BCG
The Boston Consulting Group

BCG Henderson Institute

Bridging the Trust Gap in Personal Data

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

The BCG Henderson Institute is The Boston Consulting Group's internal think tank, dedicated to exploring and developing valuable new insights from business, technology, and science by embracing the powerful technology of ideas. The Institute engages leaders inprovocative discussion and experimentation to expand the boundariesof business theory and practice and to translate innovative ideas from within and beyond business. For more ideas and inspiration from theInstitute, please visit https://www.bcg.com/bcg-henderson-institute/thought-leadership-ideas.aspx.

BRIDGING THE TRUST GAP IN PERSONAL DATA

JOHN ROSE

ALEXANDER LAWRENCE

ELIAS BALTASSIS

March 2018 | The Boston Consulting Group

CONTENTS

INTRODUCTION

IMAGINE A COMPANY THAT zealously and thoughtfully safeguards and marshals the consumer data it holds, for the good of both company and consumer—so much so that consumers preferentially choose to buy products and services from this company and to share relevant data for new and unrelated purposes. Think too about the many companies that have made headlines—and have been punished by consumers and other stakeholders—for doing just the opposite: gathering and using data in ways that distress consumers, often without their permission or even awareness.

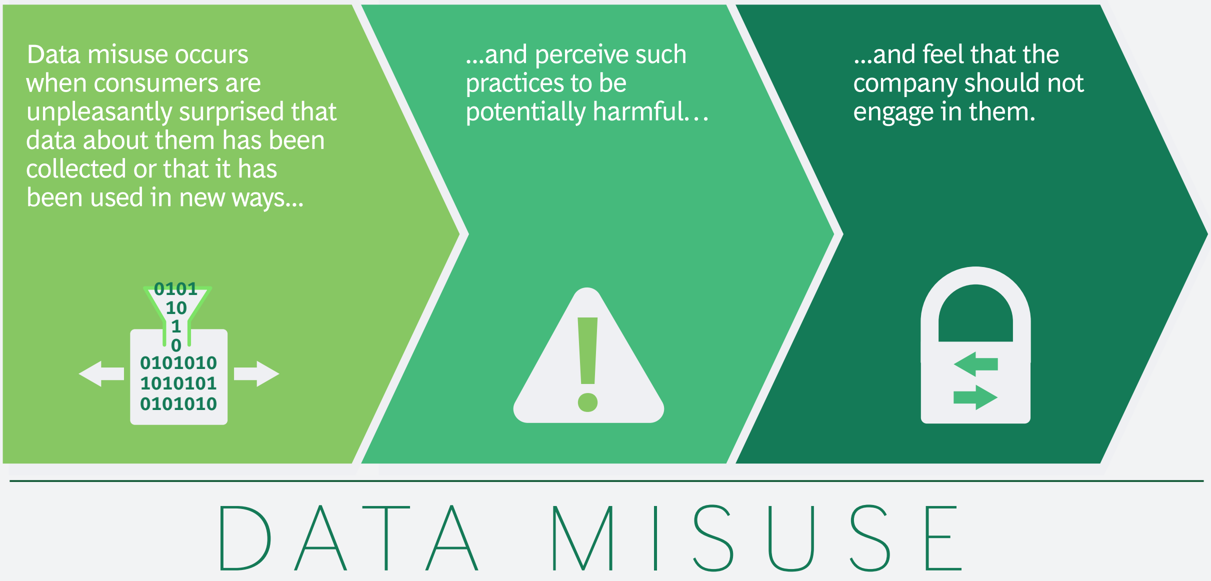
Where a company fits along this spectrum depends on its use of the big data that is increasingly available. But big data has the potential to be both friend and foe. The Boston Consulting Group conservatively estimates that trusted uses of big data and advanced analytics could unlock more than $1 trillion in value annually by 2020. (See "The Value of Our Digital Identity," BCG article, November 2012.) However, recent BCG consumer research has uncovered a previously hidden obstacle to successfully unleashing this enormous opportunity: data misuse.

Data misuse as perceived by consumers is not a legal issue and does not refer to a use of data disclosed in an agreement that almost no one reads when signing up for a credit card, mobile phone, or social media service; it is not even about whether a use actually causes harm to consumers. As Exhibit 1 shows, data misuse occurs when consumers are unpleasantly surprised to learn that data about them has been collected or that it has been used in new ways—that is, outside of the original purpose for which it was gathered—and when they perceive such practices to be potentially harmful and feel that the company should not engage in them. (An example would be when a company originally collected data in order to complete a transaction or ensure that potential customers are good prospects went on to sell that data to third parties or use it for marketing purposes that upset consumers.) Our research suggests that consumers' reaction to data misuse—defined in this way—can cause them to reduce their spending with a company by about one-third.

Companies cannot mitigate this reaction by writing even longer and more complex legal documents for consumers to ignore, or by working even harder to ensure that their company does not run afoul of regulations and legal agreements. Instead, company leaders at the highest levels must develop new ways to manage and use data, rather than confining the discussion to legal or IT, as it is at most companies. Even organizations that use data for completely legal and fully dis-

Exhibit 1 | Data Misuse Is a Hidden Landmine for Companies

The trillion-dollar big data opportunity is at stake


Data misuse occurs when consumers are unpleasantly surprised that data about them has been collected or that it has been used in new ways...
0101
10
1
0
0101010
1010101
0101010
...and perceive such practices to be potentially harmful…
...and feel that the company should not engage in them.
DATA MISUSE

Source: BCG.

closed reasons are on a collision course with their customers. The steps companies take now to assess and address this risk and to engage with their stakeholder communities in this process will confer significant, long-term, and sustainable competitive advantage and head off the looming threat to their earnings performance.

In this report, we explain the perils of misusing data—a data misuse is punished more harshly than a data breach—and the ways in which many companies are setting themselves up to fail: not only are they making missteps by misusing data, they are missing opportunities to use data well and thereby win consumer trust. Trust right now is sorely lacking, but it's entirely possible to win it back, by following best practices that we outline herein. (The chapters of this report were previously published as individual articles on bcg.com.)

So, back to that spectrum of companies and their use of consumer data. Companies at one end are at risk of jeopardizing their revenues while companies at the other end stand to reap rewards. Where does your company fit? Our recently launched Trust and Data Privacy Best-Practice Diagnostic Tool will help you answer that question.

THE HIDDEN LANDMINE IN BIG DATA

It's a simple and logical formula: if consumers believe that you are misusing their data, you lose their trust. And not surprisingly, the many and public instances of data misuse have battered the state of consumer trust overall.

And when consumer trust goes, so does consumer spending. Companies that lose consumer trust also suffer significant revenue loss.

We surveyed consumers in 2013 and again in 2016, and we see the divide between companies and consumers widening when it comes to appropriate use of consumer data. We also see that misusing consumer data has real economic repercussions. Big data capabilities are expanding companies' access to data about consumers and ways of using that data. This expansion opens up possibilities--but our findings show that it also increases opportunities for misuses of consumer data.

The Weakened State of Consumer Trust

Issues of privacy and trust are at the top of consumers' minds. In fact, feelings about these issues have intensified over time.

When we surveyed consumers across 20 countries and multiple generations in 2013, it was clear that they all cared deeply about the expanding use of "their" data. (See *The Trust Advantage: How to Win with Big Data*, BCG Focus, November 2013.) For instance, in every generation and in most countries, consumers were five to ten times more likely to share personal data with an organization if they trusted that the data would not be used to harm them. Moreover, 83% of US consumers agreed that they needed to be cautious about sharing personal data online—again with only small differences across generations and across most of the countries surveyed.

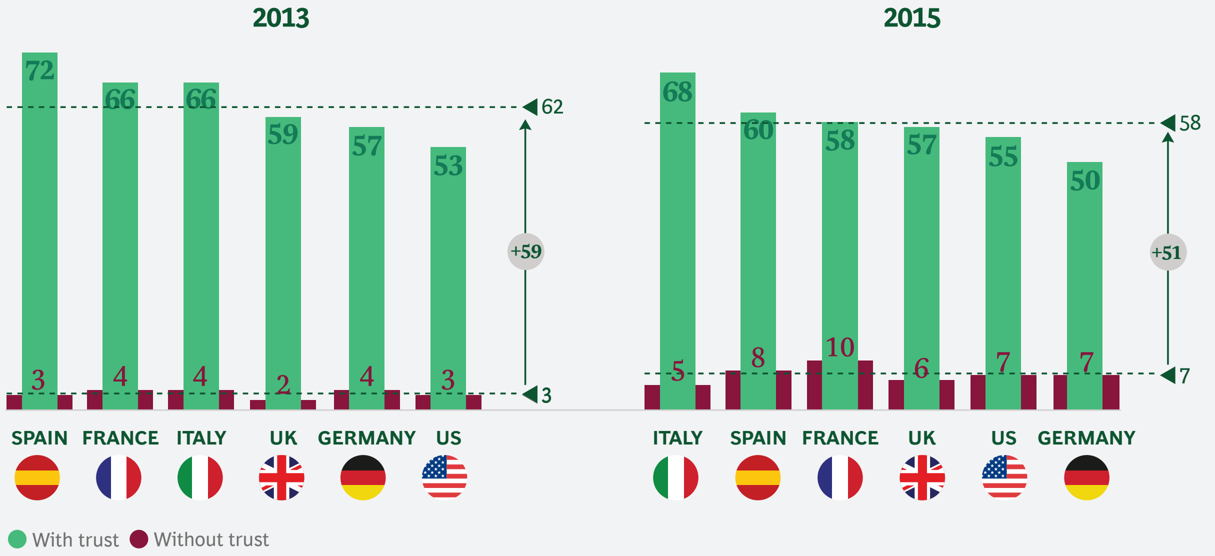
A new BCG survey of 8,000 consumers in the US and five European countries shows that these concerns remain at high levels in most product and service areas.[1] (See Exhibit 2.) Consumers who say they are concerned about the sharing of personal data online increased slightly from 83% to 86% in the US. Four out of five US millennials are similarly concerned. (See Exhibit 3.) Consumer willingness to allow companies to use data in new ways remains roughly five to ten times higher among those who trust a company to prevent harmful uses than among those who do not.

