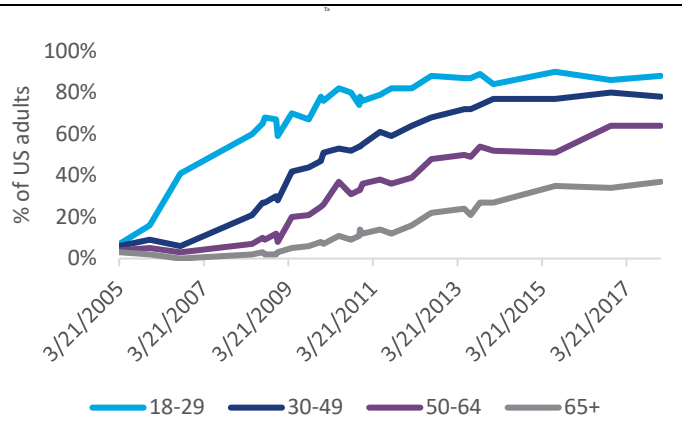


Source: IoTAgenda

Behavioral: a conflicting trend

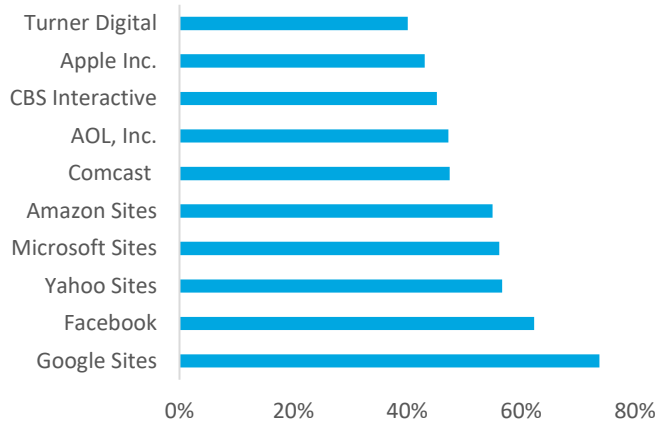
Currently, consumers generally acquiesce to the collection of their data, but studies indicate a discomfort with the practice and a concern about data privacy.

Figure 7: % of US adults using at least one social media site



Source: Pew Research Center; Cornerstone Capital Group

Figure 8: Unique monthly views as % of US population



Source: comScore; Cornerstone Capital Group

DATA SHARING

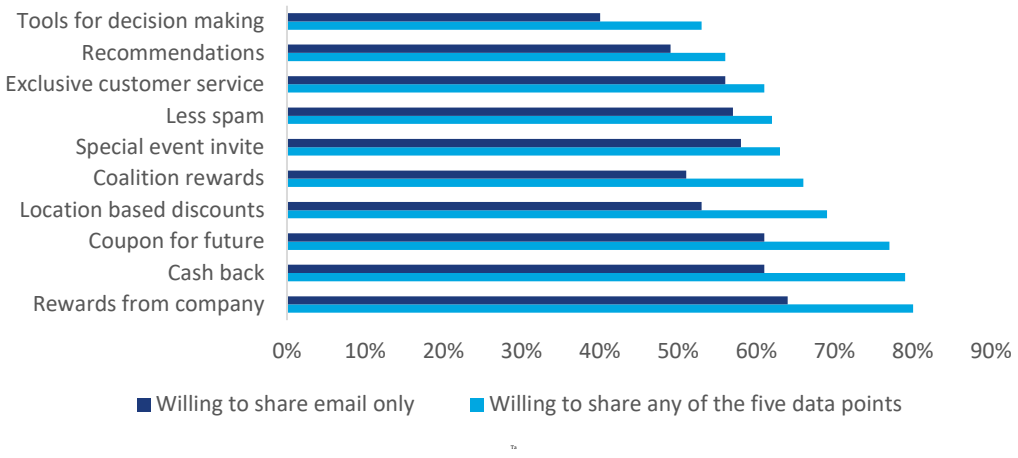
Companies collect data from consumers primarily by providing discounts in exchange for information and through free services such as search engines, social media, maps and other tools. Use of such services has grown rapidly in the past ten years and is now pervasive among adults in the United States.

Consumers generally indicate a willingness to share information in exchange for a product or service they value

Consumers generally indicate a willingness to share information in exchange for these services. A Columbia University study found that 75% of consumers would provide sensitive information (address, mobile phone number and date of birth) in exchange for a product or service they value from a brand they trust. Even more consumers (80%) would agree to share personal data with companies when they receive special offers or data-enabled benefits. These included reward points and product recommendations[11].

[11] https://www8.gsb.columbia.edu/globalbrands/sites/globalbrands/files/images/The_Future_of_Data_Sharing_Columbia-Aimia_October_2015.pdf

Figure 9: Sharing data for rewards



Source: CBS, AIMIA, 2015; Cornerstone Capital Group

PRIVACY CONCERNS

However, at the same time, consumers are becoming more concerned about data privacy. A 2016 survey on data privacy by the Pew Center[12] found that:

- 74% of respondents regarded it as very important that they control who can get information about them;
- 47% were not confident they understood how their information would be used;
- 92% of adults agreed or strongly agreed that consumers have lost control of how personal information is collected and used by companies;
- 68% of internet users believed current laws are not good enough at protecting people's privacy online; and
- 64% believed the government should do more to regulate advertisers' use of data.

"RESIGNATION"

A 2015 Annenberg School for Communication study found that consumers express concern over data privacy and the control that companies have over their personal information.[13] The study references several surveys indicating that a large majority of consumers do not consider many industry data collection practices to be "fair" or "okay."

[12] http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/
[13] https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Typically, the industry explains this paradox by suggesting that consumers consider the benefits they receive to be worth giving up data. Some industry critics claim that consumers lack enough knowledge and awareness of industry practices to make such an informed choice. For example, an earlier Annenberg study found that 78% of respondents incorrectly believed that if a company had a privacy policy, it meant that the company would not collect user data.

User resignation

Most users do not gladly trade their data for novel and useful services. Instead, many feel resigned to the collection of their data by corporations because they feel powerless to prevent it. Their objections increase as data plumbs deeper into their personal lives and characteristics, and when companies monetize data rather than using it to improve services.

Technology companies depend on the relatively high degree of consumer trust in them to "do what is right." This trust may help to explain why users have not acted on their objections to data collection. The recent trend toward declining trust may bring about resistance to the collection and use of data.

The 2015 Annenberg study concludes instead that many consumers allow data collection because they feel that they have no other choice — that they are *resigned* to sharing their data because they perceive a lack of power and agency in the marketplace. They would prefer not to share data but believe that refusing to do so would result in unacceptable costs — paying higher prices, missing contact with friends on social media, and losing access to services that feel necessary in modern society.

Evidence of consumer skepticism about the value of exchanging data for services continues to mount. A June 2018 survey by Edelman (*Trust Barometer Special Report: Brands and Social Media)*[14] found that by a 49% to 32% margin, consumers were unwilling to trade data privacy for a more personalized shopping experience. A May Morning Consult survey found that 63% of respondents would not be willing to give up their personal data for targeted ads to use an online service for free, compared to 23% who were willing.[15]

The risk for companies is that resignation evolves into active opposition or that new corporate entrants design products and services which tap into that latent discomfort and either actively block such data or figure out how to pay consumers for providing it, thereby intermediating what has, to this point, been the widespread provision of "free" data.

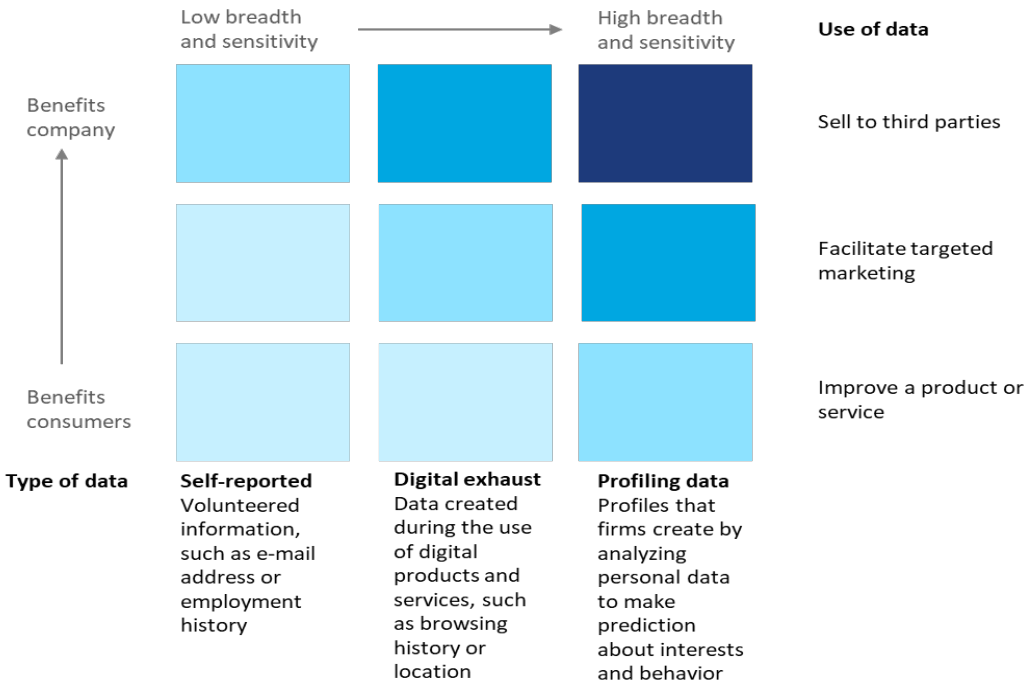
Consumer acceptance of data sharing may also depend on the nature of the data and how companies use it. A study and consumer survey of 900 people in five countries, published in the May 2015 issue of the Harvard Business Review,[16] provides a useful taxonomy of personal data and consumer value, shown in Figure 10.

Consumers are most concerned about sharing of data leading to the creation of behavioral profiles

Contrary to expectations, the survey did not find much concern about sharing *sensitive* information, such as social security numbers. Instead, the study found greatest concern around the sharing of data leading to the creation of *profiles* of likely consumer behavior and interests, less concern about *digital exhaust* (the tracking of online activities), and the least about *self-reported* (volunteered) information.

[14] https://www.edelman.com/trust-barometer-brands-social-media
[15] https://morningconsult.com/2018/05/25/most-us-adults-unwilling-share-personal-data-ads-keep-service-free/
[16] https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Figure 10: Taxonomy of data and consumer perceptions



Source: Morey et al, 'Customer Data: Designing for Transparency and Trust', HBR — May 2015
Note: Profiling analyzes data that is self-reported and data from digital exhaust to predict behavioral patterns.

Consumers, not surprisingly, were more willing to share data when they perceived benefits from doing so, and least when the data could be shared with third parties. Separately, the June 2018 Edelman *Brands and Social Media Report* found that 71% of respondents had an unfavorable view of companies selling data to third parties, and 39% believed the practice should be made illegal.

The Morey study did not look at passive data collection made possible by sensors and machine learning. However, the taxonomy suggests that consumers may have substantial concern about these practices, because they are an even more intensive version of the digital exhaust and profiling data that raises concern when gathered online.

Nevertheless, the taxonomy also suggests that at least some consumers may accept passive data collection when benefits are clear and tangible. Research firm Parks Associates, in the *360 View Update: The Value of Data—New Smart Home Business Models* report, found that 51% of smart thermostat owners, 50% of hot water heater owners, and 48% of owners of smart clothes dryers were willing to share data and control in exchange for electricity discounts[17]. However, it may be the case that smart technology early adopters would have different attitudes about data sharing than the general population.

