Data Privacy, Power, and Trust
Emerging Risks for Internet Platforms

Bret Miller, CFA, Senior Vice President, Research Analyst
Jenny Hardy, Vice President, Research Analyst

The extraordinary amount of data generated by individuals throughout their digital lives is today concentrated on the leading internet platforms. The market valuations and data-driven business models of these companies are highly dependent on the trust they have built with users. As more and more of people’s lives move online, this concentration of data and the implicit trust users have given these companies raise questions about privacy rights, government regulations, and the balance between corporate interests and social responsibility.

The broad scope and importance of this issue has led us to characterize it as an ESG (Environmental, Social, and Governance) consideration. Data and the companies that traffic in it are playing a larger role in society, its norms, and the direction of the digital economy. Given this complexity, we believe it is essential that ESG is fully integrated into the investment process. Data risks can be challenging to quantify and often have implications that cut across traditional approaches to equity analysis. In our view, a fully integrated ESG investment process allows investors a more nuanced view of data privacy issues and enables more sophisticated analysis of individual companies.
Challenges in a Data-Driven World

The rapid adoption of smartphones over the past decade has enabled virtually continuous connectivity to the internet for three billion people, with mobile devices rarely farther away than a pocket, purse, or bedside. The smartphone has transformed the way people seek and receive information, buy goods and services, and interact with others. The digital tracks left behind by this activity are enormous, as the amount of data being generated is doubling nearly every two years. More data was created during 2014–2016 than in all previous human history.

Much of this information has been collected and stored by a relatively small number of leading internet and mobile platforms, who use it as the foundation for their business models. Investors have recognized the value of this data, adding trillions of dollars to the market capitalization of these companies over the past decade. However, while these data-driven business models can create significant value, they also carry a range of risks that many investors might overlook or underestimate. We see these risks as ESG issues that fall into three principal areas:

• **Data privacy and trust** – Who owns my personal data and how are businesses using it?
• **Social responsibility** – What are the risks related to the power and control these platforms have over information and content online?
• **Regulatory** – How should governments regulate and balance consumer protection and national security in light of the potential monopolistic market share of the companies leading the digital economy?

Data Privacy and Trust

Many services on the internet—social networking, search engines, messaging apps, and streaming video content—are free, but most companies offering these services ultimately seek to monetize their users’ data. How these companies monetize user data is not always clear to users (and certainly cannot be easily understood by just reading a company’s privacy terms and conditions). Today, users have implicitly placed enormous trust in the internet platforms as they have integrated these leading mobile ecosystems into their lives, with the average US user spending over 3 hours a day on her smartphone.

Companies in this new digital economy must strike the delicate balance of providing a high quality and valuable personalized service to consumers while not breaching this trust—such as using personal data too aggressively with monetization or even being “too creepy” with personalization. This is a complex challenge with no simple answer.

For example, should Google use highway traffic data and your behavior history to wake your alarm 15 minutes early if it knows your commute to work is going to take longer today because of road construction? Or should Microsoft use your calendar content and LinkedIn network to alert you that your husband went to high school with the client you are about to meet with? Or, if your wife recently bought a pregnancy test on Amazon, should Amazon recommend prenatal vitamins to your Prime account that is shared by the family?

Efforts like these to improve the value add, user experience, and profitability of an online service may result in breaching users’ trust with their private information. Even practices that are less extreme than these examples could put a company at risk of user backlash, which could then result in lower user engagement and a reverse spiral of network effects if users leave a platform.

Publicly, many companies have been acknowledging these risks and have sought to balance the data privacy preferences of consumers versus monetization and commercial interests.

• **Google** in June 2017 announced it would stop scanning the content of users’ Gmail accounts for the purposes of targeting advertisements.

• **Apple**, also in June 2017, announced a new feature that allows Safari browser users to block the “retargeting” ads that follow consumers around the internet based on recent website visits. (An example of a “retargeting” ad is when a user visits a travel website to consider a hotel and, a week later on an unrelated news site, sees an ad for the hotel they had previously viewed.)