Of greater concern, nearly half the consumers we surveyed believe that companies are neither being honest about their use of data nor taking adequate steps to protect it. In fact, only about 20% of consumers across all the countries surveyed trust companies to "do the right thing" with their data, and approximate-

Exhibit 2 | Generating Trust Increases Access to Data by at Least Five Times

Trust continues to unlock access to consumer data

% OF CONSUMERS WHO WOULD BE WILLING TO ALLOW COMPANIES TO USE DATA ABOUT THEM

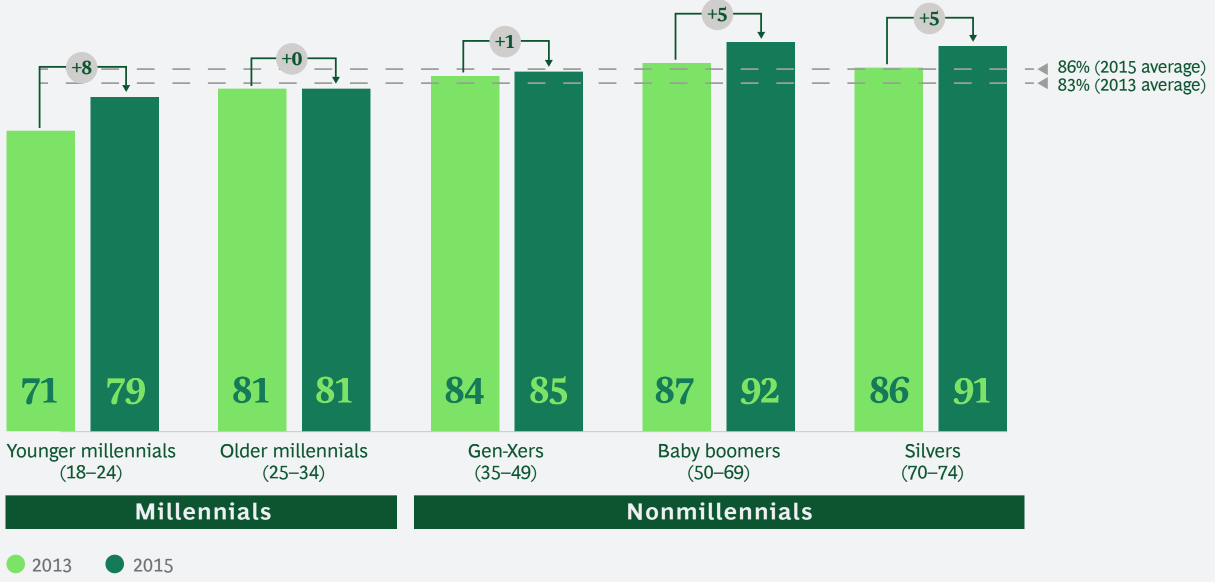


Sources: BCG Global Consumer Sentiment Survey 2013 and BCG Big Data and Trust Consumer Survey 2015.
Note: The exhibit shows survey responses that are comparable for the purposes of demonstrating the effect of trust on consumers' willingness to share personal data. Survey question (green): "If I had the ability to prevent the harmful uses of data, I would be more willing to let companies use data about me." Included are the responses "Agree" or "Strongly agree"—that is, those consumers who are willing to share data when they can trust that the potential harm will be mitigated. Survey question (red): "Data should be used by a company only for the purpose for which it was collected." Included are the responses "Disagree" or "Strongly disagree"—that is, those consumers who are willing to share data even when they cannot trust the data will not be used in contexts in which it could cause harm.

Exhibit 3 | All US Age Groups Are Concerned About Sharing Personal Data Online

Concern is increasing at the fastest rate among younger millennials

% OF CONSUMERS WHO AGREE THAT THEY HAVE TO BE CAUTIOUS ABOUT SHARING PERSONAL INFORMATION ONLINE



Sources: BCG Global Consumer Sentiment Survey 2013 and BCG Big Data and Trust Consumer Survey 2015.
Note: Survey question: "How much do you agree or disagree with the following statement: 'You have to be cautious about sharing personal information online'? Answer using a scale from 1 to 5, where 1 means 'Strongly disagree' and 5 means 'Strongly agree.'" The chart shows respondents who answered 4 ("Agree") or 5 ("Strongly agree").

ly 30% across all the countries surveyed believe that companies will not do the right thing. (See Exhibit 4.) This is particularly troubling given that 71% to 79% of the surveyed consumers said they would be unlikely to share or let data about them be used by a company they did not trust. (See Exhibit 5.)

Because consumers are already skeptical that companies will be honest about, protect, or otherwise do the right thing with existing uses of data about them, they are primed to view most new uses of data with significant distrust—and, even worse, as probable misuses.

The Cost of Crossing the Line

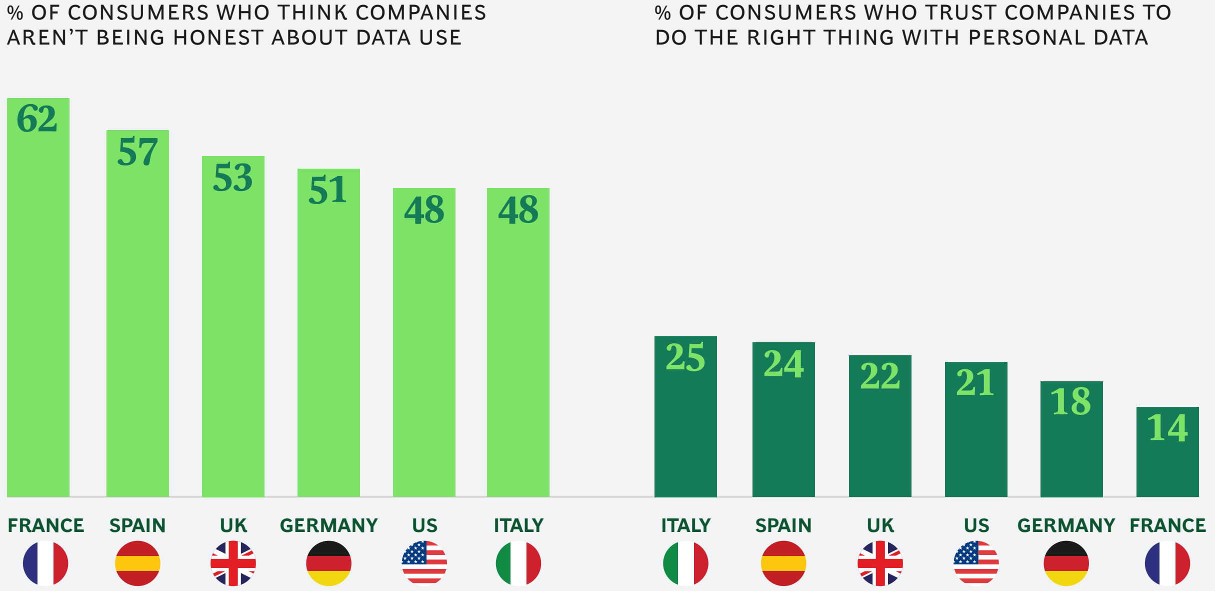
Companies face a hefty penalty for doing the wrong thing with consumer data. They lose access to five to ten times the data they could have used had they excelled at creating trust. What's new from our recent research is the real revenue impact of that loss of trust.

Consumers are now demonstrating that they will "vote with their feet"—stopping or significantly reducing spending—if they believe that a company has misused data about them or other consumers. As noted, this can have dramatic results: in the US, customers who are aware of and concerned about a data misuse reduce their spending by about a third in the first year. Overall, that means a 5% to 8% loss of total company revenues in the first year after these customers have stopped or reduced their spending, dropping to a 3% to 5% loss in year two. (See Exhibit 6.) (The overall revenue loss is a function of the much larger size of the total user population.) However, as consumer awareness and concerns increase, we believe that data misuse has the potential to cut overall revenues by 10% to 25% in year one, dropping to 5% to 15% in year two. While differences exist between the US and the European countries surveyed, the potential revenue losses are comparable.

This consumer reaction to data misuse is significantly greater than the reaction to data breaches or other cybersecurity events. In fact, 25% more US consumers have reacted to a data misuse than to a data breach by stopping or reducing their spending.

Exhibit 4 | Consumers Are Primed to Suspect Data Misuse

Distrust is high among those in the US and Europe

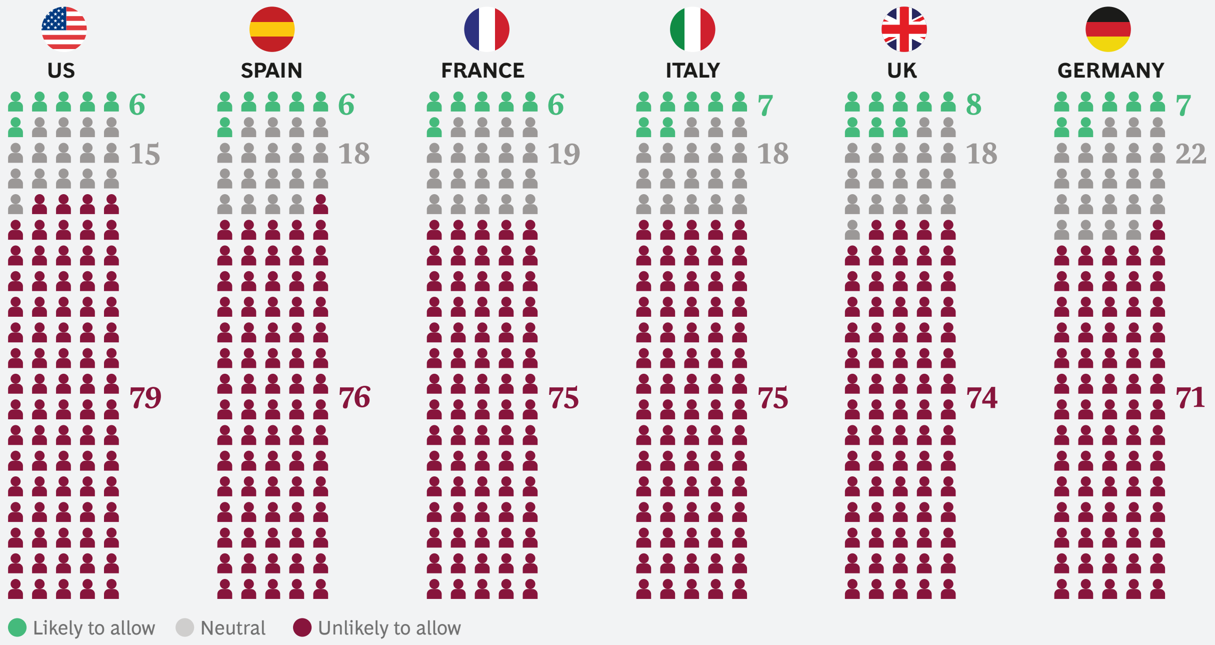


Source: BCG Big Data and Trust Consumer Survey 2015.
Note: Survey question: "How much do you agree or disagree with each of the following statements? Answer using a scale from 1 to 10, where 1 means 'Do not agree at all' and 10 means 'Agree completely.'" The charts show respondents who answered 8, 9, or 10 to the following survey prompts: "Companies don't tell you how they really use the personal data they collect" (left) and "I trust companies and organizations to do the right thing with the data they collect" (right).