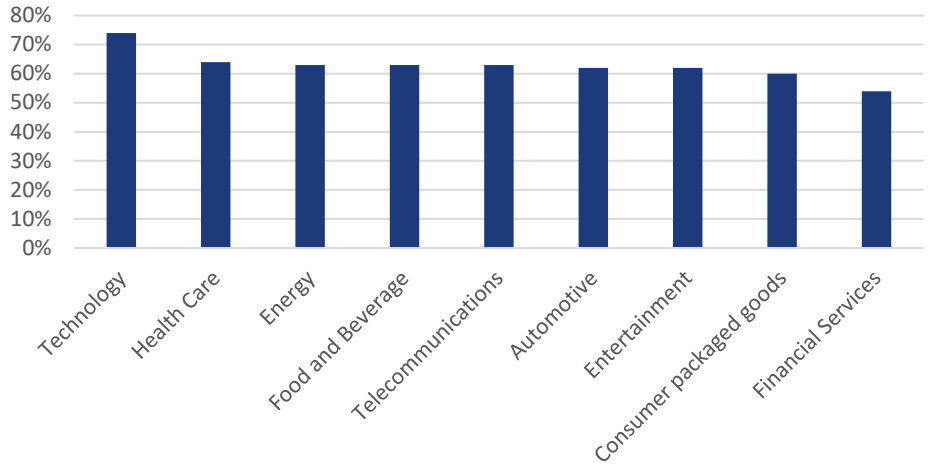
[17] https://www.infosecurity-magazine.com/news/half-of-us-consumers-daThoughta-for/

TRUST IN TECH COMPANIES

Trust in tech companies is a critical component of consumers' views on data privacy

A critical component of consumers' view on their data privacy and the tradeoff between privacy and the benefits of the digital economy is their trust in the technology companies which collect and use the data. The technology sector is routinely cited in the Edelman *Trust Barometer* as the most trustworthy sector in the global economy (Figure 11). This trust that tech companies will do 'what is right' helps explain why consumers continue to grant companies free access to their data.

Figure 11: Global consumer trust of sectors



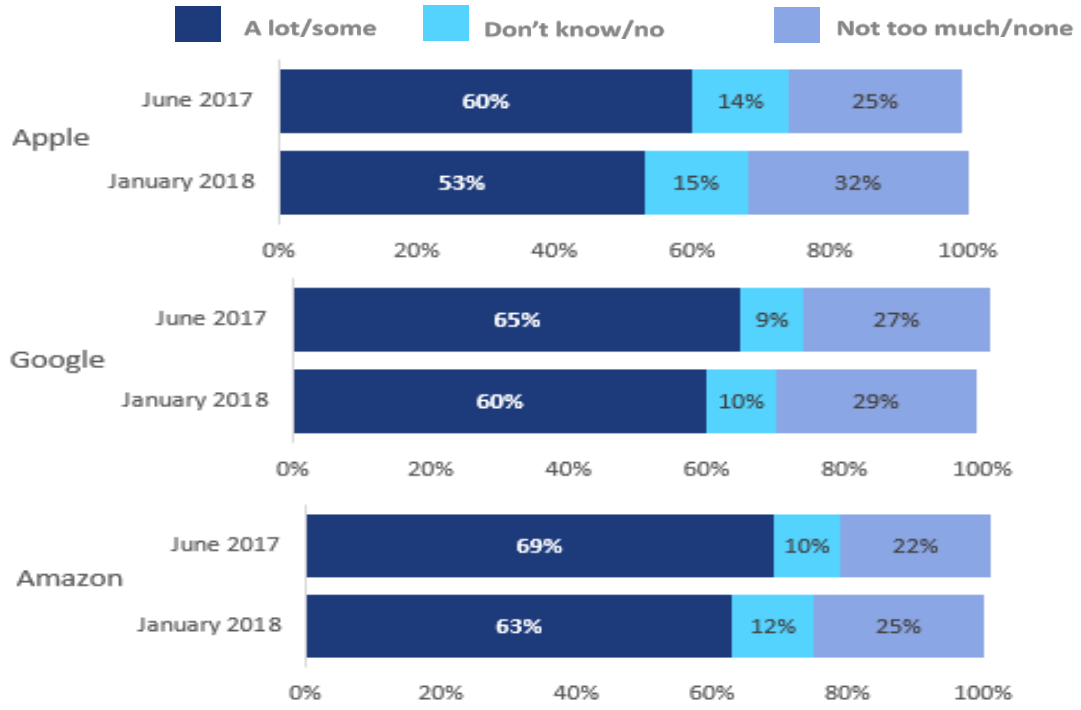
Source: Edelman *Trust Barometer*; Cornerstone Capital

However, trust is an asset that is easily lost

However, trust is an asset that is easily lost and difficult to regain. A small but consistent decline in trust was in evidence at the beginning of 2018 and has accelerated following various disclosures of violations of data privacy at Facebook. Survey firm Morning Consult polled 2,201 US adults in early 2018 on the question 'how much do you trust each of the following to keep your personal data secure and private?' This poll followed revelations about hardware vulnerabilities. Compared to a similar poll conducted in 2017, before the revelations, the number of respondents who stated that they had 'a lot/some' trust in Apple, Google and Amazon declined (although still exceeded 50%).[18] Similarly, early in 2018, the Edelman *Trust Barometer* survey found that average trust in social media platforms had fallen from 54% to 51%[19] from the previous year.

[18] https://morningconsult.com/2018/01/10/poll-shows-falling-trust-in-tech-companies-security-amid-disclosure-of-chip-flaws/
[19] https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf

Figure 12: Recent changes in trust in tech companies



Source: Morning Consult, 2018

More recent data suggests that consumer trust has declined more significantly over the last several months. In June 2018, The Edelman survey *Brands and Social Media Report* found that 60% of users reported do not trust social media companies to behave responsibly with the personal information they collect. [20]

While this question is not entirely comparable to the Morning Consult and *Trust Barometer* surveys, this result indicates a substantial decline in trust relative to a similarly worded question in the 2015 Morey study, which found that 56% of users did trust social media firms in the use of data.[21] The attention in the media to various data privacy scandals likely contributed to this finding, though respondents to the *Brands and Social Media* survey cited a wide range of concerns, including fake news, clickbait and bots for their growing distrust.

Trust is likely to be an important indicator going forward to assess whether consumers remain willing to trade data for services or step up pressure on companies and regulators to address their concerns.

[20] https://www.edelman.com/trust-barometer-brands-social-media
[21] https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

Regulatory: Divergent trends

Policymakers seeking to maintain consumer privacy while encouraging the free flow of information must begin with a fundamental question: Do companies or consumers own the data?

The EU defines privacy as a fundamental consumer right, while the US implicitly grants companies ownership of data; neither approach may be sustainable

The EU sides with consumers by defining privacy as a fundamental consumer right, requiring consumer consent for the use of data. The US, with its emphasis on freedom of speech and free markets, implicitly grants companies ownership through a regulatory framework that offers broad latitude in the use of data while seeking to reduce specific harms. Many emerging markets are evolving towards the EU standard, as is the state of California, in tension with the overall US approach.

The enactment of the General Data Protection Regulation in the EU will provide the first test of a comprehensive effort to manage data privacy, with a key challenge to attain interoperability with the US approach.

EU General Data Protection Regulation

Companies' ability to collect and analyze data was significantly curtailed as of May 25, 2018, with Europe's introduction of the General Data Protection Regulation (GDPR)[22]. The regulation's key elements are:

- Users must give consent for the processing of their personal data (opt-in) and this consent can be withdrawn;
- Users may, at any time, access their personal data as stored by the organization and be provided with information on its use;
- Any breaches of data must be reported within 72 hours of discovery; and
- Fines for breaching the GDPR are up to 2% of annual worldwide turnover (revenue) or €10mill (whichever is greater) per non-compliance event.[23]

The legislation empowers consumers to question any company in the world that collected their personal data as to its use and implications in the company's operations, as well as compel the company to delete data that was collected without clear permission. The implication for emerging technologies (such as smart home sensors and machine learning) may even be more significant as the GDPR compels companies to explain to customers how these technologies and algorithms considering consumer data are integrated into final marketing and pricing of products and services. There also are concerns that small companies may find the GDPR to be a formidable barrier to entry.

[22] https://www.eugdpr.org/
[23] http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

US Federal Trade Commission

The US to date has had a narrower focus than the EU in regulating data use. The Federal Trade Commission (FTC) is the primary government agency responsible for data privacy, including both issuing guidance and enforcing regulations under the Federal Trade Commission Act. The Act empowers the FTC to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe rules defining with specificity acts or practices that are unfair or deceptive; and (d) establish requirements designed to prevent such acts or practices[24].

An uncertain regulatory future

Who owns data? Europe, many emerging markets countries, and now the state of California, have determined that consumers own their own personal data. By contrast, US Federal laws and regulations implicitly assign ownership to the companies that have collected them.

The ongoing evolution of data privacy regulations presents three distinct challenges for companies:

- ***Inconsistency:*** Companies require a consistent global standard to manage a flow of data that transfers across borders with ease. The tension between the restrictive European and global standard and the more permissive US federal standard creates ambiguity for companies in how they manage the flow of data.
- ***Effectiveness:*** the sheer complexity of general data privacy laws present challenges in compliance for companies and enforcement for regulators. Companies with a strategic competency in data collection and use have every incentive to attempt to avoid regulations.
- ***Desirability:*** Consumers accustomed to easy access to services may dislike cumbersome consent procedures or diminished availability of useful free services.

In 2010, the FTC outlined its approach to data privacy using two primary models: the "notice-and-choice model," which encourages companies to develop privacy notices describing their information collection and use practices to consumers, so that consumers can make informed choices, and the "harm-based model," which focuses on protecting consumers from specific harms — physical risk, economic injury, and unwanted intrusions into their daily lives[25]. Legal actions are then brought against companies based on instances where a company's actions contravene its own privacy notice or where there is clear injury to consumers.

The FTC noted at the time that the results of this approach were mixed. Privacy notices seemed long, legalistic, and more designed to protect the company from liability than to empower consumers. The harm-based approach was too narrow, omitting reasonable consumer concerns about losing control of sensitive information, risks to reputation, privacy, and possibility of being monitored continually. Yet, little action has been taken to update these regulations since that report was published in 2010.

Other Jurisdictions

GDPR has been framed as a right of European citizens, not specifically a responsibility of European companies. For this reason, it applies to any company globally that holds the data of European citizens. Particularly for emerging markets democracies eager for access to European markets, there is pressure to adopt policies consistent with the strictest available standard.

In India, the court established a constitutional right to privacy in August 2017. While this development has not yet resulted in the adoption of

[24] https://www.ftc.gov/enforcement/statutes
[25] https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

a general data privacy law, the judgment calls for a robust data protection regime, including "the right to be forgotten" similar to what is found in Europe.[26]

In South Africa, the Protection of Personal Information Act (POPIA) comes into effect in 2018. POPIA has been described as a "stepping stone" to GDPR compliance, and is similar in requiring companies to obtain consent for the collection and specific uses of data.[27]

In Brazil, legislation inspired by GDPR has passed the Chamber of Deputies (the lower house of the national legislature), a key step towards enactment.[28] The law would replace existing data privacy regulations that apply only to specific sectors such as medicine and banking.

Finally, the state of California has passed a general data privacy rule, setting the stage for a potential conflict with federal regulators over the scope of legislation. The legislation requires companies to provide data to users and to delete it upon request.