• **Facebook** recognizes that it is not only dependent on the trust of users, but also on the trust of advertisers. In 2016 and 2017, Facebook discovered a series of errors in how the company calculated certain advertising metrics for its advertisers, such as video view duration, daily reach, and time spent on publisher articles. Following an outcry from advertisers that Facebook shouldn’t be allowed to essentially “grade its own homework,” the company expanded its relationship with third-party ad monitoring and measurement firms, who will be able to add more validity to Facebook’s reported advertising performance metrics.

**Information Insecurity**

Information security threats from both criminal and nation-state hackers remain well-known but serious risks. Corporations continue to invest significantly to protect their data. The information security industry is an $80 billion market growing 8%–9% annually, and this spending still has not prevented recent attacks that have disrupted the operations of large businesses such as Mondelez, Maersk, and Reckitt Benckiser.
Many of these changes are a response to a growing awareness among consumers of the importance of privacy, which has been reflected in the growing adoption of ad blocking tools.

There are no simple solutions to these dilemmas, but we believe the large internet platforms must use caution and carefully test new features in order to maintain user trust, as this is one of their key competitive advantages. Factoring in the risk of breaching this trust, in our view, is a crucial component of analysis. While the large internet platforms have mostly avoided serious trust issues with users—so far—there are a number of smaller companies that have not and are paying the consequences.

Slice Intelligence, which operates the email management program Unroll.me, faced a backlash in April 2017 after users discovered how their data were being used. Unroll.me is a free service that scans through a subscriber’s email and allows the user to unsubscribe from email marketing lists. However, Unroll.me also compiled receipts from the company Lyft, anonymized the content, and sold it to Lyft’s rival Uber. This was all deemed legal and within the company’s privacy policy, but this did little to calm upset users. After an angry tweet, the company implied its practices were typical. “We totally understand how you feel. Just know, Gmail has more data on you than we ever would.”

In our view, this defense should not comfort tech investors.

**Social Responsibility and Scrutiny**

Almost half of all time spent consuming media is now done online, with a significant portion of that time taking place on the leading internet platforms. Tencent users on average spend over an hour a day using its services; Facebook users spend 50 minutes; YouTube users spend 40 minutes. These platforms have gained enormous power as they have become the de facto gatekeepers and distributors of news, content, and information.

That power, in our view, is an ESG issue, and with it comes greater social responsibility and growing public scrutiny. How companies choose to take on—or avoid—responsibility for the content on their platforms may have minimal financial implications in the short term, but these decisions could have a significant impact on how consumers and partners trust and engage with these platforms over the long term. For example:

- Some YouTube advertisers in early 2017 halted their spending on the site after their ads appeared alongside terrorist propaganda and racist videos.

- Following the election of Donald Trump, Facebook was criticized for becoming a tool for the viral distribution of “fake news.”

- After public concern grew about youth addiction to the video game *Honor of Kings* within Tencent apps, the company placed daily restrictions on how long users of a certain age could play the game.

- Apple resisted the FBI’s request that it unlock the smartphone of the San Bernardino shooter in the interest of national security, arguing that the process would provide “a master key, capable of opening hundreds of millions of locks.”

These controversies highlight the challenges for these leading platforms, given their scale and powerful roles in the distribution of news, content, and information.

**Advantages Lead to Dominance**

Many tech platforms have built upon their competitive advantages to generate extraordinary growth and take dominant positions in their industries. These companies have been able to benefit from “network effects,” in which a service becomes more valuable as it attracts more users. (In social media, for example, people can be enticed to sign up because so many of their friends and families are already there.) Tech platforms can also benefit tremendously from scale, since the cost of a technology service (via a website or program) is largely fixed and can be expanded to meet demand. Having more users allows the company to gather more data, provide better services, and create nuanced profiles that can generate revenue. This success (Exhibit 1), however, has also become a vulnerability, as critics contend these companies have become so dominant that they are, in effect, monopolies. Some have asked these tech companies to be regulated like a utility.

**Exhibit 1**

**Winner Takes All**

Google and Facebook have accounted for virtually all growth in the global digital advertising market in 2016.