Exhibit 5 | Distrust Drastically Limits Access to Consumer Data

Consumers offer much less data about themselves when they do not trust a company

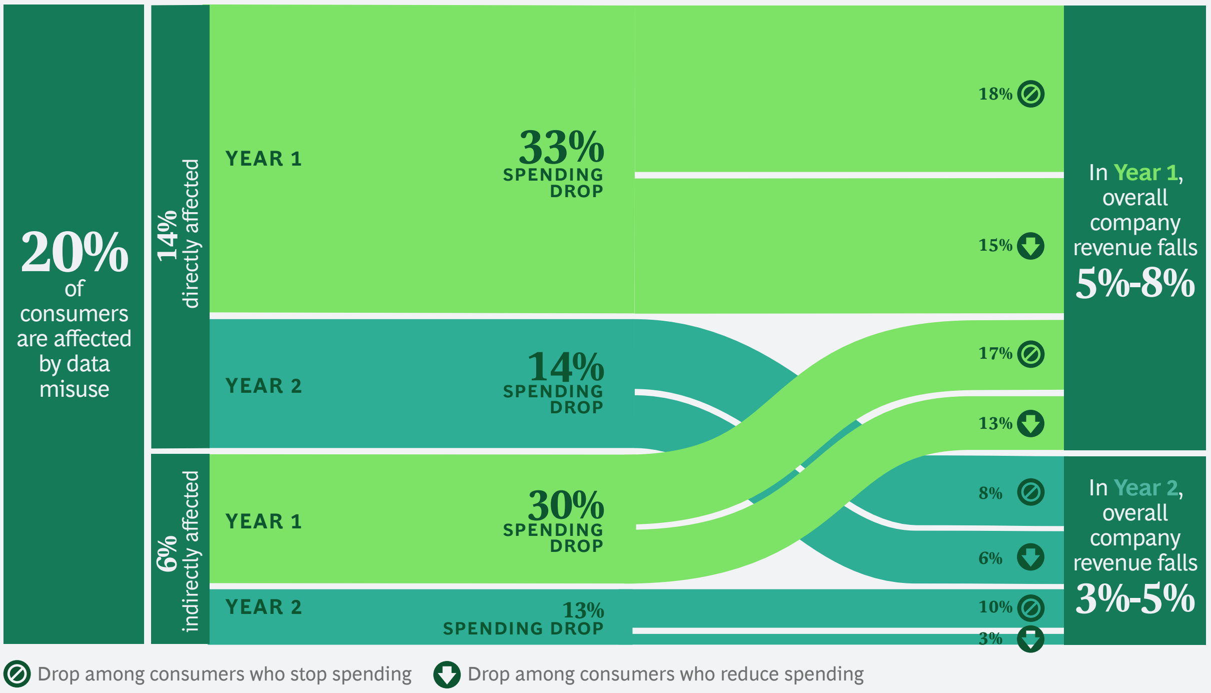
% OF CONSUMERS WHO WOULD ALLOW A COMPANY THAT THEY DO NOT TRUST TO USE DATA ABOUT THEM



Source: BCG Big Data and Trust Consumer Survey 2015.
Note: Survey question: "How much do you agree or disagree with each of the following statements? Answer using a scale from 1 to 10, where 1 means 'Do not agree at all' and 10 means 'Agree completely.'" The charts show respondents who answered 8, 9, or 10 (likely to allow); 4, 5, 6, or 7 (neutral); and 1, 2, or 3 (unlikely to allow).

Exhibit 6 | Data Misuse Has a High Cost

Misuse costs companies one-third of revenue from affected US customers in the first year



Source: BCG Big Data and Trust Consumer Survey 2015.
Note: The drop in spending reflects the share of company revenue at the time of a data misuse that is subsequently lost.

The impact of data misuse on a company is a function of several factors:

- **The Size of the Population Affected.** Our survey suggests that 20% of US consumers believe they have been affected by data misuse. This group comprises 14% who are aware of a misuse involving data about them (those "directly affected") and 6% who are aware of a misuse involving data about other consumers (those "indirectly affected"). We expect this combined population to significantly increase over the coming years. (See Exhibit 7.)

- **The Behavior of the Affected Population.** Of those surveyed in the US who believe they were directly affected, 76% took some sort of action: half cut their spending by 56% on average; the other half stopped using the company's services entirely. Combined, the actions of these two groups of directly affected consumers led to a 33% drop in the company's revenues in the first year. Of those indirectly affected, 71% took some sort of action: three-fifths reduced their spending by an average of 48%, while two-fifths stopped using the company's services entirely. The actions of these two groups of indirectly affected consumers led to a year-one reduction in spending of 30%.

- **The Passage of Time.** By the end of the first year, many of the consumers who had abandoned the company returned, reducing the impact in year two. In the US, only 8% of the reduction in revenues resulting from the actions of the directly affected population, and 7% of the reduction in revenues resulting from the actions of the indirectly affected population, endured past the end of year two. By year three, we would expect the balance to be restored—assuming the company does not again misuse customers' data.

- **The Geographic Area Affected.** This is not a geographically isolated phenomenon. As noted above, companies experience similar levels of economic damage

Exhibit 7 | 20% of US Consumers Have Perceived a Data Misuse
Over the next five years, the number of affected consumers could more than double

We predict that the number of consumers who perceive a data misuse will **dramatically increase** over the coming years as a result of rising **press coverage** and exploding **social media use**.
NOW
THE FUTURE
● Directly affected
● Indirectly affected

Source: BCG Big Data and Trust Consumer Survey.

from data misuse in the US and Europe. More than one-third of revenues from directly and indirectly affected consumers will be lost during the first year, with the reaction slightly harsher in Europe than in the US. About one-tenth of revenues from these consumers will be lost during the second year, with differences between Europe and the US beginning to level out. (See Exhibit 8.)

Why the Cost of Crossing the Line Will Increase

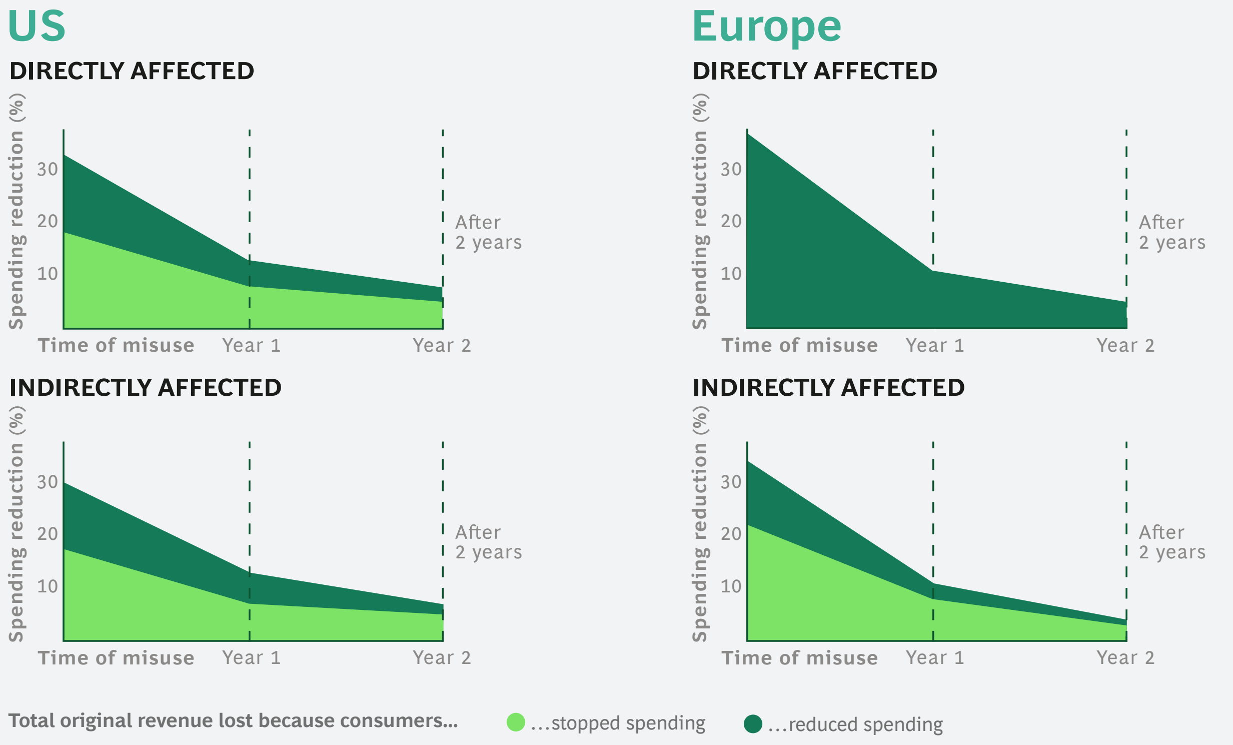
A worrisome trend—and one that will increase the potential impact of data misuse—is the increasing attention that the phenomenon is receiving in traditional and social media. One example is the uproar that greeted Uber's disclosure of the uses of its "God view" capabilities. This software functionality allows the company to track the location of drivers in real time and tie that data to their passengers. While the feature can be seen as relatively benign in the context of fleet management, many considered Uber's internal data-sharing practices to be an invasion of privacy (there were even allegations that Uber had broadcast the data on giant screens at parties in cities where it was launching a new service). It is worth noting that much of Uber's collection and use of data has been within the bounds of both the law and the company's privacy policy, as is the case with many perceived incidents of data misuse.

As coverage of data misuse becomes the new normal in traditional and social media, the number of consumers who become aware that data about them is being collected and used in new ways, who consider those uses to be potentially harmful, and who feel that companies should not engage in such practices is likely to increase—and with it the economic impact of any spending reductions that consumers may make in response.

FEW companies see the landmines that are looming under the surface of their attempts to use data in new ways. They overlook these risks because their focus is on data

EXHIBIT 8 | Data Misuse Causes Similar Economic Damage in the US and Europe

European consumers have a slightly harsher reaction to data misuse than those in the US



Source: BCG Big Data and Trust Consumer Survey 2015.

privacy—a necessary requirement in an intense and rapidly changing regulatory environment. In the process, however, they are overlooking the needs of their customers, who define data misuse on the basis of their perception of right and wrong, not on the basis of regulatory rules or legal agreements. Make no mistake, this strategic blindness will lead to a painful loss of revenues and customers.

As we will discuss in the next chapter, most companies are poised to fail in their pursuit of new data uses. In fact, they have set themselves on a recklessly conservative path, which is leading them to unnecessarily limit their own opportunities while at the same time ensuring that they act in ways that engender the negative consumer reactions they hope to avoid. By focusing privacy and data stewardship practices on the regulations and guidelines that have arisen around big data and advanced analytics—many of which were designed to protect consumers—companies are creating a gap between themselves and their customers. The economic harm that is likely to result is something that few if any C-suite executives can afford to disregard.

Instead, companies need to fundamentally change their approach to data stewardship. They can build consumer trust by making significant improvements in the four main dimensions of robust data stewardship: internal policies and practices, current and new data usage, transparency about current practices, and usage-specific notification and permissions. Adopting best practices in these areas will not only help companies avoid the pitfalls of perceived data misuse but also enable them to expand the range of opportunities they can pursue. Ultimately, companies will foster a broader and deeper level of consumer trust.

[1] The survey was conducted in November and December 2015 in France, Germany, Italy, Spain, the UK, and the US.

WHY COMPANIES ARE POISED TO FAIL WITH BIG DATA

Companies' data stewardship practices and consumers' expectations are fundamentally at odds. Most companies approach privacy and data usage from a narrow legal or regulatory perspective. They ask whether their data collection and management practices are consistent with laws and regulations and meet disclosure requirements. Unfortunately for most companies, consumers take a wider and much less legalistic approach to these issues. They want to be informed about how companies gather and safeguard data about them, and they want to understand the different ways in which companies *use* personal data. Additionally, they want that information delivered in clear language.

The lack of alignment between companies and consumers about data privacy has real consequences. When consumers perceive data misuse—when they are unpleasantly surprised by the collection or new use of personal data—they either reduce their spending drastically or boycott a company's products and services altogether.