In more authoritarian countries, the state of data privacy is ambiguous. Both Russia and China have data privacy laws, but in these countries the state may gather and use data for its own purposes in ways that conflict with these laws. For this reason, global firms may face uncertainties regarding the use of data, and may face risks to their global reputation if it appears that they are cooperating with foreign governments seeking to monitor citizens.[29]

Implementation Challenges

Numerous commentators have raised concerns about how the more restrictive regime envisioned by GDPR can be effectively implemented.[30]

Companies and investors should be concerned that neither the EU nor the US approach may be sustainable if the increased flow of data conflicts with rising consumer demand for data privacy. Also, challenges that are common in an innovative, global economy may create difficulties for the regulation of data use.[31] Some of the key challenges are:

- Global consistency in data regulation is important because of the ease with which data crosses national boundaries. Radical differences in regulatory approaches may undermine the objectives of policymakers by increasing the compliance burden for companies and encouraging regulatory arbitrage (the practice of locating operations in the most favorable regulatory environment).

[26] https://www.lexology.com/library/detail.aspx?g=818a8528-f387-4ccd-b42f-080ea58ffe34;https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time
[27] https://www.dlapiperdataprotection.com/index.html?t=law&c=ZA; http://www.epicrecruit.co.za/wp-content/uploads/2017/01/POPI-Summary.pdf
[28] https://iapp.org/news/a/brazilian-general-bill-on-the-protection-of-personal-data/
[29] https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr; https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region
[30] https://www.theverge.com/2018/5/22/17378688/gdpr-general-data-protection-regulation-eu; https://www.ft.com/content/624f813e-5f5e-11e8-9334-2218e7146b04; https://www.mycustomer.com/marketing/data/opinion-why-gdpr-will-fail
[31] Adapted from http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

- Both regulators and companies may be overwhelmed by the cost and complexity of compliance and enforcement.
- Companies may seek ways to evade regulations in order to continue to gather data, such as by requiring users to provide blanket consent to data as a condition of using services.
- Technologies may evolve faster than policymakers can adapt, rendering rules obsolete, perhaps even before they are finalized.
- Satisfying the public's demand for both data privacy and new data-enabled services may be a difficult balance to achieve and maintain.

Bringing it together: increasing uncertainty

A self-reinforcing cycle currently exists where new and more effective data-gathering technology enables innovations that exploit this rising flow of data and improve companies' ability to gather still more data. The future growth stories of many technology companies, supported by the market in the form of rich valuations, depend on this cycle continuing without limits.

However, this cycle also brings more and more of people's lives under scrutiny while diminishing their control over what is known about them, who knows it, and how the information is used. At present, dissatisfaction among consumers in the US has not led to practical efforts to curtail this trend because consumers as individuals feel powerless to prevent it. But this should not be considered a stable set of circumstances. If the public perceives the rising tide of data to be unacceptably invasive of individual privacy rights, consumer *resignation* could eventually turn to active *opposition* in the form of mass, collective action resulting in stringent regulation, or widespread action by individual consumers to block the gathering of their personal data. Companies would be at heightened risk if consumer trust continues to fall.

A global network of shared data cannot be effectively regulated at the national or regional level

Moreover, given the ease with which data travels, a global network of shared data cannot be effectively regulated at the national or regional level. The long-term result could be that the most stringent local laws will apply everywhere for all practical purposes. Some technology companies, including Facebook, have indicated that they plan to implement GDPR worldwide, for example. Alternatively, the diversity of approaches worldwide may make enforcement impossible in any jurisdiction as companies pursue regulatory arbitrage or exploit loopholes in local rules to their advantage.

Future scenarios: risks and opportunities

Future scenarios for data privacy will depend on the corporate response to the uncertain actions of consumers and policymakers

To help investors factor the uncertainty around data availability into company valuations and into their stewardship/engagement activities, we describe a set of possible future scenarios for data privacy, explore each scenario's impact on business drivers, and assess eight case-study companies and emerging business models.

These scenarios are necessarily speculative, but we believe they can serve as a useful benchmark to assess how well companies are positioned to adapt to changing circumstances, whatever they may be.

A stakeholder map

Future scenarios for data privacy will depend on the corporate response(s) to uncertain actions of consumers and policymakers:

- *Companies* will use data in the most expansive possible way that the market and regulators will allow. Company strategy is driven by desire to continually introduce new and more useful technologies to support and grow valuations, as well as internal corporate cultures valuing technological progress as a primary social good.

- *Consumers* may come to demand greater ownership and agency over their data, limiting the growth of data available for corporate use. Alternatively, these concerns may never coalesce into a popular movement, but instead diminish over time as the perceived benefits of new technologies outweigh negative impacts.

- *Policymakers* will need to respond to conflicting societal pressures, possibly including: (1) the influence of industry; (2) public demand for regulation; (3) the impact of future scandals related to data privacy similar to Cambridge Analytica; (4) governmental priorities affected by data or data-enabled technology (e.g., national security concerns).

- *Employees* are critical stakeholders because sustained success in tech requires a deep reservoir of talent and motivation. The best employees seek out opportunities for innovation and advancement. The regulatory environment will determine whether whole industries can offer employees attractive opportunities, while consumer acceptance may drive whether incumbents or new entrants are preferable as employers. A company that had a sustainable advantage in access to data might also have an advantage in attracting employees as well, especially if these firms are able to offer the most generous compensation and opportunities for rewarding work.

We categorize the possible futures based on consumer and regulatory trends:

We categorize the possible futures based on consumer and regulatory trends

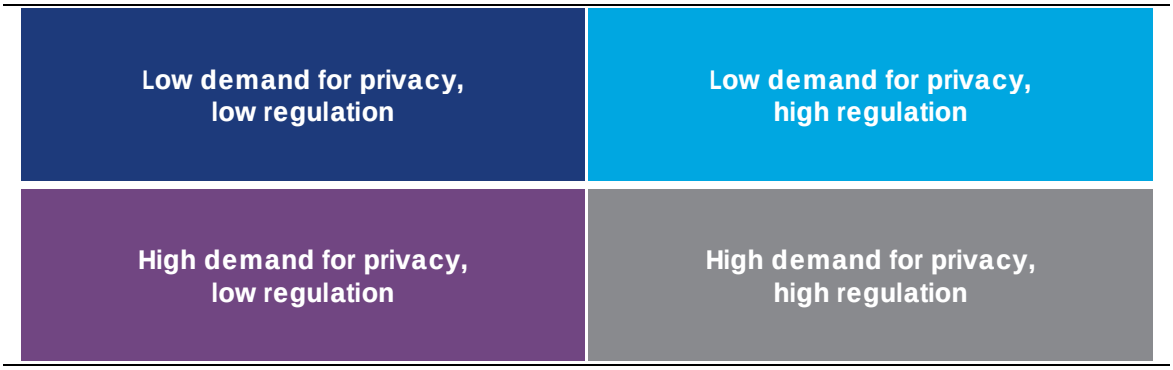
- **Regulation:** Regulation resolves the issue of whether companies or consumers own data. Prior to enactment of the GDPR, companies were largely self-regulated in their collection and use of data. GDPR raises a number of uncertainties about the future of data:
  - To what extent will GDPR hinder the collection of data regionally and globally?
  - Will global policymakers follow the lead of the EU in developing regulations?
  - Will global regulatory inconsistency thwart the objectives of GDPR?
- **Consumer:** The state of *resignation* — dissatisfaction coupled with inaction — is unlikely to persist. Either consumers will find a means to oppose the collection of at least some data, or will come to view data collection as an acceptable price of new and beneficial services. Of course, not all consumers will react in the same way, and consumer attitudes may differ by company, by product, by geography, and by the nature of data collection activities. The issue will resolve based on whether consumers (in general) expect robust privacy protections, or are willing to trade privacy for new services that they expect to come to market.

Some uncertainties include:

- How will consumers react to the increasingly comprehensive data being collected about them, and particularly to the collection of passive data that they did not willingly provide?
- To what extent will consumers consider emerging technology products to be essential to their lives, work, or community?
- Will consumer trust in technology companies be affected by future scandals or other perceived misuses of data?

Together, these two trends create four future scenarios, as shown in the Figure 13. The speed of technological advances, such as smart home security systems, smart speakers and other voice-operated input devices, and other sensor technology, are likely to put pressure on regulatory and behavioral trends.

Figure 13: Potential future operating environments



Source: Cornerstone Capital Group

Four potential operating environments

Figure 14: Potential corporate operating environments and impact on business drivers

Scenarios	Business drivers	Implications
Low demand for privacy, low regulation (LD/LR)	*Regulatory:* Business models are unaffected	Companies continue using data and consumers willingly trade data for free and improved services, at the risk of violating social norms.
	Consumer: Market demands are met with innovation	Sustainable competitive advantage possible for companies with access to the most robust data sets and data-gathering capabilities.
	Employee: Increased retention	Talent likely to concentrate in leading firms with best access to data.
Low demand for privacy, high regulation (LD/HR)	*Regulatory:* Regulatory burden increases	Compliance costs reduce opportunities for new technologies.
	Consumer: Decreased ability to anticipate consumer needs	Lack of progress dampens consumer interest in data-driven products and services.
	Employees: Decreased retention	Talent seeks opportunity for innovation elsewhere.
High demand for privacy, low regulation (HD/LR)	*Regulators:* Unresponsive or ineffective regulation leads to new services that protect consumer privacy	Alternative business models emerge to fill consumer demand for products and services built to ensure their privacy.
	Consumers: Increased ability to price at a premium	Companies that are trusted can charge higher fees to advertisers, or consumers may be willing to pay for privacy; larger, well-known companies may have a "trust advantage" over less established entrants, which can engender product loyalty.
	Employees: Increased retention of consumers and employees	Incumbent companies with the benefit of consumer trust will be more attractive to employees as well.
High demand for privacy, high regulation (HD/HR)	*Regulators:* Regulatory burden increases	Compliance costs increase but public trust increases as well.
	Consumers: Increased ability to price at a premium	Companies are differentiated by response to regulation; consumers may be willing to pay for privacy; consumer trust eases introduction of new technologies and entrants.
	Employees: Entrepreneurial culture is significant	Entrepreneurial companies innovate to limit the impact of reduced access to data and fill customer demand.

Source: Cornerstone Capital Group

1. Low demand for privacy, low regulation

In this scenario, consumers, companies and regulators are aligned in support for the free flow of data

In this scenario, consumers, companies and regulators are aligned in support of the free flow of data. Consumers' concerns diminish and regulators take a hands-off approach to regulating data privacy. Companies largely are free to gather data in whatever manner is technologically feasible and to use data to further business objectives. Consumers come to expect that much of their online and offline lives are known to companies. Employee engagement is high given the lack of constraints on their ability to innovate. Oligopoly or monopoly is possible for companies that acquire a data advantage, but entry may be possible for companies that offer a distinctive service. Regulation is post-hoc and situational, designed only to reduce "harms" rather than enforce any overriding consumer right to information.

Technologies come into the market more quickly than under other scenarios, and companies may also use this information for other purposes not fully practical currently, such as making hiring decisions or recommending more individually tailored health care treatments, etc.

"Privacy" is not a priority societal concern, but the relinquishment of privacy may create risks of other violations of social norms that could become risks to companies. For example, companies could use personal data to discriminate against protected classes; monitor employee off-hour activities; or gain political influence.

A ProPublica report found that Facebook's algorithm at one time allowed advertisers to exclude people with "ethnic affinities" from their content;[32] also, according to a Bloomberg analysis, Amazon is more likely to offer same day delivery to neighborhoods with high white populations than with higher minority populations. In neither case has it been suggested that the companies are *intentionally* discriminating, but both examples demonstrate how purely data-driven business strategies can result in *inadvertent* discrimination (possibly reflecting the inequities in the society at large) absent specific policies to promote equal treatment.