<table>
<thead>
<tr>
<th>Service</th>
<th>Users (in billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>2.0</td>
</tr>
<tr>
<td>YouTube (Google-owned)</td>
<td>1.5</td>
</tr>
<tr>
<td>WhatsApp (Facebook-owned)</td>
<td>1.3</td>
</tr>
<tr>
<td>Facebook Messenger</td>
<td>1.2</td>
</tr>
<tr>
<td>WeChat (Tencent-owned)</td>
<td>0.9</td>
</tr>
<tr>
<td>Instagram (Facebook-owned)</td>
<td>0.7</td>
</tr>
<tr>
<td>Twitter</td>
<td>0.3</td>
</tr>
<tr>
<td>Snapchat</td>
<td>0.2</td>
</tr>
</tbody>
</table>

Source: Facebook, Google, Magna Global, Snapchat, Twitter
of content. Most of these companies seek to be open and neutral distributors or forums for third-party content, but they increasingly find themselves in situations without clear lines defining how they should curate, edit, or block the independent content of third parties. Even if they can set clear standards for content, it is extremely difficult to build machine-learning algorithms to enforce them without blocking or censoring suitable content.

Public opinion is wide ranging on what social responsibilities these platforms should be held accountable for, and what liability they should have for the content posted to their sites. As with data privacy, there are no right answers. We believe, however, this issue will continue to grow in importance, and the decisions these companies make could have a lasting impact on user trust and engagement, as well as advertiser and media company partnerships.

**Government Regulation: Big Data = Big Brother?**

While governments have had years to develop regulations for financial and payment transactional data, they are just beginning to design regulations for the social, web, and location data being gathered and used in the new digital economy (Exhibit 2).

As of June 2016, 110 countries have data privacy laws, though about 50% of developing nations do not (Exhibit 3). While the European Union (EU) and the United States (to a lesser extent) seek to balance their regulations between governments’ national security interests and consumers’ data privacy protections, Chinese regulation is opaque, with domestic companies largely expected to comply with government and commercial interests at the expense of user privacy.

**The European Union**

Of the many efforts to implement new data privacy laws or strengthen existing regulations, the EU General Data Protection Regulation (GDPR)—which becomes effective in May 2018 and replaces the original EU data privacy regulation codified in 1995—is among the most important.

The goal of the EU GDPR is to “protect all EU citizens from privacy and data breaches in an increasingly data-driven world.” One of the most significant changes in this directive is its expanded territorial reach—it applies to all companies processing the
personal data of EU citizens regardless of the company’s location. Companies that are in breach of the GDPR rules can be fined up to 4% of annual revenues or €20 million, whichever is greater.3

While the new data privacy laws offer greater protections to consumers, many new regulations also strengthen national security. Legislation being considered in Finland, for example, “would give its military and domestic security forces broad access to civilian web communications to gather intelligence.” Countries with long traditions of safeguarding user privacy, such as Germany and the Netherlands, are considering similar measures.4

European regulators are also investigating US technology companies for potentially anti-competitive use of their dominant market positions. The European Commission has opened investigations into Google’s behavior within its Android, AdSense, and search businesses, and recently fined Google €2.42 billion for using its dominant search position to promote its Google Shopping service ahead of competitors. Other European regulations are forcing companies to keep user data stored locally, which creates complications for US cloud infrastructure and software vendors such as Amazon, Microsoft, and Salesforce.com.

While these regulations may not always be in the best interests of consumers, we believe some European regulators are seeking to give some European companies competitive advantages against the rising power of the US technology platforms. This is a growing risk for those leading internet and mobile platforms as the digital economy consolidates around them.

China

In China, the government puts significant demands on internet platforms. The government can suspend and filter content, and the platforms have mostly complied with government demands for personal user data. This creates potential risks for internet companies operating in China. Official censorship threatens many uses of the internet that are fundamental in other parts of the world—the ability for users to express themselves freely and have access to unfettered information.