In this chapter, we highlight the results of a recent global survey of the data stewardship practices of 140 companies in eight industries. Our survey data suggests that most companies are being *recklessly conservative*: they are failing to pursue new uses of data that consumers are actually open to. When they do pursue a new use, they typically don't feel the need to inform and educate their customers or to ask for permission—something most consumers clearly want. With each mistake, companies are slowly but surely setting themselves up to fail with big data.

The Landscape of Data Stewardship

The requirements of data stewardship can be grouped into four major areas. Good performance in each will prove critical to capturing the value that lies in acceptable new uses of data and to avoiding the real economic harm of data misuse. However, while many companies are executing well in one or two areas, few—if any—are doing so in all of them.

Internal Policies and Procedures. Companies often do a great deal to document how they handle data, through public privacy policies and internal procedures governing data collection, management, and usage. We see a large gap, however, in the involvement of senior executives up front in creating and enforcing data privacy policies and procedures. That's a problem given the major business implications of the adverse reactions that customers might have to these decisions later on.

First, the good news: 76% of the companies we surveyed have privacy policies that explain how they collect, manage, and use consumer data; 54% have a separate and distinct set of internal guiding principles for how to use that data. Companies in the insurance industry are the most likely to have both privacy policies (94%) and guiding principles (76%), while consumer companies show the lowest frequency of having privacy policies (64%) and energy companies show the lowest frequency of having guiding principles (38%).

Few of the companies that have these policies and principles create or enforce them with C-suite or senior executive involvement, however. They may be adequately managing legal and technical risk, but they are not managing consumer risk—the source of the greatest upside and downside potential.

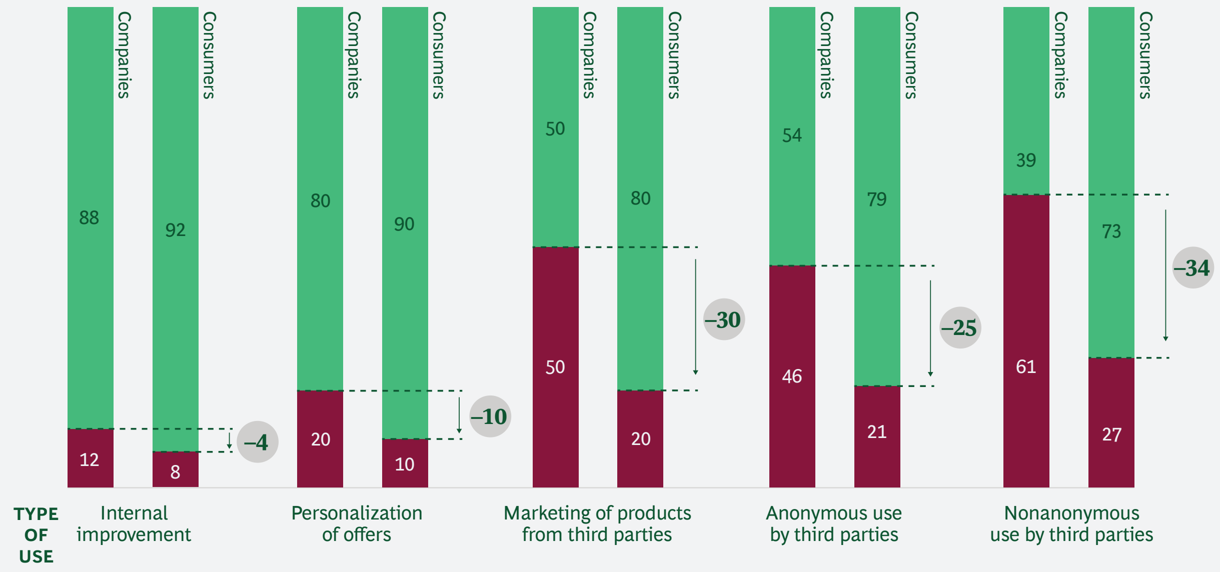
Of companies with privacy policies, 73% make legal or IT teams responsible, while only 22% give the responsibility to operating or executive teams; of companies with guiding principles, 59% make legal or IT teams responsible and just 34% assign responsibility to operating or executive teams. Industrial goods and insurance companies are the least likely to make operating or executive teams responsible for their guiding principles (22% and 23%, respectively); in the consumer, health care, energy, and technology, media, and telecommunications (TMT) industries, at least 40% of the surveyed companies make guiding principles the responsibility of operating or executive teams.

Data Use and Collection Practices. One of the most surprising findings of our survey was the degree to which companies pursue fewer uses of data than consumers are comfortable with. (See Exhibit 9.)

We asked consumers whether it was acceptable for companies to tap personal data for five types of use: the internal improvement of products and services, the personalization of offers, the marketing of products from third parties, the anonymous use by third parties (the data is not linked to a consumer's name), and the nonanonymous use by third parties (the data is linked to a consumer's name). The vast majority of consumers felt company use of data was acceptable in all cases, if (and only if) companies effectively informed them (transparency) and offered them some form

Exhibit 9 | Companies Are Being Recklessly Conservative About Data Usage

Companies are failing to use data for new purposes that are acceptable to consumers



🟢 % who believe companies can use consumer data for the stated purpose if consumers are properly engaged
🔴 % who believe companies cannot use consumer data for the stated purpose regardless of consumer engagement

Sources: BCG Big Data and Trust Consumer Survey 2015 and BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "For each of these new uses, what do you believe your company must do to gain customer consent to use the data?" and "Which approval should an organization have from you for the following uses?"

of control (permissions). The use that drew the most negative response—use of nonanonymous data, or data linked to a consumer's name, by third parties—was nonetheless acceptable to 73% of consumer respondents.

We also gathered company opinions regarding the same types of use. Companies are generally comfortable using consumer data for internal uses, with 88% thinking that use for internal improvement is acceptable and 80% thinking that use for personalizing offers is acceptable. When it comes to third-party uses, however, companies are extremely—and, we argue, overly—cautious. Companies are 25 to 34 percentage points less likely than consumers to think a third-party use of consumer data is acceptable. For example, 50% of companies think consumer data could be used to market products from third parties, while 80% of consumers find this use acceptable. This caution is echoed across industries. For every industry surveyed, at least 40% of companies indicated that, in general, third-party data uses are unacceptable.

When it comes to third-party data uses, companies are overly cautious.

We believe companies are conservative in their pursuit of new data uses, in the hope that this will insulate them from risk. (The same finding applies to data collection as well.) But this is a misguided notion in terms of consumer perception.

Transparency About Current Practices. Companies frequently fail to make sure consumers and prominent stakeholders are aware of and fully understand the data that companies hold and the ways they use it. Companies often do make important information about their data practices available, but they usually do so in a way that is ineffective. In general, they require consumers to take the initiative. Even when consumers do go looking for this information, they do not absorb nearly as much of the details as companies think, or hope, they do.

Most companies overwhelmingly rely on "pull" methods of notifying and engaging their customers, forcing customers to find or request important information about data privacy. Forty-one percent of companies make their privacy policy available to customers who request it, and 62% of companies post the policy on their website. These figures are 44% and 20%, respectively, for information about the personal data a company holds and 49% and 24% for information about how companies use such data.

Far fewer companies engage their customers via "push" methods to actively send out important information:

- No companies in our survey send regular updates via e-mail or letter regarding their privacy policies or the data they hold about their customers.

- Only 8% of companies regularly send letters and only 4% regularly send e-mails about how they use consumer data. (These companies are mainly in the financial, insurance, and TMT industries.)

- Only 16% send an update letter and 15% send an update e-mail when there is a change to their privacy policy, and those figures drop to 6% and 8%, respectively, for data held about consumers and 5% and 6% for how that data is used.

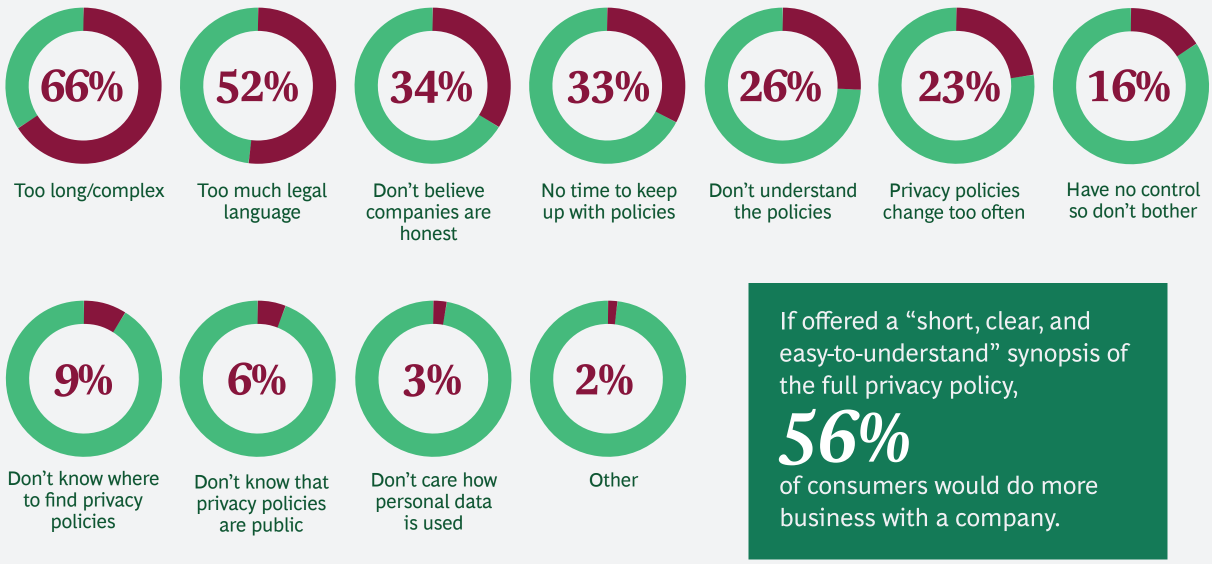
- Fourteen percent of companies said they had no way for their customers to view their privacy policies; this number grew to 38% and 33%, respectively, for the data that companies hold about consumers and how they use that data.