Longer-term, "profiling" data could be used to shape the behavior of consumers for perceived social good

Longer-term, "profiling" data could be used to shape the behavior of consumers for perceived social good (as defined by the profiling entity).[33] For example, the Chinese government is experimenting with a "social credit system" to measure the "trustworthiness" of citizens using their data, and possibly rewarding or punish them accordingly.[34] Among private companies, "social engineering" remains an internal discussion,[35] but such systems are not impossible to implement in practice with existing technology.

The "low demand, low regulation" scenario could be stable, unless the public becomes aware of the violation of social norms or specific harm enabled by free access to data.

2. LOW DEMAND FOR PRIVACY, HIGH REGULATION

In this scenario, innovation is restricted, consumer demand goes unmet, and there are material gaps in data

In this scenario, the policy environment places stringent restrictions on the collection and use of data despite diminishing consumer demand for privacy. This scenario could arise because of the global adoption of the most severe restrictions, or because a powerful special interest group emerges that successfully advocates for limits on the flow of data.

Innovation is restricted, consumer demand goes unmet, and there are material gaps in data. Cheating is common because market participants have little incentive to comply with the regulatory regime, and monopoly or oligopoly power may accrue to the companies with sufficient resources to determine legal means of evading the intent of rules, or to make use of more permissive jurisdictions. Violations of social norms (e.g., discrimination) may be less common

[32] https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race
[33] https://hbr.org/ideacast/2018/05/how-ai-is-making-prediction-cheaper (See the speculative discussion about how Amazon could use its user data to ship goods to consumers before they order them.)
[34] http://www.wired.co.uk/article/china-social-credit; https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; http://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4; https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/
[35] https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy;

because of the relatively lower use of data, but those that do occur may not be resolved because of the system's lack of legitimacy.

This scenario would be unstable because of its lack of perceived legitimacy among stakeholders, but may be difficult be difficult to dislodge, particularly if consumers come to no longer expect data-driven innovations. Another concern may be the potential use of data by autocratic governments to crack down on activities and technologies that may promote democracy in their countries.

3. HIGH DEMAND FOR PRIVACY, LOW REGULATION

In this scenario, consumer concerns about data privacy persist but no effective regulatory regime arises. Either regulators support companies' desire for the free flow of information, or are unable to keep up with fast-moving technological changes, or fail to achieve global policy coordination, or a powerful special interest group emerges that successfully advocates against limits on the flow of data and in favor of commercialization of technologic advances.

In this scenario, innovation is high but consumer acceptance of new products is more difficult to obtain

Innovation is high, but consumer acceptance of new products is more difficult to obtain. Consumers are more directly engaged in the products and services that they use and require a high degree of trust in the companies whose services they use. Consumers may also demand more control over their data at the product level (e.g., through more powerful privacy controls), potentially rendering material gaps in the data that is collected. Employee attraction and retention will also depend on maintaining trust, since talent may become frustrated by consumer resistance to innovations, or by the perception that they are being asked to deceive or manipulate other stakeholders.

Violations of social norms (e.g., discrimination) may become key risk factors for companies. If such violations become commonplace, this scenario may not be sustainable as the market will demand more stringent regulation.

Companies may obtain market power through both data advantages and inspiring high degrees of trust. New entry is difficult for companies lacking existing stores of both data and trust.

This system is likely to be unstable, unless a few companies gain monopoly or oligopoly power and can maintain public trust through self-regulation. Moreover, under this scenario, users may seek products and services that allow them to take control of their own data. (Please see the section "Investing in Privacy Protection".)

4. HIGH DEMAND FOR PRIVACY, HIGH REGULATION

In this scenario, both consumers and regulators consider data privacy to be a priority, curtailing corporate access to data. In turn, consumers accept that there is a trade-off in terms of slower information services innovation.

In this scenario, companies compete on their ability to innovate within the regulatory framework

Governments limit access and use of data in response to consumer and public concerns about data privacy. Innovation is slower and perhaps impossible for some applications, but public trust in the regulatory regime renders consumer acceptance of new products easier for companies to obtain. Global cooperation facilitates corporate compliance efforts, and a more level regulatory landscape makes it more difficult for companies to gain monopoly power using a data advantage. Companies compete on their ability to innovate within the regulatory frameworks, and new entry is relatively feasible. Employee engagement is high, though with some frustration about regulatory constraints on their work.

Enforcement is burdensome but manageable for companies. Cheating happens but is punished by the market and the legal and regulatory system. Occasional serious lapses in data privacy can have serious consequences but also lead to improvements in the system.

This scenario, which closely resembles established regulatory structures such as food and auto safety, is highly stable, but relies on regulators to continually update rules to keep pace with technological advancements.

Data dependency and business models[36]

Access to consumer data has always been important to marketing companies' products and services. Improved quality and quantity of personal data makes possible new business models where data itself is the product or service, or at least among the core competencies of the firm. Investors in these firms should understand how they are exposed to uncertainties related to public acceptance of data collection and use, and how the magnitude of those uncertainties will increase exponentially with the widespread adoption of the internet of things and the explosion of available passive data.

Investment risk will depend on two issues:

1. ***Exposure:*** The exposure of the company business model to scenario uncertainty, including what kind of data it gathers and how dependent its business model is on data;

2. ***Trust:*** How well positioned the company might be to adapt to societal change, based on its trustworthiness to key stakeholders, including consumers and employees.

The next sections consider *exposure* and *trust*.

Exposure

Companies that are both highly dependent on data and exposed to changes in attitude around data collection will face a high degree of risk related to data privacy scenario uncertainty.

Three factors will help to identify the nature of company exposure to uncertainty:

- ***Data usage:*** what does the company do with data?
- ***Data breadth:*** how comprehensive is the data collected?
- ***Data dependency:*** How reliant is the company's business model on data?

"Data usage" and "Data breadth" are informed by the taxonomy detailed in Morley, et.al, cited earlier in this report. These two factors support an assessment of the degree of exposure to consumer opposition faced by the company's data collection activities. "Data dependency" assesses the importance of data access to the company's business model.

Companies that are both highly dependent on data and exposed to changes in attitude around data collection will face a high degree of risk related to data privacy scenario uncertainty.

We add the data dependency factor as an indication of a company's exposure to change in the data privacy environment, either from behavioral or regulatory shifts. The aim of this framework is to enable investors to better understand a company's relationship to data in the face of converging trends.

[36] The company business models are based on Cornerstone's research using company 10Ks (annual reports), disclosures on company websites, Bloomberg, various media articles and some brokerage research. Companies were invited to provide comment.

Figure 15: Data collection and use assessment

Factor	Explanations		
Data usage:	Internal ⟷		External
	Uses data to improve product offering or promote company's products	*Sells or share insights from data with external organizations*	*Sells or shares data with external organizations*
Data breadth:	Given ⟷		Profiled
	Only uses data that is given	*Collects data from use of products*	*Combines given data with external data to create profiles*
Business dependency:	Low ⟷		High
	Model little impacted by data collection	*Model enhanced by data collection*	*Model relies on data collection*

Source: Cornerstone Capital Group

To illustrate the application of our data collection and use framework, we selected a representative set of eight US companies that interact heavily with consumer data. Our aim is to give a snapshot of industries with a range of exposure to the issue of data privacy, and we picked companies that exemplified data usage within their industry. The selection is not intended to represent the entire economy.

Figure 16: Companies used as case studies (Market Capitalization is as of July 31, 2018)

Company	Market Cap ($ billion)	Sector
Alphabet	$848.8	Internet media
Amazon	$886.2	E-commerce consumer discretionary
American Express	$85.5	Consumer finance
AT&T	$231.5	Telecom / media
Facebook	$499.1	Internet media
MasterCard	$207.4	Consumer finance
Twitter	$24.3	Internet media
Walmart	$261.1	Mass merchants

Source: Bloomberg

ALPHABET

What does Alphabet do?

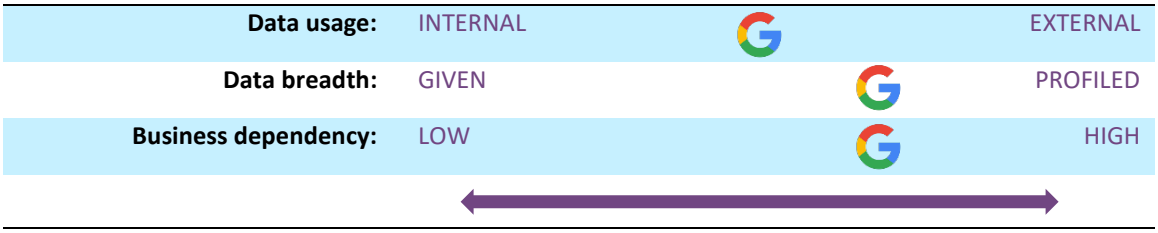
Alphabet's core business is internet services including search (Google), communications (Gmail) and cloud computing. The company generates revenue primarily from targeted digital advertising on its platforms. Google offers its services for free to consumers, and in turn collects and analyzes their data to identify potential spending needs and patterns. This data allows marketers to target ad spending to consumers who are most likely to buy their products. Alphabet charges advertisers based on the viewership of and or actions taken (clicks) on their ads. A smaller portion of sales comes from apps, in-app purchases, and digital content from the Google Play Store.[37] [38]

Google is the leading platform in programmatic ad buying industrywide versus its peer group, including Facebook, Yahoo, and Twitter. Programmatic ad buying is growing as an industry and is likely to account for over 80% of US display ad spending in 2018[39].

How does Alphabet collect and use data?

- *Data usage:* Alphabet uses its data to create demographic and spending profiles of its consumers, and then bills advertisers for individualized and targeted marketing space. Alphabet also shares generalized data to show trends.
- *Data breadth:* Alphabet tracks consumers' online activity, including what they search, what they buy online, how they navigate any site that uses Google Analytics, and email uses.
- *Business dependency:* Alphabet is relatively dependent on data, as the company's value-add to advertisers is its individualized insight into consumers.

Figure 17: Alphabet's data collection and use



Source: Cornerstone Capital Group

[37] Annual Report
[38] Research from Canaccord Genuity, June 15, 2017
[39] Bloomberg

AMAZON

What does Amazon do?

Amazon provides an online e-commerce platform, with its competitive advantage built from data collection and analysis. Amazon's mass data allows the company to target consumers, boosting sales, while also utilizing sophisticated logistics to decrease costs. To increase revenue, Amazon builds individual consumer profiles to recommend additional products, as well as to manage and individualize pricing. To decrease costs, the company uses big data to predict what products consumers are likely to purchase, when they might buy them, and where they may need them.

Most of Amazon's revenue is generated from its Amazon e-commerce store, with a smaller portion from third-party sellers. The third-party revenue includes a commission based on the types of goods sold, as well as advertising revenues. Estimates suggest that recommendations to consumers based on their profiles increases revenue by up to 30%.[40] Subscription services represent 5% of sales, primarily fees from Amazon Prime, a premium subscription offer for users which includes free two-day shipping and access to streaming services. Amazon Web Services, a highly profitable cloud computing service, accounts for 10% of sales and generates a steady cash flow stream which allows Amazon to invest generously in its e-commerce and related business.[41]

How does Amazon collect and use data?

- *Data usage:* Amazon uses data to individualize product recommendations and prices for consumers, as well as efficiently stock local warehouses and facilitate distribution of products. Amazon does not share data with third parties beyond data needed to fulfill their functions (e.g., transactions).