However, differences in government privacy laws and regulations can also create opportunities and drive innovation. Chinese micro-lenders, for example, use personal transaction data to assess personal risk and provide lending. Such business models could arguably not exist in Europe, where data is more closely regulated and controlled. In addition, the Chinese government has largely supported and developed its own national champions in the internet space by limiting competition from well-funded US companies. China has blocked Facebook since 2009, and Google closed its local search engine in 2010 because of strict censorship rules and attempts made to access users’ personal email data, which Google believed violated its values about freedom of speech. See Exhibit 4 for an in-depth look at how Facebook and Tencent treat data differently.

The net effect of the Chinese regulations has been an advantage to domestic internet companies such as Baidu, Alibaba, and Tencent because they have avoided competition with US-based companies in their home market. This has helped foster innovation and investment in domestic internet firms, and in many cases, we believe the Chinese platforms are among the most innovative globally.

The United States

The United States has been on the forefront of tech innovation and development, but it also has tensions and contradictions as US companies seek to balance data privacy, social responsibility, and government oversight. US technology companies have regularly complied with data requests from the US government (which can number in the tens of thousands per year). At the same time, companies have taken a stance against government access to personal data (for example, the aforementioned San Bernardino case, or encrypted text within messaging apps), and there is an ongoing passionate debate about how much companies should share with government agencies and under what circumstances.

There is historical precedent for US antitrust cases against technology leaders in the past, such as Intel and Microsoft, when they yielded dominant power in the personal computer industry. More recently, there is growing concern in the United States about the power of the internet leaders, and the potentially destructive economic impact ecommerce, artificial intelligence, and online advertising could have on jobs and the viability of other sectors. We believe antitrust cases on these grounds would require the government to rethink whether its mandate is to protect the consumer, jobs, or industry competitors.

The United States has also favored its own industry over those from other countries in some situations. The United States has effectively banned US operators from purchasing telecom equipment from China (Huawei) due to fears of data snooping. Furthermore, some US government officials have accused Europeans of using privacy issues as a form of protectionism to favor their domestic tech companies, and have defended US companies involved in tax liability lawsuits brought in Europe.

While different countries have taken different approaches to data privacy and digital economy regulation, the aggregation of data within the leading internet platforms makes them central to debates about regulation as governments seek to balance the interests of consumers, national security, and domestic competitors.
An ESG Challenge

The data being collected by companies today can be a tremendous source of competitive advantages, innovation, and long-term returns. However, it is also a potential source of risk, including invasive business practices that test user trust, social responsibility for content, and government regulations.

We believe that these issues should be considered within an ESG framework, which considers them not as separate, unrelated questions but as connected to a single theme. Trillions of dollars of market cap is dependent on the ability of tech companies to successfully navigate these issues. At Lazard, our analysis considers these issues within a unified context that we believe is crucial to stock selection in today’s—and tomorrow’s—markets.
This content represents the views of the author(s), and its conclusions may vary from those held elsewhere within Lazard Asset Management. Lazard is committed to giving our investment professionals the autonomy to develop their own investment views, which are informed by a robust exchange of ideas throughout the firm.

Notes
3 EU General Data Protection Regulation, (www.eugdpr.org)

Important Information
Published on 18 September 2017.
This document reflects the views of Lazard Asset Management LLC or its affiliates (“Lazard”) based upon information believed to be reliable as of 17 August 2017. There is no guarantee that any forecast or opinion will be realized. This document is provided by Lazard Asset Management LLC or its affiliates (“Lazard”) for informational purposes only. Nothing herein constitutes investment advice or a recommendation relating to any security, commodity, derivative, investment management service or investment product. Investments in securities, derivatives and commodities involve risk, will fluctuate in price, and may result in losses. Certain assets held in Lazard’s investment portfolios, in particular alternative investment portfolios, can involve high degrees of risk and volatility when compared to other assets. Similarly, certain assets held in Lazard’s investment portfolios may trade in less liquid or efficient markets, which can affect investment performance. Past performance does not guarantee future results. The views expressed herein are subject to change, and may differ from the views of other Lazard investment professionals. This document is intended only for persons residing in jurisdictions where its distribution or availability is consistent with local laws and Lazard’s local regulatory authorizations. Please visit www.lazardassetmanagement.com/globaldisclosure for the specific Lazard entities that have issued this document and the scope of their authorized activities.