As a consequence, companies think that twice as many consumers, on average, understand their data stewardship practices at a detailed level as actually do. (See Exhibits 10 and 11.) Company and consumer estimates are in alignment when it comes to the percentage of consumers who are simply aware of privacy policies, but the fact that the figure is below 50% shows how ineffective companies are at getting this information out to their customers. Even less promising is the fact that only 10% of consumers said they believe they know what data a company holds about

Exhibit 10 | Consumers Do Not Read Privacy Policies

Plain-language versions of privacy documents can increase consumer spending

REASONS RESPONDENTS DO NOT READ PRIVACY POLICIES

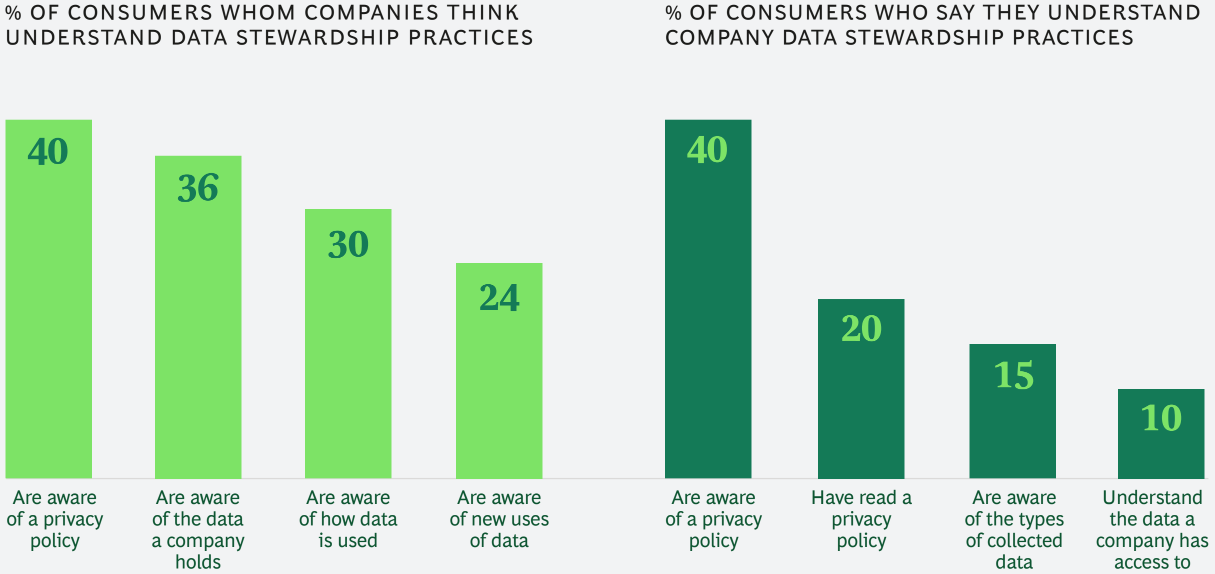


If offered a "short, clear, and easy-to-understand" synopsis of the full privacy policy, ***56%*** of consumers would do more business with a company.

Source: BCG Big Data and Trust Consumer Survey 2015.
Note: Survey questions: "What are the major reasons you tend not to read these privacy policies?" and "If a company whose services or products you use were to offer a short, clear, and easy-to-understand policy regarding how it uses your personal data, how much would this influence you to do business with that company?"

Exhibit 11 | A Knowledge Gap Exists Between Companies and Consumers

Companies think that more consumers understand data stewardship practices as really do



Sources: BCG Big Data and Trust Consumer Survey 2015 and BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "Are you aware of the privacy policies that describe how the companies you deal with treat your consumer data?"; "Have you read the privacy policies of the companies you deal with?"; "Do the companies you deal with list (online or in paper form) the data they collect about you?"; "Do you know which private data the companies you deal with have access to?"; and "To the best of your knowledge, what percentage of your customers are aware of your privacy policy, the data your company holds about them, how your company uses the data you hold, and new uses of data?"

them, even though companies estimated that 36% of consumers have this knowledge.

This lack of knowledge represents a significant issue for companies. Given that the main cause of perceived data misuse is unpleasantly surprised consumers, the current lack of consumer understanding represents a significant risk. In fact, the absence of a committed effort to create transparency is reckless.

At present, organizations are not even getting recognition or credit for their conservative data usage. While only 11% of companies reported allowing third parties to use data on an anonymous basis and 4% reported allowing third parties to use data on a nonanonymous basis, consumers thought that 21% and 19% of companies, respectively, allow such uses. If companies cannot successfully educate consumers about how they use data about them, they are doomed to inhabit a world in which consumers presume that every new use they find out about is a misuse.

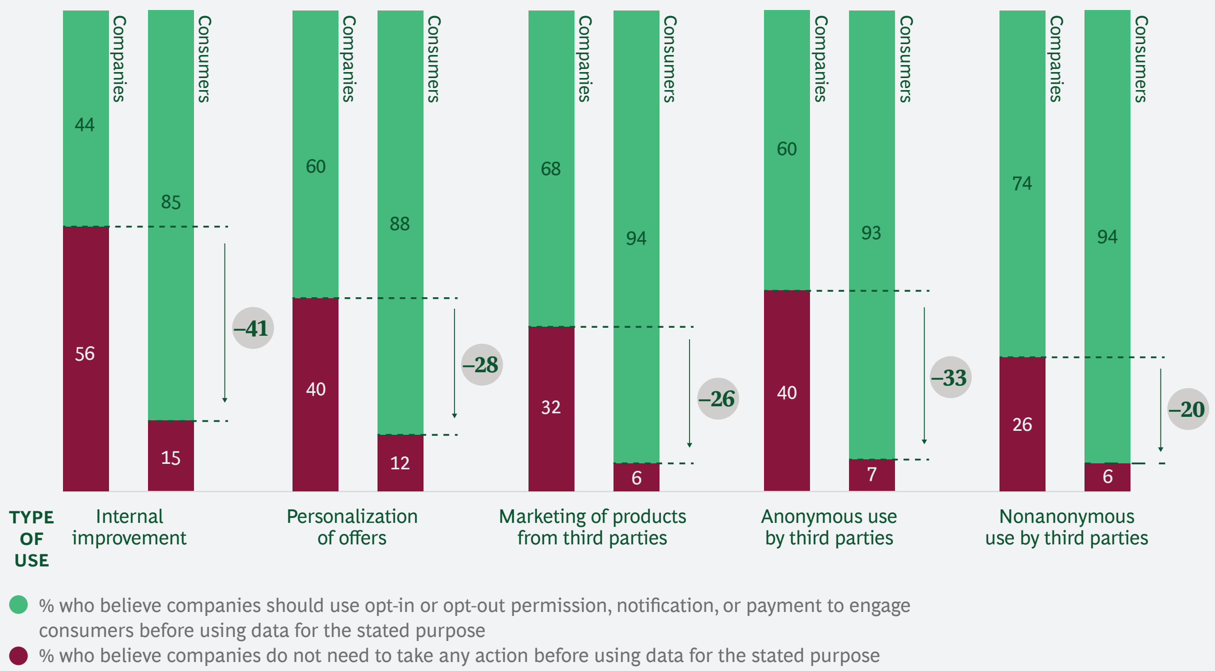
Notifications and Permissions for New Data Uses. Finally, few companies actively engage with customers about new uses of personal data or allow them to influence how companies use it. To assess company performance in this area, we asked companies about the same five types of use: the internal improvement of products and services, the personalization of offers, the marketing of products from third parties, the anonymous use by third parties, and the nonanonymous use by third parties. We offered a choice between five permission or notification methods: opt-in permission, opt-out permission, notification, payment for access to data, or no notification or permission required.

Of the companies in our survey, 26% to 56% thought that they did not need to take any action before using data for each of the five types of use. (The sentiment was highest among companies in the consumer and TMT industries.) This compares with only 6% to 15% of consumers. Indeed, the vast majority of consumers want companies to take active steps to secure notification or permission. (See Exhibit 12.)

More than 60% of consumers believed that opt-in or opt-out permissions should be re-

Exhibit 12 | Companies Are Not Being Transparent with Consumers About Data Use

They are recklessly disregarding the notifications and permissions that consumers want



● % who believe companies should use opt-in or opt-out permission, notification, or payment to engage consumers before using data for the stated purpose

● % who believe companies do not need to take any action before using data for the stated purpose

Sources: BCG Big Data and Trust Consumer Survey 2015 and BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "For each of these new uses, what do you believe your company must do to gain customer consent to use the data?" and "Which approval should an organization have from you for the following uses?"

quired for all five types of use. Only two uses of data were acceptable to more than 10% of consumers without being preceded by action on the company's part: internal improvement and personalization of offers. Opt-in permission was the top choice among companies for marketing third-party products and allowing third parties to use consumer data on a non-anonymous basis. Paying consumers for access to data was by far the least popular option, with no more than 3% of companies thinking it was necessary.

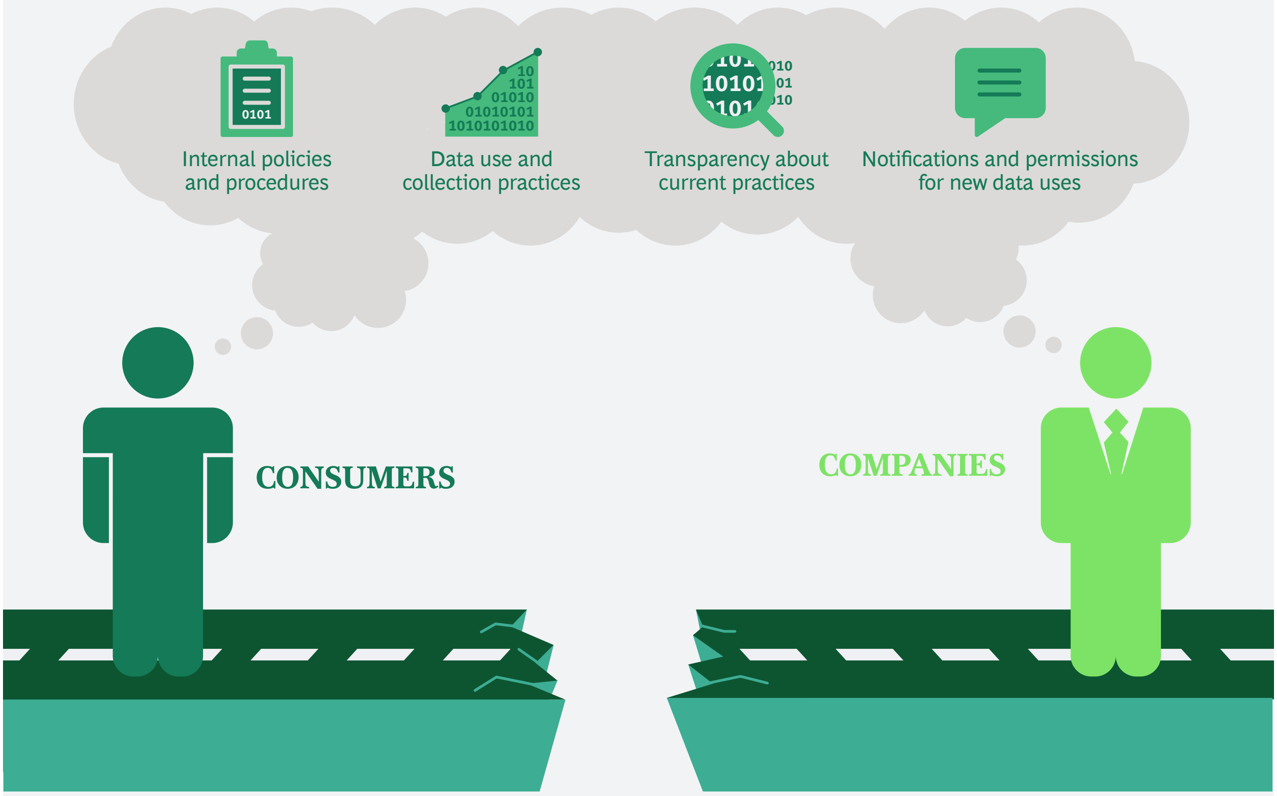
To study how companies engage with customers about new uses of data, we also investigated whether companies offer customers ways to change or control the data that's collected about them or how it's used. Only 4% of companies offer their customers control over what data they collect and manage, and 4% offer control over how they use personal data.