- *Data breadth:* Amazon processes personal data from consumers, including purchasing history, shopping cart history, and most searched-for products, to determine how they spend their money.

- *Business dependency:* Amazon's business offering focuses on e-commerce but sources its competitive advantage from dynamic pricing that is enabled by data collection. Amazon typically offers discounts on best-selling items and charges more for less-popular items, earning higher margins on the latter.

Figure 18: Amazon's data collection and use

Source: Cornerstone Capital Group

[40] https://www.investopedia.com/articles/insights/090716/7-ways-amazon-uses-big-data-stalk-you-amzn.asp
[41] Annual reports

American Express

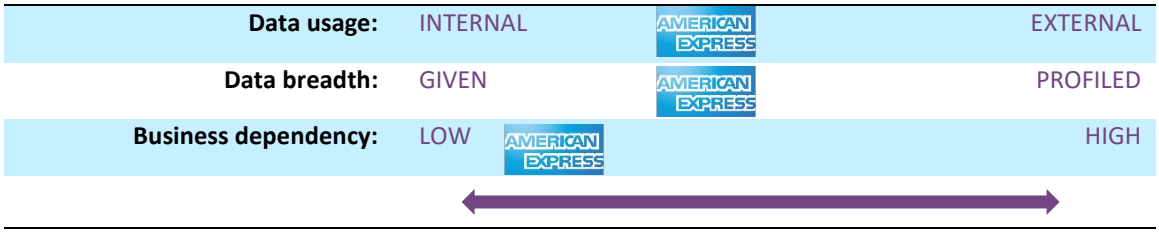
What does American Express do?

American Express is a payments and processing business, facilitated through its charge and credit card offerings along with travel-related services. American Express receives revenues from card spend and fees, merchant transaction processing (swipe) fees as well as interest from some of its credit card products. American Express's model builds its own momentum, as high spending on its cards allows American Express to invest in rewards and other benefits for its consumers, incentivizing consumers to spend more[42].

How does American Express collect and use data?

- *Data usage:* American Express utilizes consumer data internally to encourage spending by its customers on its card products;
- *Data breadth:* American Express collects data on consumers' spending habits and shares its data with third parties to provide products and services to its consumers. Customers are informed of and authorize the use of the data;
- *Business dependency:* American Express uses data to better target consumers, but its business model builds its own momentum.

Figure 19: American Express's data collection and use



Source: Cornerstone Capital Group

[42] Annual reports

AT&T

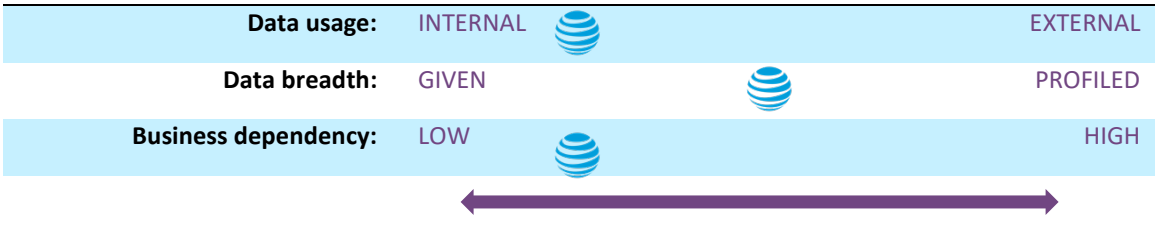
What does AT&T do?

AT&T is a communications infrastructure company with two focuses: internet and wireless service provision, and entertainment services. For internet and wireless, AT&T facilitates internet and cellular communications for companies, government, and individual subscribers. For entertainment, AT&T provides satellite TV programming. For both services, AT&T enhances its revenue by providing targeted advertising of additional relevant products to customers.[43] On June 12, 2018, a federal judge approved AT&T's $85 billion acquisition of Time Warner. The deal will unite Time Warner's TV and movie content with AT&T's distribution system, including cell phone and satellite networks. In the deal, AT&T will own HBO, CNN, Warner Brothers and other Time Warner brands.[44]

How does AT&T collect and use data?

- *Data usage:* AT&T uses data to target advertisements towards consumers who are likely interested and willing to spend further on AT&T's products;
- *Data breadth:* AT&T collects data around consumers' internet and data usage, including account information, network usage, web browsing and wireless location, and TV viewing information;
- *Business dependency:* Currently, AT&T moderately engages in using profiled data while primarily focusing on providing the infrastructure of digital communication. This will likely change as the company grows its entertainment business with the acquisition of Time Warner (assuming the merger survives remaining legal challenges). The company will probably profile data to better target advertising to viewers.

Figure 20: AT&T's data collection and use



Source: Cornerstone Capital Group

[43] Annual reports
[44] http://money.cnn.com/2018/06/12/media/att-time-warner-ruling/index.html

FACEBOOK

What does Facebook do?

Facebook is a social media website which offers targeted digital advertising. Facebook provides a free platform for consumers to communicate with their personal network and, in exchange, collects their data to analyze consumers' demographic and spending profiles. Facebook charges advertisers to display their targeted ads in front of consumers who are most likely to view their products[45].

Facebook generates nearly all revenue from offering advertising across its products, which include Facebook, Instagram, Messenger, and third-party affiliated websites along with mobile apps. Facebook also owns WhatsApp, a messaging and Voice over IP service. Payments are based on the number of impressions delivered or the number of clicks on ads. Facebook has 1.4 billion daily active users as of December 31, 2017, or 18% of the world's population[46].

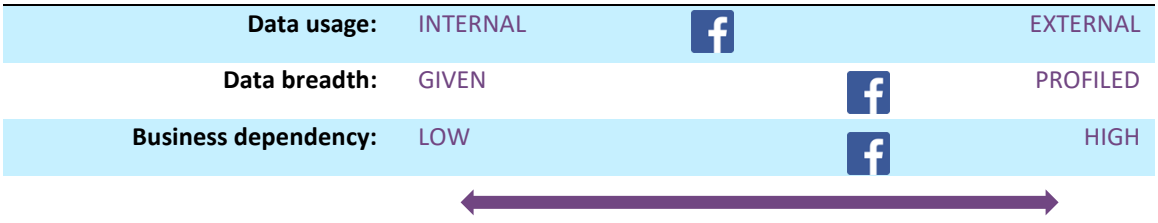
How does Facebook collect and use data?

- *Data usage:* Facebook uses its data to increase its value-add for advertisers. Facebook creates profiles of its consumers and can facilitate advertisers' targeted marketing of goods and services. The company also shared data with broker firms that monitor customers' spending habits, a practice the firm announced it would discontinue on March 28th, 2018[47].

- *Data breadth:* Facebook collects all the information on communication, likes, etc. it receives from consumers, including data from partner apps, and can track web surfing at any time the consumer is logged onto the site.

- *Business dependency:* Facebook receives almost all its revenue from advertising.

Figure 21: Facebook's data collection and use



Source: Cornerstone Capital Group

[45] Annual Report
[46] https://www.census.gov/popclock/world
[47] https://venturebeat.com/2018/03/28/facebook-ends-data-broker-partnerships-in-blow-to-targeted-ads/

MASTERCARD

What does MasterCard do?

MasterCard is a payment processing company, with a growing focus on data analytics. Through its consumer credit, charge, debit cards and related services, MasterCard provides the financial structure to facilitate and process transactions for products and services. This allows MasterCard to observe billions of transactions globally, which MasterCard uses to provide spending insights to commercial clients looking for help in their marketing and business decisions.

Data analytics and security fees are a growing focus for MasterCard. In 2017, data analytics and security fees were 23% of revenues, compared to 14% in 2010[48]. Two years earlier in 2008, MasterCard said "we do not anticipate consulting and research fees becoming a significant percentage of our business"[49].

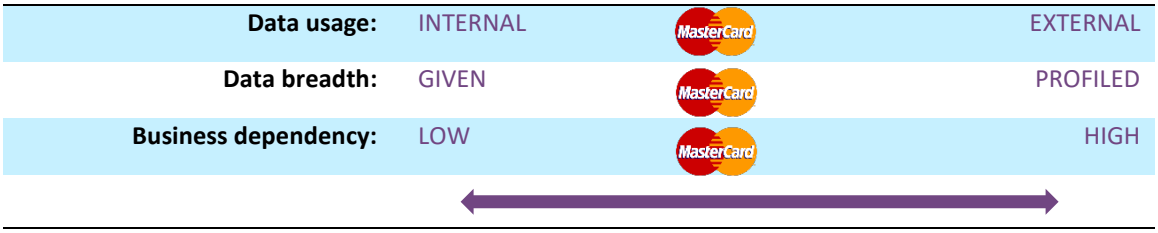
How does MasterCard collect and use data?

- *Data usage:* MasterCard uses data from consumers to provide insights on payment patterns for its data analytics products, though it does not sell personal data. In addition, MasterCard engages in data philanthropy, where it shares some data with organizations doing socially minded work[50].

- *Data breadth:* MasterCard collects data through its payment business and holds the personal account and transaction data for customers, financial institutions, and merchants.

- *Business dependency:* MasterCard is increasing its focus on data collection with the growth of its data analytics product, though its core services remain payment processing.

Figure 22: MasterCard's data collection and use



Source: Cornerstone Capital Group

[48] http://d1lge852tjjqow.cloudfront.net/CIK-0001141391/4f9c4d33-a295-484c-adfc-8028189cf402.pdf
[49] http://d1lge852tjjqow.cloudfront.net/CIK-0001141391/200495d7-59ef-413c-97d7-873b581d6f76.pdf
[50] https://mastercardcenter.org/action/call-action-data-philanthropy/

TWITTER

What does Twitter do?

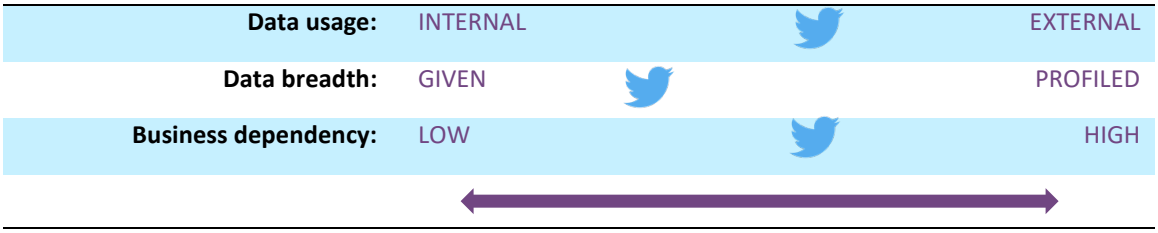
Twitter is a social networking site and news service which engages in data collection about consumer behavior. Twitter provides a platform for consumers, media outlets, and platform partners to contribute public content and interact with messages. In addition, Twitter operates a mobile app which lets anyone broadcast and watch video live publicly. Twitter uses the data collection to create insights into consumers' interests and then provides targeted advertising and promoted "tweets" for marketers. Twitter also licenses and sells the data to other businesses[51].

Twitter stands out from the other companies assessed by its public nature. Consumers' interactions with the other companies are mostly private to only the consumer, select other individuals (e.g., a merchant or a network of friends), and the company. In contrast, consumers using Twitter's platform primarily post on a public network.

How does Twitter collect and use data?

- *Data usage:* Twitter's technology platform enables Twitter to provide targeted advertising and promoted "tweets" based on customer interests and demographics. The company also licenses its consumers' data to other organizations.
- *Data breadth:* Twitter collects information on customers' interests (what a customer likes and reads, and demographics).
- *Business dependency:* Twitter receives all its revenue from advertising or data licensing.