There is no easier way for a company to be perceived as misusing data—and therefore to lose significant business—than by failing to engage with consumers about data use in the way that they expect. Actively engaging consumers through opt-in or opt-out permissions gives them the chance to say no, of course. But our research clearly shows that most consumers will allow most uses of data about them, particularly if things are explained in plain language rather than tech-speak or legalese.

The Consequences of Poor Data Stewardship

Companies are standing on the edge of a precipice. They are not showing consumers how seriously they take the issues of trust and privacy. They are failing to pursue profitable uses of data that consumers would find acceptable, and they are neglecting to actively and transparently educate consumers about how they use data. Finally, they are not engaging with consumers about new data uses in the ways consumers expect. Exhibits 13 and 14 illustrate the divide.

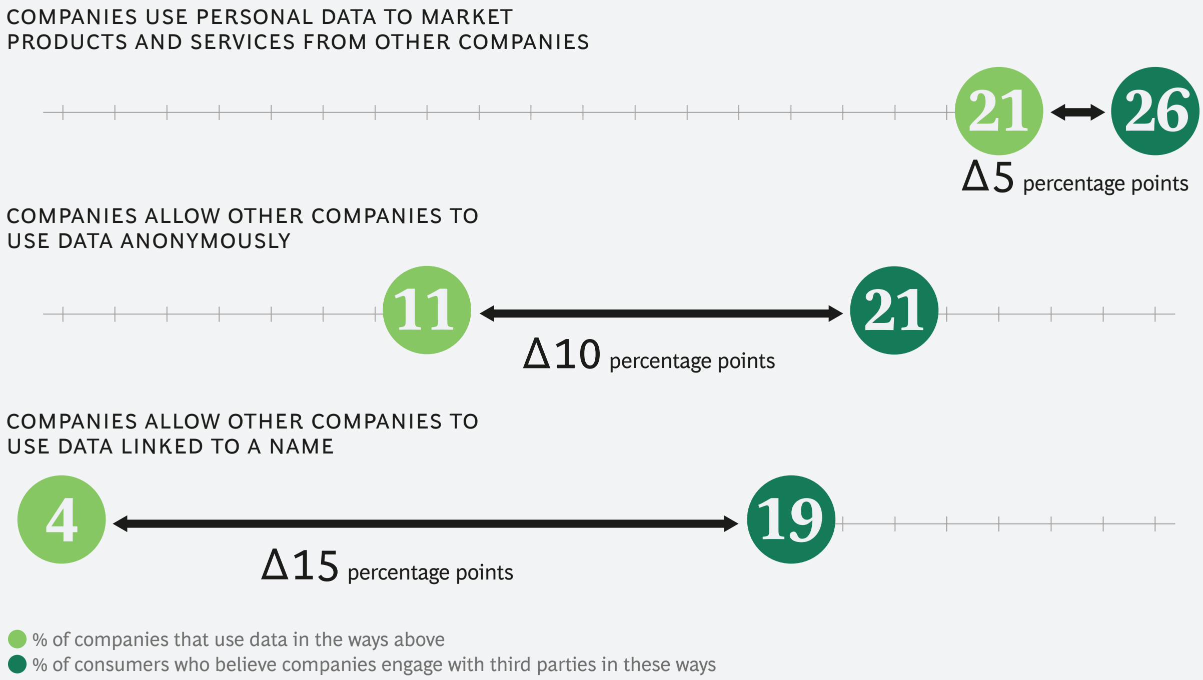
Exhibit 13 | But Data Stewardship Is Critically Flawed at Many Companies
Consumer expectations are disconnected from company practices


0101
Internal policies and procedures
10
101
01010
01010101
1010101010
Data use and collection practices
10101
Transparency about current practices
Notifications and permissions for new data uses
CONSUMERS
COMPANIES

Source: BCG.

Exhibit 14 | Consumers Don’t Understand How Companies Actually Use Data

Consumers overestimate how often third parties use personal data



Sources: BCG Big Data and Trust Consumer Survey 2015 and BCG Big Data and Trust Company Survey 2015. The 2015 Company Survey surveyed 140 companies in eight industries.
Note: Survey questions: “How does your company use this customer data?” and “How do you believe these companies use your personal data?”

The wonder, then, is not that 20% of consumers today have perceived some sort of data misuse, but that the figure is not significantly higher. Data misuse is subjective, which means companies must not only perform much better at data privacy than their competitors but also be seen to take actions that reflect consumer expectations. In the next chapter, we will discuss best practices that can help companies realign themselves with consumers. The competitive advantage they gain will allow them to maximize the potential value promised by big data and help them avoid the pitfalls of perceived data misuse.

HOW TO BECOME A TRUSTED DATA STEWARD

Only about 20% of consumers say that they trust companies to do the right thing with their personal data, and more than half think that companies aren't honest about their data use. Such mistrust translates into damage to a brand's reputation and a quantifiable decline in revenue; consumers who perceive that a company has misused data will cut or curtail their spending with that company, as the previous chapters have shown.

Companies must become trusted data stewards. Few have attained that status.

Consider the opposite scenario, though. Our research, which included surveys of companies and consumers, found that consumers are more willing to do business with companies they trust to manage their data. It stands to reason that as consumers decrease spending with companies they don't trust, they will increase it with those they do. So, both to avoid the looming downsides of poor data use and to capture the upside potential of optimal data use, companies must be able to prove to consumers that they can manage data well. They must become trusted data stewards.

Few companies have attained that status. To do so, they must establish a set of best practices and work to embed a new mindset about consumer data usage: that companies themselves own the responsibility of ensuring that consumers and other stakeholders (such as regulators) fully understand the collection and use of consumer data. This article outlines the best practices required to achieve trusted data stewardship—both internally focused practices that define how a company collects, manages, and uses data and externally focused practices that establish how it engages with its stakeholders about its collection and use of data. (See Exhibit 15.) Further, we have developed a diagnostic that companies can use to assess their progress relative to both competitors and state-of-the-art data stewardship benchmarks. (See the sidebar, "What Is a Trusted Data Steward? Where Does My Company Stand?")

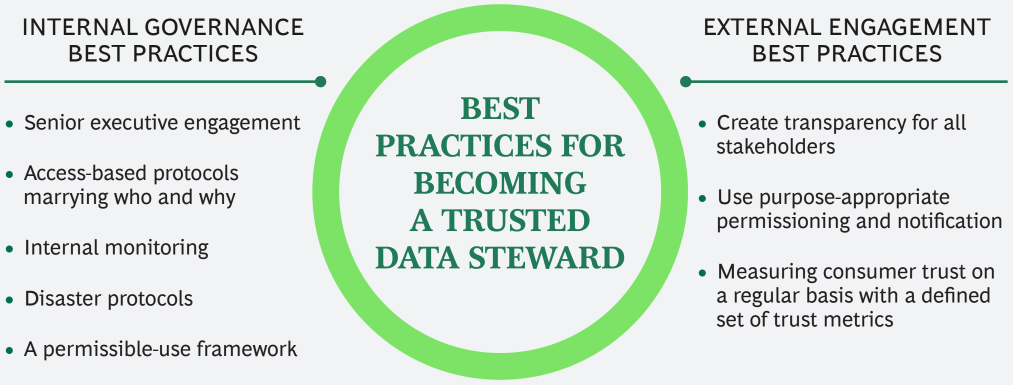
Internally Focused Practices

Becoming a trusted data steward begins at home; companies can establish—or enhance—best practices internally, in several ways.

Ensuring Engagement by Senior Line Executives. Senior line executives should be actively involved in establishing policies and principles. They need to determine overall policy and approve both legal-language and

Exhibit 15 | Both Internal and External Best Practices Matter

Successful execution creates a sustainable trust advantage



INTERNAL GOVERNANCE BEST PRACTICES

- Senior executive engagement
- Access-based protocols marrying who and why
- Internal monitoring
- Disaster protocols
- A permissible-use framework

BEST PRACTICES FOR BECOMING A TRUSTED DATA STEWARD

EXTERNAL ENGAGEMENT BEST PRACTICES

- Create transparency for all stakeholders
- Use purpose-appropriate permissioning and notification
- Measuring consumer trust on a regular basis with a defined set of trust metrics

Source: BCG.

plain-language versions. Plain language matters—consumers would be 56% more likely to do business with companies that offer a short, clear, and easy-to-understand version of their full privacy policies. (See “Data Misuse and Stewardship by the Numbers,” BCG slideshow, October 2016.)

However, in most companies senior line executives are not substantively engaged in policy and procedure. Instead, responsibility is delegated to the legal and IT teams. (See Exhibits 16 and 17.) These teams should be involved, of course; they have the expertise to address legal and regulatory issues and cybersecurity. But the collection and use of consumer data directly affect brand value, market share, and revenue growth through consumer and stakeholder perceptions of these actions. So, these issues require active line guidance and decision making.

Consider the situation Google encountered when the news of Google Maps’ true scope emerged. While Google cars were collecting data for Street View, they were also grabbing data from home Wi-Fi networks, including passwords and e-mails, and creating individually identifiable consumer profiles. Google subsequently admitted that it should have in-

WHAT IS A TRUSTED DATA STEWARD? WHERE DOES MY COMPANY STAND?

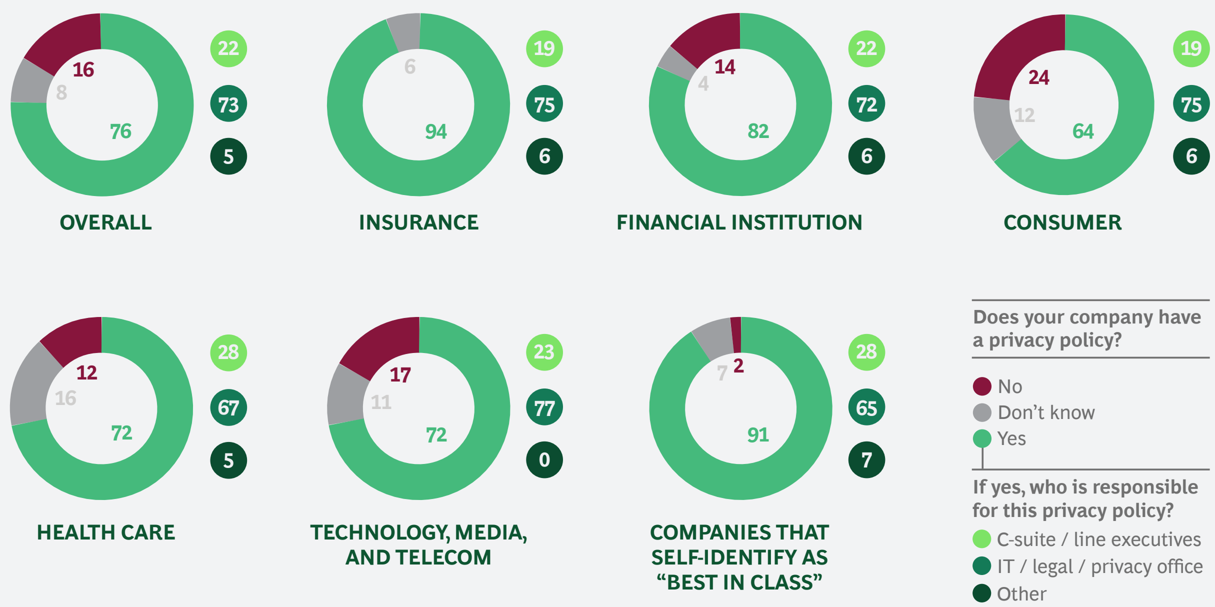
A company that is a trusted data steward manages the collection of consumer data even before the collection occurs: Which data will we gather and why? How will we ensure that consumers understand and approve our data capture? Finely tuned management must continue, as the gathered data is properly stored, secured, and repurposed, always with transparency and adherence to policies and procedures that govern access, notifications, and permissions. A trusted data steward also stands ready to address any real or perceived misuses of consumer data, and it measures and shares its performance on all fronts.