Figure 23: Twitter's data collection and use



Source: Cornerstone Capital Group

[51] Annual Report

WALMART

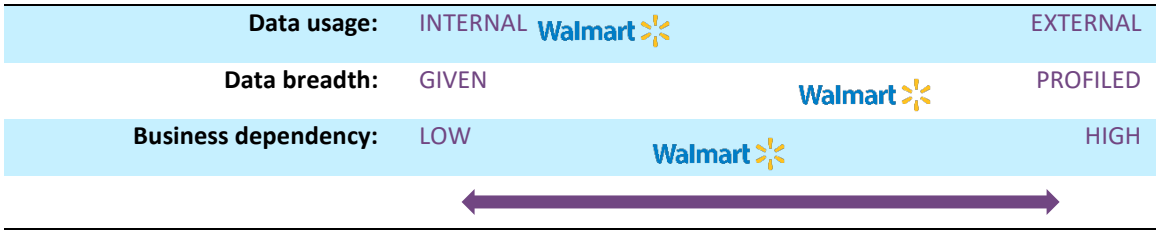
What does Walmart do?

Walmart provides discounted retail products both in store and online. The company revolutionized the "big box" retail store and logistics model starting in the 1950s and has since built a global network of stores with sophisticated merchandising and distribution; logistics optimization is its competitive advantage[52]. However, Walmart has faced competition from Amazon and the growth of e-commerce. To adapt, Walmart acquired a series of e-commerce companies, including Jet.com, to improve online data capability and appeal to a younger, more urban customer[53]. Still, Walmart's core strategy remains price leadership and superior distribution.

How does Walmart collect and use data?

- *Data usage:* Walmart increasingly uses its data to personalize suggested offerings to customers and to better target inventory selection to specific retail stores.
- *Data breadth:* Walmart collects data from its online platform and combines this information with data from third-party sources to build profiles of its customers.
- *Business dependency:* Walmart is increasing its focus on data collection. The Jet.com purchase boosted Walmart's efforts and capacity for data collection and analysis.

Figure 24: Wal-Mart's data collection and use



Source: Cornerstone Capital Group

[52] Annual Report
[53] https://techcrunch.com/2016/08/08/confirmed-walmart-buys-jet-com-for-3b-in-cash/

COMPARING BUSINESSES' DATA COLLECTION AND USE

We provide a summary assessment of the eight companies' data collection and use below.

Figure 25: Eight assessed companies' data collection and use

Source: Cornerstone Capital Group

Key takeaways from the assessment above include:

- None of the companies was assessed as "Given" on Data Breadth, signaling that companies have moved beyond merely collecting data that is given voluntarily towards more passive forms of data collection.
- Companies whose heritage predates the internet show less dependence on data than their online-only counterparts. However, the general trend across sectors is towards greater dependence on data analytics.
- Companies are still calibrating their data-collection strategies. Facebook's recent shift to discontinue sharing data with external brokers is notable, as it reduces its extreme position along the factors. The enactment of the GDPR in late May 2018 has required most companies to reset their privacy policies.

COMPANY DATA USE AND EXPOSURE

Companies that are built to collect and use data are likely to face downside risk in the case of increased regulation of data designed to increase privacy for consumers. We use the company data collection and use assessment from above as an indication of business model exposure. Companies that sell or share data externally, profile consumers, and rely on data collection are likely to face higher burden from regulation and could see the emergence of substitutes.

We assess the exposure to a change in data privacy scenarios of the eight case study companies through the three indicators described above. A 'high' exposure suggests that a company may face difficulty in retaining consumers or employees or adapting its business model in a scenario other than "low demand, low regulation."

Given the range of possible future scenarios, this assessment is descriptive and directional, not specific. Our aim is to help investors understand how companies are positioned if data privacy scenarios quickly change. Investors can start their engagement on the issue of data privacy with companies that are assessed as having a 'high' exposure.

Figure 26: Company scenario exposure: summary and notes

	Company data use
Alphabet	Data gathering and analysis is core to Alphabet's business model but its use is mostly, though not exclusively, for internal purposes.
Amazon	Data gathering and analysis for internal purposes is core to Amazon's business model, but it does not share data externally.
American Express	Data is not core to American Express's business, though it supports the company's core payments business and the company shares data with external partners.
AT&T	AT&T has limited data use, collection, and dependency. However, the company will likely focus more on data as it integrates the Time Warner acquisition.
Facebook	Facebook's model depends on data collection and profiles its users. Facebook has a history of sharing data with outside partners, but has scaled back recently.
MasterCard	MasterCard is increasing its dependency on data collection and shares data insights externally
Twitter	Twitter's strategy depends on robust collection of data, and use for internal purposes and with external partners.
Wal-Mart	Wal-Mart has not traditionally relied on data, but is increasing its use in its marketing and operations, particularly through the acquisition of e-commerce companies.

Source: Cornerstone Capital Group

Consumer and Employee Trust

The trust of key stakeholders is critical to managing under any scenario

Our model considers not only the exposure of the company to uncertainty, but also the company's resilience in the face of societal change. While assessing this factor is necessarily speculative, we believe that maintaining the trust of key stakeholders — consumers, employees and regulators — is critical to managing under any of our scenarios.

We examine the eight case-study companies through the lens of employee and consumer trust (the trust of regulators is assumed to be consistent with the other stakeholders). These indicators are not meant to be exhaustive, but instead to serve as signposts for investors in understanding how certain companies are positioned for all scenarios.

CONSUMER TRUST

Consumer trust is especially central to the "high demand, low regulation" scenario but could be important in all, especially as regulators are more likely to intervene when consumers complain about broken trust. In each of our scenarios, consumer trust becomes an important indicator of consumer retention, a company's ability to price products at a premium, and continued permission to access consumer data.

However, we find limited data on consumer trust at the company level across sectors. We therefore combine a series of different surveys to infer insights into consumers' trust of the assessed companies.

Particularly noteworthy are the results associated with Facebook. As shown in Figure 27, a Cohn & Wolfe survey conducted in spring 2017 rated Facebook in the middle of its "authentic brands" survey. This preceded revelations about the company's relationship to the political consulting firm Cambridge Analytica and its sharing of user data with business partners apparently in conflict with their own policies and a 2011 consent order with the Federal Trade Commission.[54] Federal lawmakers have criticized the company for failing to identify these practices to a Congressional Committee during CEO Mark Zuckerberg's testimony in April.[55] Facebook has claimed that the practices were never hidden and that they are in the process of winding them down. However, continued revelations undermine confidence in Facebook's account of the matter.[56]

By 2018, following disclosures of its relationship with Cambridge Analytica and several other concerning actions related to data privacy, the company decisively emerged as the least trusted social media brand.

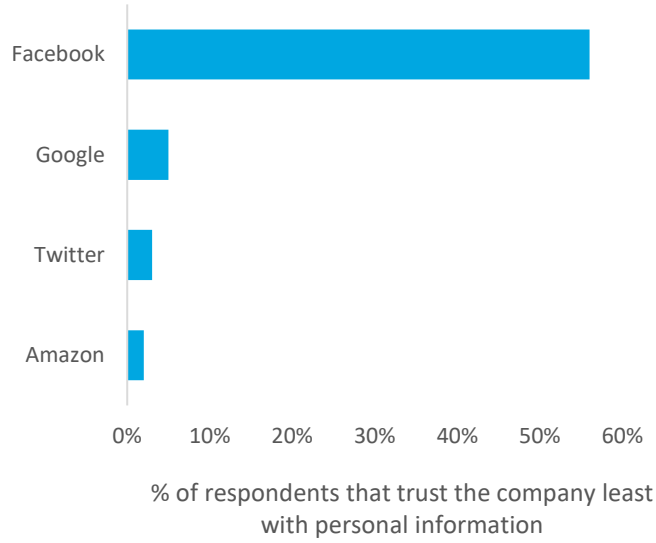
[54] https://www.nytimes.com/2018/06/05/opinion/facebook-china-privacy-data-security.html; https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html;https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer
[55] http://ewn.co.za/2018/06/07/us-lawmakers-press-facebook-over-chinese-data-sharing
[56] https://www.engadget.com/2018/07/12/sec-is-reportedly-investigating-how-facebook-disclosed-data-scan/;

Figure 27: Trust proxies' benchmarking

Company	Authenticity benchmark: Global top 100	Loyalty benchmark: US top 329
Amazon	1st	15th
American Express	-	56th
AT&T	-	286th
Facebook	92nd	-
Google	4th	191st
MasterCard	34th	-
Twitter	-	-
Walmart	-	241st
YouTube	68th	

Source: Cohn & Wolfe[57]; Temkin Group[58]; Cornerstone Capital Group
Note: Google and YouTube are separated in both surveys

Figure 28: Least trustworthy tech companies



Source: Recode[59]; Cornerstone Capital Group
Note: this survey was conducted in April 2018, after news of Cambridge Analytica and Facebook broke

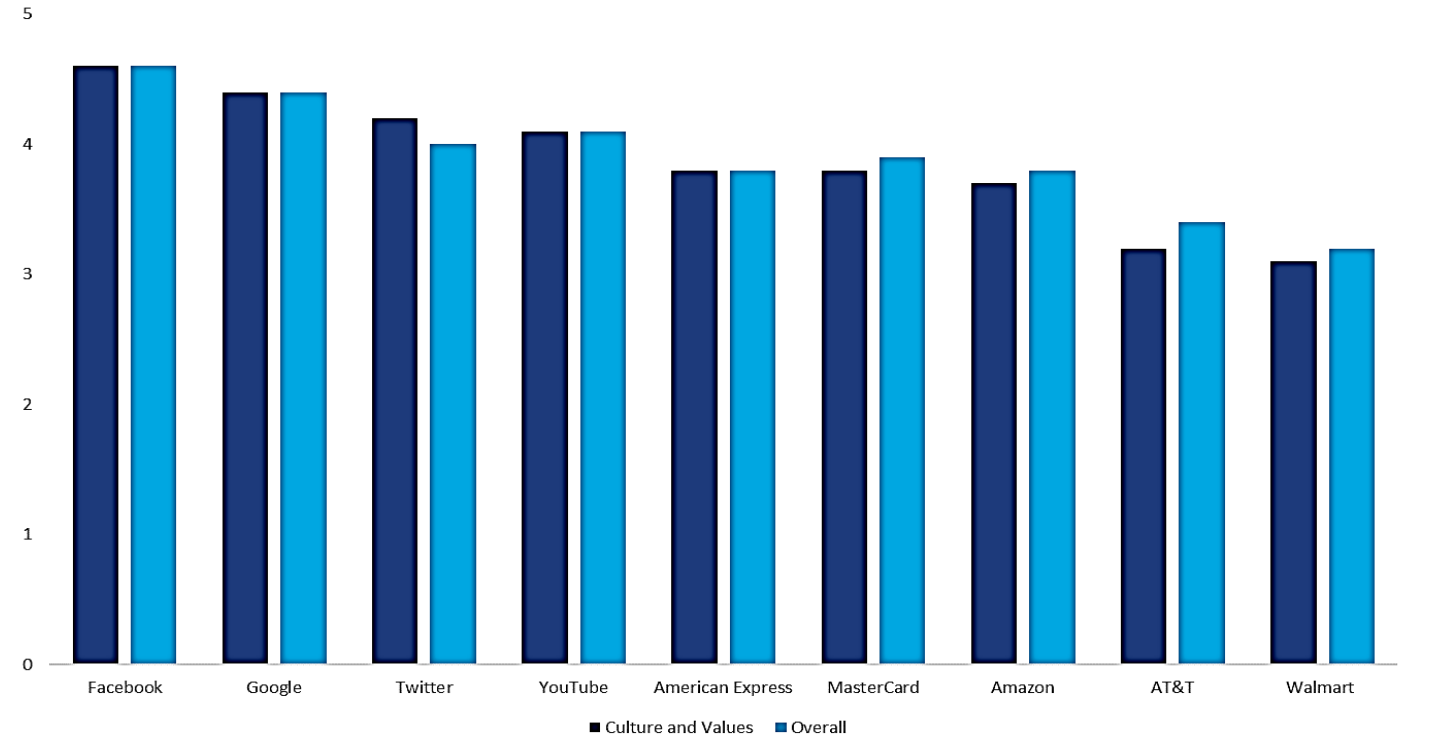
EMPLOYEE ALIGNMENT

The companies we assessed rely on human capital for building algorithms, creating brand awareness, and selling their products, including marketing and advertising. Employees' attitudes towards working at these companies thus becomes important for the companies' ability to source human capital and maintain their competitive advantage.

We assess employees' review of company culture and overall opinion from Glassdoor, as shown in Figure 29.

[57] http://authentic100.com/
[58] https://temkingroup.com/temkin-ratings/temkin-trust-ratings/#2017
[59] https://www.recode.net/2018/4/10/17220060/facebook-trust-major-tech-company

Figure 29: Employees' review of companies



Source: Glassdoor; Cornerstone Capital Group
Note: Ratings out of 5, with 5 representing top performance. Overall rankings include culture and values; work/life balance; senior management; comp & benefits; and career opportunities. YouTube is part of Alphabet, but receives a separate score in the survey.

Figure 30: Stakeholder trust in companies: summary and notes

Company	Consumer trust	Employee alignment
Alphabet	Mixed: Google rates highly, but YouTube is lower. Alphabet may face decreasing trust if consumers start associating YouTube with Alphabet's overall brand	Employees rate Google and YouTube highly, though YouTube's ratings dropped significantly in the past two years
Amazon	Consumers view Amazon favorably; the company benchmarked the strongest in all three surveys	Amazon may face challenges with human capital. Employees rank the company poorly on culture and values
American Express	Loyalty benchmarking indicates that consumers view American Express relatively highly	Employees rank American Express as average
AT&T	AT&T struggles with the lowest levels of consumer loyalty compared to the other companies assessed	AT&T faces low levels of employee alignment
Facebook	Facebook ranks poorly on consumer trust, particularly since the headline allegations concerning Cambridge Analytica	Employees rank Facebook highly
MasterCard	Consumers rate MasterCard as average in terms of authenticity compared to the other companies assessed	MasterCard receives average employee reviews
Twitter	Trustworthy rankings suggest that Twitter is viewed on par with most tech companies	Reviews imply that employees enjoy working at Twitter
Walmart	Loyalty benchmarking finds that Walmart ranks poorly	Walmart struggles with the lowest employee reviews

Source: Cornerstone Capital Group

Conclusions: trust and exposure

We identified future scenarios for the market according to uncertainties in consumer and regulatory responses to data privacy concerns. Each company was assessed according to exposure to these uncertainties, and for the reserves of consumer and employee trust that may help companies weather possible disruptions.

We conclude that there is no one optimal positioning for companies, but that companies will be relatively better or worse off depending how their positioning is suited to a particular operating environment.

Companies with high data exposure may be at risk in more restrictive scenarios, but will encounter greater upside in more permissive scenarios. While greater trust is always better than less trust, trust may be a more important asset in some scenarios than in others. We group our operating scenarios (demand for privacy/degree of regulation) with the optimal positioning as follows:

Low demand, low regulation (LD/LR): This scenario rewards ***high exposure***. While trust is always an essential corporate asset, the diminished importance of data privacy for consumers and regulators suggests that trust has a lower level of significance for the management of this issue. The absence of limitations on the use of data implies that accelerated growth is possible for companies positioned to capture and exploit a data advantage.

Low demand, high regulation (LD/HR): This scenario rewards ***low exposure***. Because of the outsized role of the government and limited opportunities for innovation, trust is not a special advantage. Companies with high exposure may find data to be a less valuable resource than hoped.

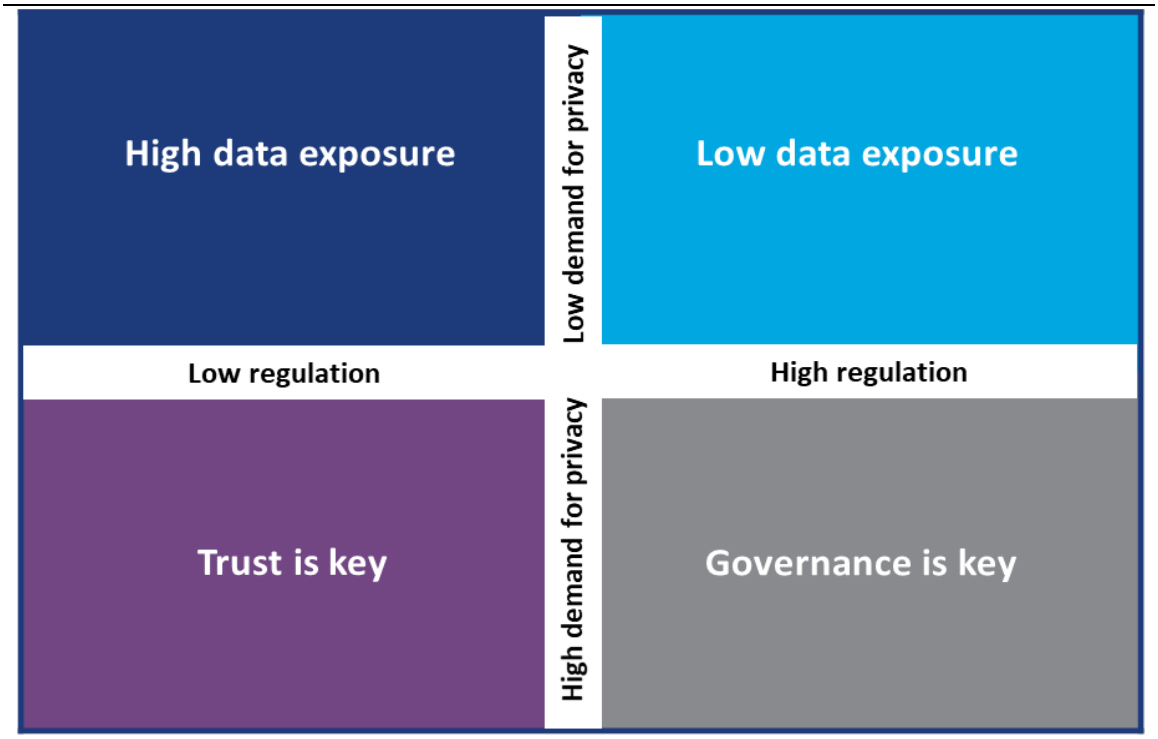
High demand, low regulation (HD/LR): This scenario rewards ***high trust***. In this unstable scenario, exposure to data privacy concerns may yield opportunities but is highly risky. Companies will be more likely to succeed in carrying out their data strategy (whether core or peripheral to their overall business strategy) if they earn the trust of consumers and employees.

High demand, high regulation (HD/HR): In this scenario, ***trust is not at a premium*** because of public confidence in the system to appropriately manage data privacy issues. Companies have less opportunity to monetize data, but business models are available to those companies able to manage the regulatory and market expectations for data privacy. In this scenario, governance of ***data privacy is at a premium***, and shareholder engagement to understand how the company balances privacy and innovation is important to the investment decision.

While our scenarios reflect the uncertainty in the market, we believe that given current trends the “high demand, low regulation” scenario is the most likely medium-term outlook for the industry, at least in the United States. Overall, surveys appear to demonstrate that consumer awareness and concern about data privacy is increasing. Whether the recently enacted GDPR in Europe will properly balance privacy concerns without undue interference in the market’s need

to innovate is not yet known. However, we are skeptical that regional regulations can exercise effective oversight over a global market.

Figure 31: Operating scenarios and exposure to data



Source: Cornerstone Capital Group

We therefore believe that consumers in the developed world will increasingly seek to manage their own data privacy, either by limiting the data that is collected on themselves or by doing business only with companies that earn their trust. For this reason, investors should welcome the currently high levels of trust in the technology industry, but be concerned about recent declines.

Figure 32 summarizes our view on each company in our sample.

Figure 32: Summary view of case study companies

Company	Consumer trust	Employee alignment	Data Exposure	Best suited to Scenario	Commentary
Alphabet	High, but at risk	High, but at risk	High	LD/LR or HD/LR	Alphabet's model relies on data collection, Consumer trust could quickly decrease if consumers begin to associate YouTube with Alphabet
Amazon	High	Low	Medium	HD/LR	Amazon is well positioned, as the company only uses data internally and holds a high level of consumer trust. However, employee engagement is a risk to the company.
American Express	High	Average	Low	HD/LR	American Express is likely protected through consumer loyalty and a low data dependent model. Yet, the company's sharing data externally might pose a risk to its brand if opposition to the practice grows
AT&T	Low	Low	Low	LD/HR	Medium: AT&T currently has a low data dependent model. This may change with the impending acquisition of Time Warner, but the company would need to overcome low trust to execute on a data-dependent strategy
Facebook	Low	High	High	LD/LR	Facebook relies on data collection, while also raising concerns about consumer trust
MasterCard	Average	Average	Medium	HD/HR	MasterCard is moving towards a high-dependency data model; however, it is not yet clear whether the company will gain the trust needed to execute the strategy under all scenarios
Twitter	Average	High	High	LD/LR	While Twitter's model is focused and reliant on data, consumer and employee ratings imply the company is viewed positively
Walmart	Low	Low	Medium	LD/HR	Wal-Mart struggles with consumer loyalty and human capital, which may raise concerns about the company's move towards increasing data dependency

LD = low demand for privacy; LR = low regulation; HD = high demand for privacy; HR = high regulation

Data privacy and investment: How can investors take direct action?

1. Corporate governance and engagement

Our case studies demonstrate a model for assessing the implications of data privacy for investors that can be applied to companies across numerous consumer-facing fields where the collection and use of personal data are becoming more important to business models.

Our framework includes three broad areas of inquiry:

- How important is data collection and use to the company's business model?
- What kind of personal data does the company collect and/or use?
- How strong is consumer trust and employee engagement in the company?

Because the circumstances are rapidly evolving and the availability of data is limited, investors will also want to evaluate how well the company's governance is positioned to manage changing norms, expectations and regulations that may affect access to data, stakeholder trust and, ultimately, company strategy. Investors will want to be informed about the company's strategic adaptability, its approach to managing stakeholder relationships, and its overall strategy for risk management.

These topics are best explored through engagement with the company. The responses will inform investors about how much confidence to have in the company's governance of these issues, as well as the likely scenarios for which the company is best suited.

STRATEGIC ADAPTABILITY

1. **Who is responsible for data privacy and to whom do they report?** Reporting lines can suggest how companies view certain risks. For instance, a reporting line through the legal department may indicate that a company views data privacy as a regulatory risk, while a reporting line through operations could indicate the company is addressing data privacy concerns by design.

2. **How does the board ensure that it accesses diverse viewpoints from its stakeholders on the issue of data privacy?** Board members with different professional experiences may be more effective at understanding and managing emerging stakeholder issues. Reference to global best practices may also provide confidence in the company's data privacy policies.

3. **How do compensation incentives include data privacy risk mitigation metrics?** Management that is rewarded for risk mitigation as well as growth generation may be more likely to position a company for medium-term flexibility.