Our accompanying online diagnostic, called the Trust and Data Privacy Best-Practice Diagnostic Tool, allows companies to assess their data stewardship strengths and weaknesses and their performance versus industry peers. Answering a few questions will allow companies to gauge their potential trust risk—and reward.

Exhibit 16 | Few Companies Have Senior-Executive-Level Oversight of Privacy Policies

Responsibility is vested in IT and legal instead

EXISTENCE OF AND RESPONSIBILITY FOR PRIVACY POLICIES BY INDUSTRY (%)

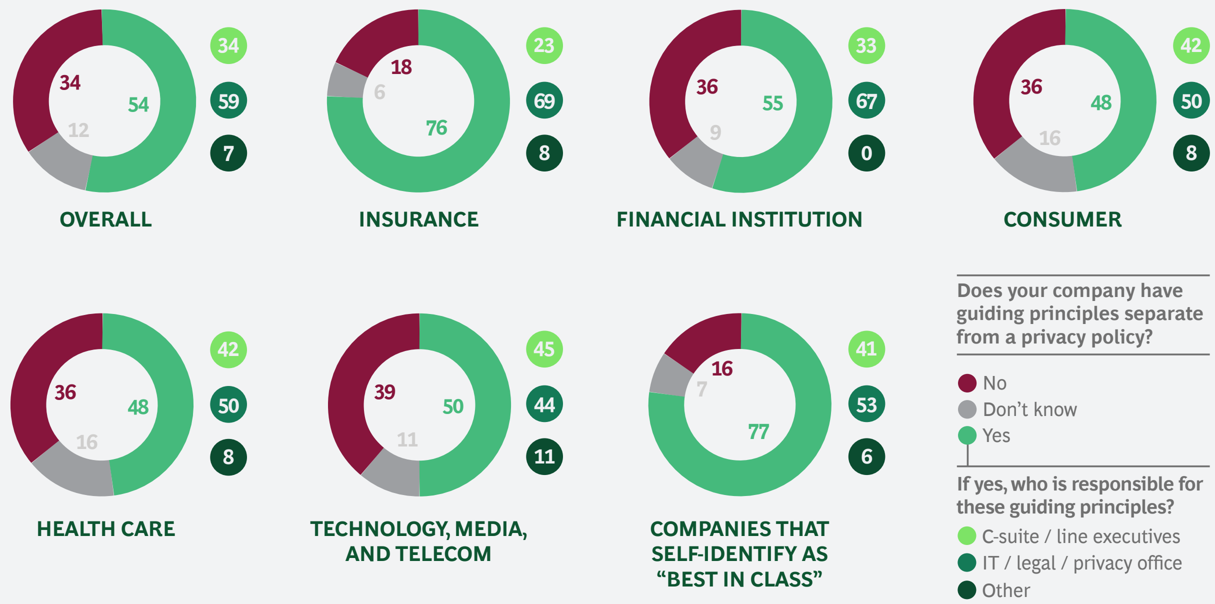


Source: BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "Has your company established a privacy policy that explains how you collect, manage, and use customer data?" and "Who has been responsible for determining the privacy policy?"

Exhibit 17 | Few Companies Have Guiding Principles for Data Privacy

Senior executives must be actively involved in developing internal best practices but often are not

EXISTENCE OF AND RESPONSIBILITY FOR GUIDING PRINCIPLES BY INDUSTRY (%)



Source: BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "Has your company established a set of guiding principles for how to use customer data that are separate and distinct from the privacy policy?" and "Who has been responsible for determining the guiding principles?"

formed consumers that it was collecting their data and using it to profile them—but an even greater shortcoming was revealed: senior executives were not aware of these activities; had they been aware, they likely would not have approved them.

Projects like this need the expertise that rests in multiple functions and at multiple levels of an organization. In this case, in the absence of either clear guidelines about new data collection and use or a decision-making framework that surfaced these new practices to the right, senior line levels, the decision to collect the data and create the profiles was made in isolation by the team doing the work. The backlash was provoked not by the project's original intent—creating functionality for Google Maps—but by the collection of new data elements for new uses that were not specifically part of Google Maps and that had not been explicitly discussed and approved. Google has since limited its data collection approach, destroyed the profiles, and settled the resulting multistate lawsuit. But the kind of disconnect that led to Google's issue is not uncommon in large organizations, demonstrating the need for clear guidelines and the active engagement of senior line executives in the governance process.

Companies must create data access protocols that cover "who," "what," and "why."

Creating Robust Protocols for Data Access—and Use. Once a company has established its policies, principles, and governance mechanisms, it must embed them in its approaches to regulating access to the data it has collected.

The good news is that many companies—71%, according to our survey results—have created protocols that govern access. These protocols establish which individuals have access to which particular types of data—the "who" and "what" aspects of the protocol.

But to truly steward data and avoid the pitfalls of unapproved uses, companies must also regulate the "why" aspect: the ways in which individual employees are allowed to use the data they are approved to access. Most companies do not have usage-based controls in place. They need to create protocols that consider "who, "what," and "why" in order to achieve a well-rounded, purpose-based approach to data control.

The poster child for the problem of failing to control usage came into public view when Edward Snowden leaked classified information from the National Security Agency's PRISM electronic-data-mining program. One of the issues that emerged was that people with appropriate access were, in the absence of usage-based controls, misusing data. Whether people agree or disagree with PRISM's original intent—to defend against terrorism—and its extent, few would argue that the data collected should be used to intrude on a neighbor's privacy or check up on a significant other.

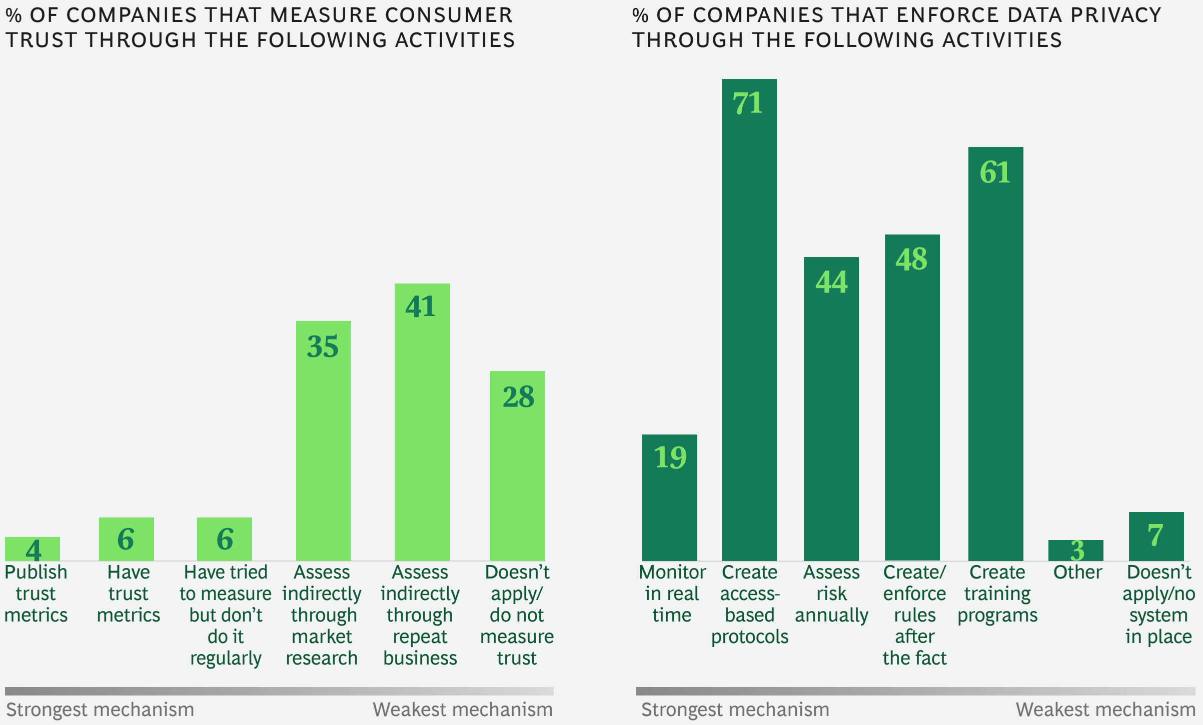
In another example, from the corporate world, Uber took steps to better manage data after the revelation that its employees could access customer data and track customers' location and that this data was being used for purposes far beyond providing outstanding car service. To mitigate such misuse in the future, Uber encrypted and password-protected location data. It also instituted a who-what-why approach to data access and use: the company restricts data access to a small number of employees, who can view and use the data related to drivers and customers only for legitimate business purposes.

Instituting Real-Time Monitoring and Proactive Responses. In a perfect world, everyone would follow the intent of guidelines, and purpose-based access protocols would work flawlessly. In the real world, it is important for companies to ensure that their employees are following the rules and that there are no violations of access or intent. (See Exhibit 18 for a look at our survey results showing the percentage of companies that enforce data privacy.)

This requires supplementing access protocols with real-time data monitoring. Monitoring approaches must focus on the same who-what-why elements that access-based proto-

Exhibit 18 | Companies Don't Know If Consumers Trust Them

And they may not deserve that trust because of weak internal enforcement mechanisms



Source: BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: "With regard to your company's approach to measuring customer trust, which of the following statements are true?" and "With regard to your company's approach to ensuring compliance with its privacy rules, which of the following statements are true?"

cols must address: the individual accessing the data, the data that he or she can access, and the usage for which the data is being accessed. Currently, though, only one in five companies has any kind of real-time data-monitoring protocol in place, much less one that incorporates usage—meaning that more than 80% of companies are highly vulnerable to data misuse.

By building in ways to respond when employees improperly access and use data, a company can repair inevitable breaches before they do harm to their stakeholders and, in turn, to their own brand and financial performance.

Right now, data misuse (whether real or perceived) is usually uncovered through consumer or media scrutiny. External rather than internal discovery of misuse has two unfortunate consequences: the misuse continues for longer and has a more significant impact on consumers than would be the case if it had been identified and shut down before being built into widely distributed products and services. And when a company uncovers a misuse itself, its response can be managed internally instead of in the context of public scrutiny. As our research suggests, the implications of public reactions to data misuse are highly negative: company revenues fall by 5% to 8% in the first year after a real or perceived data misuse. We believe that the year-one loss could be more severe—10% to 25%—as consumer awareness and concerns increase.