4. **How has the company adapted its business model and/or risk management to the introduction of GDPR?** Investors will want to know whether the company intends to adapt its data approach to greater demands for privacy or seek ways to continue to access the same kinds of data.

STAKEHOLDER RELATIONSHIPS

5. **Do management and the board track consumer trust and, if so, how does the company engage consumers to develop long-term trust?** Consumer trust of a company is likely to influence consumers' willingness to share their data going forward and thus is a key indicator of customer retention and pricing ability.

6. **How does management reconcile internal reporting of employee feedback on company culture with views on social media?** A review of public comments on social media can complement internal employee surveys as a means of evaluating employee engagement.

7. **Has the company faced any regulatory actions related to data privacy?** How were these resolved?

RISK EXPOSURE AND MANAGEMENT

8. **Does the company disclose data privacy as a risk issue?** A company with a business model dependent on data faces specific risks if behavioral or regulatory trends accelerate. Appropriate disclosure in the annual and sustainability reports as well as legal privacy statements indicates that the company is at least considering data privacy risk as material to its business.

9. **How does the company anticipate and avoid use of data that would contradict company values?** The accelerated use of data could result in undesirable societal outcomes such as discrimination, employee surveillance, or disruption of the political process (such as the dissemination of "fake news"). Companies should disclose how they monitor the use of data and provide disclosure to stakeholders to avoid these negative outcomes.

10. **Will the company manage passively collected data differently from data gathered from users?** Because it is difficult to ensure that passive data is collected with consent of the user, except in the most general way, does the company view these data differently from other methods of data collection that are the result of voluntary actions on the part of users?

2. Investing in Data Privacy Protection

We also identify three areas of data privacy that offer growth opportunities for investors based on the potential future scenarios of data privacy:

- Enterprise-focused data management;
- Consumer-focused privacy control; and
- Further ad-supported business models.

ENTERPRISE-FOCUSED DATA MANAGEMENT

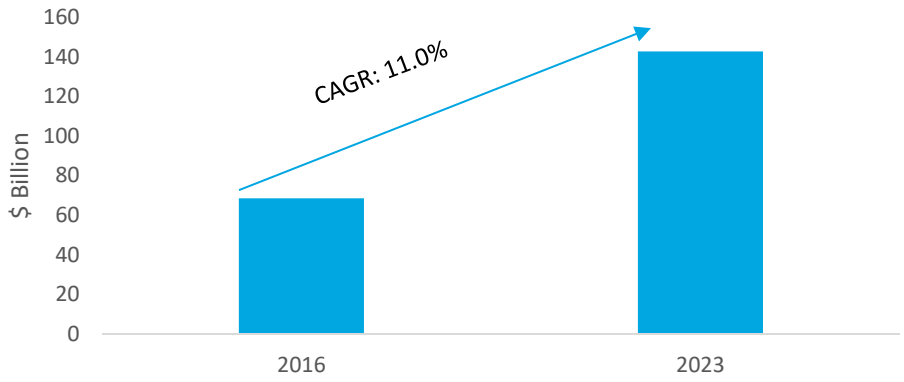
Below we describe companies that help enterprises deal with privacy issues and regulation. Companies with this model are well positioned if consumer or regulatory concern increases.

A few private companies are emerging to fill the need created by emerging regulation (e.g., GDPR). Nymity and OneTrust offer services to ensure compliance with changing data privacy regulation; Nymity provides software, assessments, and compliance strategies, while OneTrust provides privacy readiness and impact assessments through data inventory, website scanning, and vendor risk management. TrustArc offers software that integrates with companies' systems to show that the company is privacy-compliant to consumers.

Few public companies market data-privacy management products, though IBM is a rare example. IBM provides a privacy framework to help manage risk, determine readiness for regulations, and develops standards for companies' privacy offices.

Market sizing is difficult given the level of uncertainty about future data regulation. However, one study found that the market for enterprise data management (the systems used by an organization to integrate and retrieve data for use and communication) solutions is expected to post an 11% compound annual growth rate from 2016 to 2023 (Figure 33)[60]. We include this as a representation of how quickly the market can move.

Figure 33: Global market size of enterprise data management



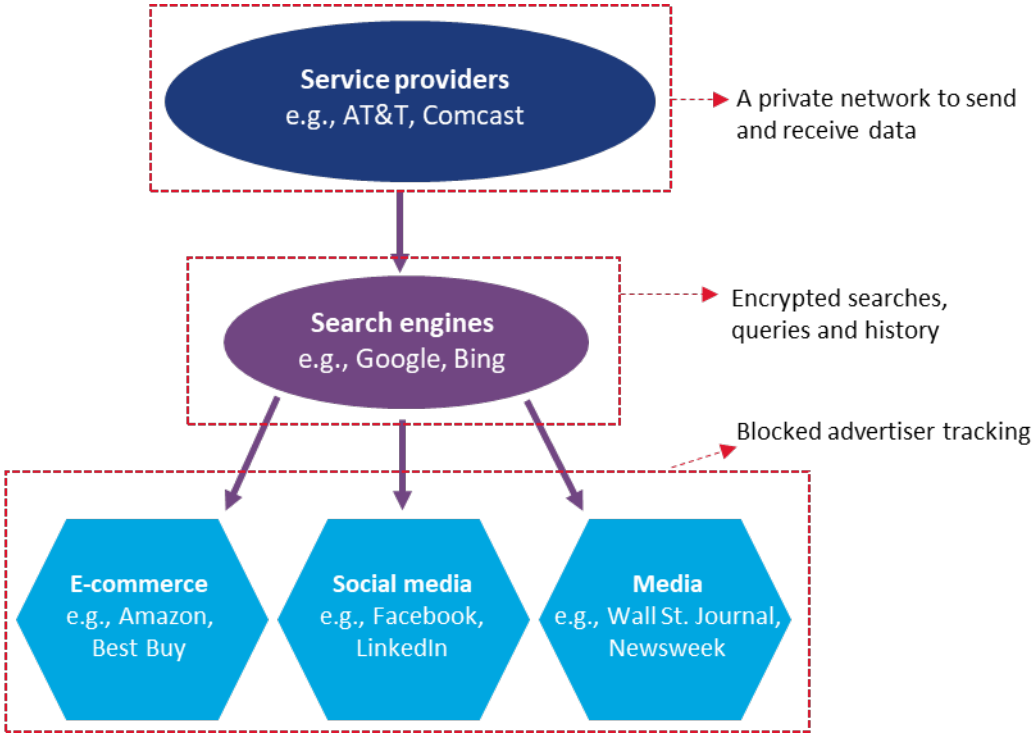
Source: Reuters; Cornerstone Capital Group

[60] https://www.reuters.com/brandfeatures/venture-capital/article?id=24923

CONSUMER-FOCUSED PRIVACY CONTROL

Companies that are built for data privacy and to ensure consumer trust are attractive if the world moves to a scenario of 'trust is key.' In this scenario, consumers would likely look for technology to securitize their data while still using existing companies' products and services. Privacy focused technology would thus act as an additional layer between consumers and existing companies (Figure 34).

Figure 34: Additional layers of technology to strengthen privacy



Source: Cornerstone Capital Group

We find that there are currently few services that protect consumers' data while using existing companies. However, we found select examples, including Disconnect.me and Piriform. Disconnect.me lets consumers visualize and block websites that track their online movements, and Piriform creates software that erases consumers' browser search history and cookies.

FURTHER AD-SUPPORTED BUSINESS MODELS

Shared mobility services such as Uber, Via, and Lift use big data and mined personal data to offer ride services. Uber has a massive database of drivers and using its algorithm matches a customer to the nearest on-duty driver. The data are collected, analyzed and used to predict the customer's wait time, and to recommend where drivers should place themselves to take advantage of the most passengers and fares. Uber manages billions of GPS locations. The company uses a customer's personal anonymized data to monitor which services are used most and determine where to offer or focus those services. According to Uber's privacy statement, the company may retain a customer's information even if the account has been deleted. Generally, this use of personal data is beneficial to shared mobility service customers[61].

This model presents an opportunity for further advertisement revenue. A new company called Vugo has contracts with about 3,500 Uber and Lyft drivers in New York City to install video screens in their vehicles. The screens will display video advertising and can't be turned off or muted. Drivers get paid to carry this service, supplementing their income in addition to fees charged to passengers for the ride service. If shared mobility fleets and drivers start to rely more on funding from advertising, these companies may have more incentive to use personal data to track and market to its passengers.

To quote a blog from Vox: "Look at Facebook and Google, which we allow 360-degree surveillance of our lives."[62]

[61] https://blog.kissmetrics.com/how-uber-uses-data/
[62] https://www.vox.com/energy-and-environment/2018/3/27/17163264/autonomous-car-self-driving-advertising-business

John Wilson is the Head of Research and Corporate Governance at Cornerstone Capital Group. He leads a multidisciplinary team that publishes investment research integrating Environmental, Social and Governance (ESG) issues into thematic equity research and manager due diligence. Previously, he was Director of Corporate Governance for TIAA-CREF, the largest private pension system in the U.S. John writes and presents widely about the relevance of corporate governance and sustainability to investment performance for academic, foundations, corporate and investor audiences. John has more than two decades of experience in sustainable investing and corporate governance. john.wilson@cornerstonecapinc.com

Heidi Bush, CFA is Director, Global Research. Heidi was previously a Managing Director, Sector Research at JUST Capital where she focused on S&P 500 company research to evaluate financial and corporate governance metrics. Prior to JUST Capital, Heidi was a Senior Equity Analyst at Lord Abbett & Co., LLC, covering small cap growth stocks. Before that, she was a large cap equity portfolio manager and analyst at the YMCA Retirement Fund, a defined contribution pension fund. Heidi received an MBA from Columbia Business School and BA from State University of New York at Albany. She holds the Chartered Financial Analyst designation. heidi.bush@cornerstonecapinc.com

We would like to give special thanks to Sebastian Vanderzeil and Emma Currier for their significant contributions to this report:

Sebastian Vanderzeil is a is an ESG and Impact Strategist and member of Cornerstone Capital Group's Global Advisory Council. Sebastian served as Director and Global Thematic Analyst with Cornerstone Capital Group's Research team until April 2018; his research spanned a range of themes including climate, energy, income inequality, automation and technology. Previously, Sebastian was an economic consultant with global technical services group AECOM, where he advised on the development and finance of major infrastructure across Asia and Australia. Sebastian holds an MBA and was a Dean's Scholar at New York University's Stern School of Business, and has a bachelor's degree in natural resource economics from the University of Queensland.

Emma Currier is a former Research Associate for Cornerstone Capital Group. She joined the firm following her graduation from Brown University in May 2016, and recently accepted an opportunity to work with an impact-oriented investment firm in Myanmar. While at school, she worked with the Socially Responsible Investing Fund and as a teaching assistant for the Public Health and Economics departments. She spent her sophomore summer researching differences between American and Indian educational styles in Arunachal Pradesh, India, and completed a summer investment bank analyst position with Citi in the Media & Telecom group in 2015.

For more information on this report or our services, please contact our Investment Advisory team:

Phil Kirshman, CFA, CFP®	Chief Investment Officer	+1 646-650-2234
Alison R. Smith	Managing Director, Head of Business Development	+1 646-808-3666
M. Randall Strickland	Director, Client Relationship Management	+1 646-650-2175

1180 Avenue of the Americas, 20th Floor, New York, NY 10036 | +1 212 874 7400
www.cornerstonecapinc.com | info@cornerstonecapinc.com
Follow us on Twitter, @Cornerstone_Cap

Important disclosures