However, it is unlikely that companies will execute perfectly to identify in advance all instances of data collection and usage that will ultimately result in adverse reactions from consumers or other stakeholders. So, companies must prepare protocols in advance so that they are ready to address these types of situations. Predefined actions to repair the specific collection and usage issues and to communicate effectively with consumers and other stakeholders will help ensure that companies emerge from these incidents with equal—or greater—trust rather than suffering brand and revenue erosion.

Establishing a Permissible-Use Framework. Designing new decision-making processes to evaluate and to approve or reject new uses of data is also critical. Best practices can be established by following a permissible-use framework, such as the one shown in Exhibit 19. Such a framework guides those contemplating a new data use to consider four key inputs:

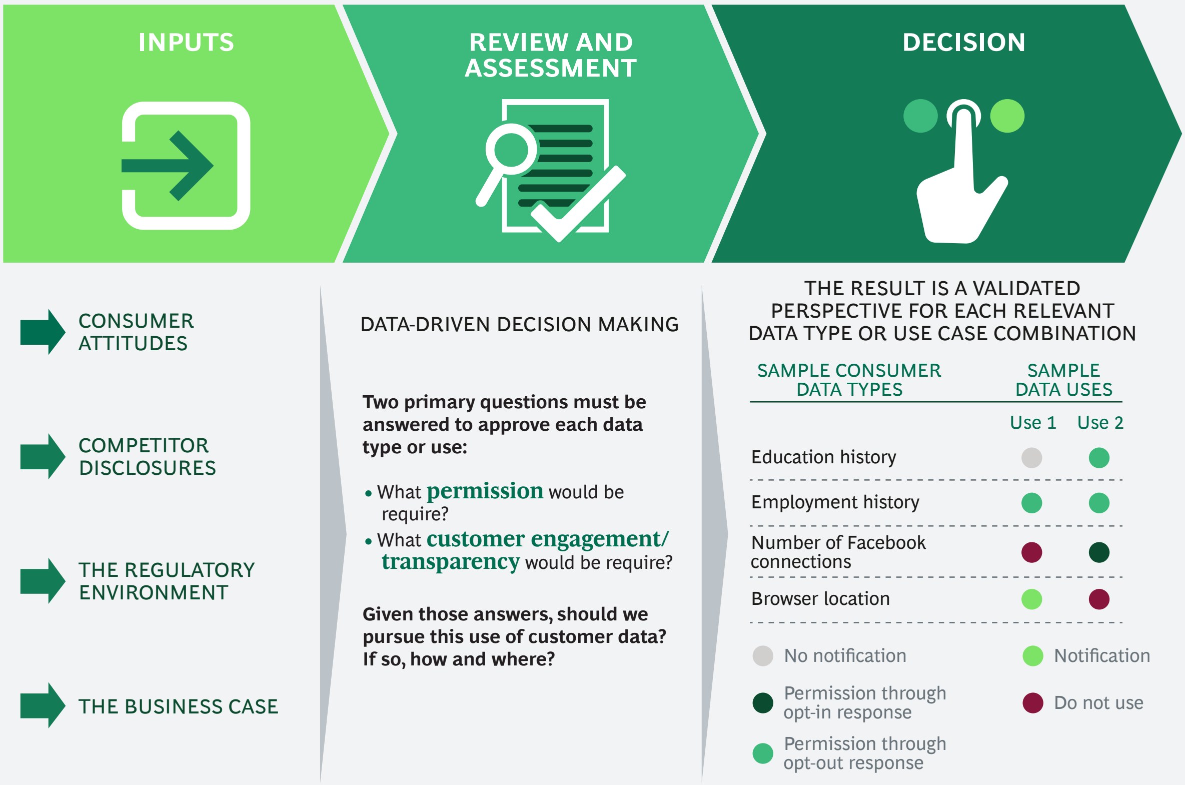
- **Consumer Attitudes.** How will different segments of consumers react upon being made aware of this new use?
- **Competitor Disclosures.** Is this an innovative new use or is it already prevalent in the market?
- **The Regulatory Environment.** Is the new use allowable under current rules and agreements?
- **The Business Case.** What are the direct and indirect benefits to the company of this new use?

These four inputs allow executive teams to make a fully informed decision regarding the risks and value associated with potential new data uses. This perspective can help them to decide not only whether to approve or reject a new use but also how to extend their best practices externally—to determine the best approaches for engaging consumers and other stakeholders.

Externally Focused Practices

In addition to taking internal actions to reduce the potential for adverse reactions, companies must actively engage with consumers and other stakeholders through external best practices. (Understanding consumers is key; Exhibits 20 and 21 show some survey-derived basics regarding consumer attitudes toward data types and industry reliability.) These requirements of good data stewardship are as important as internal best practices—but more elusive. Currently, these are the biggest stumbling blocks and sources of failure for

Exhibit 19 | Example of a Permissible-Use Framework
The framework lets teams make fully informed decisions



INPUTS

REVIEW AND ASSESSMENT

DECISION

CONSUMER ATTITUDES

COMPETITOR DISCLOSURES

THE REGULATORY ENVIRONMENT

THE BUSINESS CASE

DATA-DRIVEN DECISION MAKING

Two primary questions must be answered to approve each data type or use:

- What **permission** would be require?
- What **customer engagement/ transparency** would be require?

Given those answers, should we pursue this use of customer data? If so, how and where?

THE RESULT IS A VALIDATED PERSPECTIVE FOR EACH RELEVANT DATA TYPE OR USE CASE COMBINATION

SAMPLE CONSUMER DATA TYPES	SAMPLE DATA USES	
	Use 1	Use 2
Education history	○	◉
Employment history	◉	◉
Number of Facebook connections	🔴	●
Browser location	🟢	🔴

○ No notification
🟢 Notification
● Permission through opt-in response
🔴 Do not use
◉ Permission through opt-out response

Source: BCG.

EXHIBIT 20 | Consumers Are Sensitive to Data Misuse in Both the US and Europe

Financial, family, and health data are considered the most important to safeguard

% WHO CONSIDER THE DATA TYPE MODERATELY OR EXTREMELY PRIVATE 0 10 20 30 40 50 60 70 80 90 100

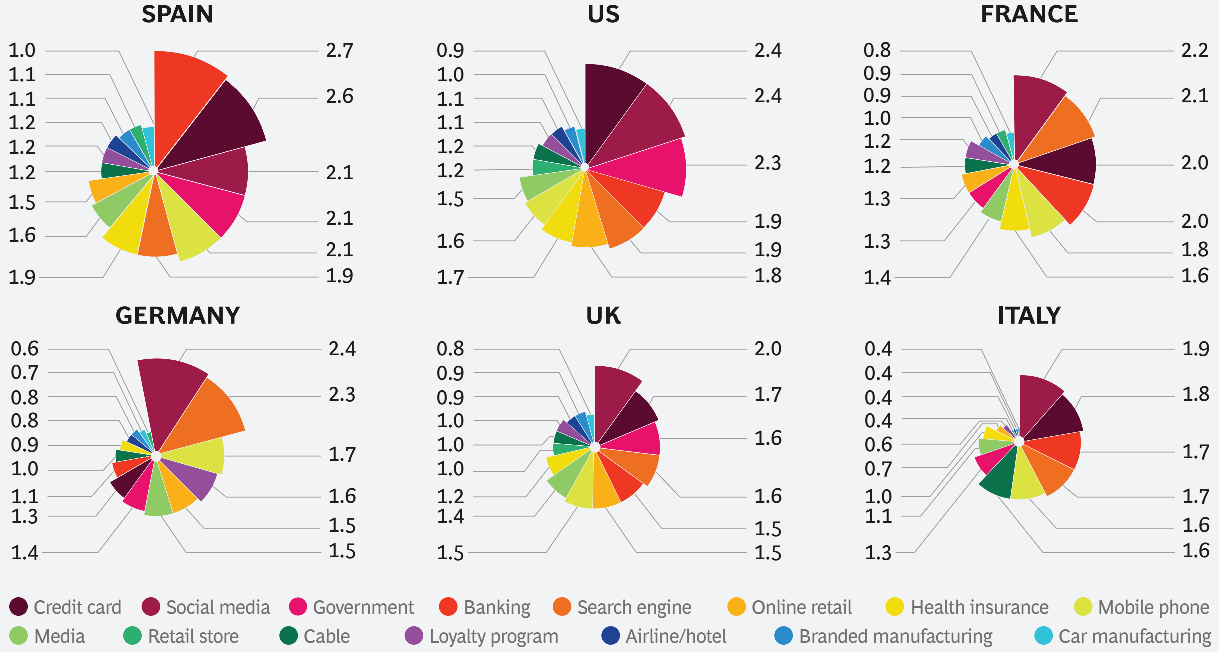
DATA TYPE	ITALY	UK	US	SPAIN	FRANCE	GERMANY
Credit card	84	79	79	81	89	85
Financial information	83	78	78	79	87	86
Tax information	70	72	77	72	83	83
Information about children	74	70	70	75	81	77
Health or genetic information	68	65	67	71	78	77
Information about spouse	67	59	63	69	78	78
Exact location	46	54	59	58	67	67
Dialed phone numbers	65	60	58	66	77	76
E-mail	42	50	53	45	54	48
Surfing history	50	48	47	52	64	66
Planned purchases	33	46	45	41	44	47
Important dates	34	45	44	43	48	55
Purchase history	32	42	43	40	53	52
Social network activity	40	38	40	43	54	53
Media usage	32	35	35	38	42	50
Products viewed online	26	33	32	32	39	42
Name	28	26	32	32	46	40
Interests	32	29	30	47	32	43
Age and gender	22	29	30	29	31	37
Brand preferences	15	24	23	22	22	34
Frustrations with products	25	26	22	32	32	32

Source: BCG Big Data and Trust Consumer Survey 2015.
Note: Survey question: "How private do you consider the following types of personal data? Answer using a scale from 1 to 5, where 1 means 'Not at all private' and 5 means 'Extremely private.'"

EXHIBIT 21 | Consumer Concern Varies Widely by Industry

Uses by financial, technology, and government organizations elicit the most concern

INDEXED LEVEL OF CONCERN (1.0 = 25% OF CONSUMERS EXPRESS CONCERN ABOUT AN INDUSTRY)



Source: BCG Big Data and Trust Consumer Survey 2015.
Note: Survey question: "Are you concerned about any of the following types of companies or organizations sharing your private data? Identify those you are concerned about."

companies attempting to make use of consumer data.

Increasing Transparency. Our survey data is clear: consumers want to know what data companies are collecting and how it will be used. Such transparency is rare, however.

Ensuring a high degree of transparency is, for most companies, a major mindset and cultural shift. It is a shift from “making information available” and “adhering to legal requirements for disclosure” to something much more fundamental: being responsible for ensuring that consumers and all other stakeholders understand what a company is doing with personal data. This is a significant pivot, with inherent challenges—but companies face an additional barrier: the likelihood that the new transparency will engender negative near-term reactions from some consumers who are surprised by the existence of data practices that they perceive as new.

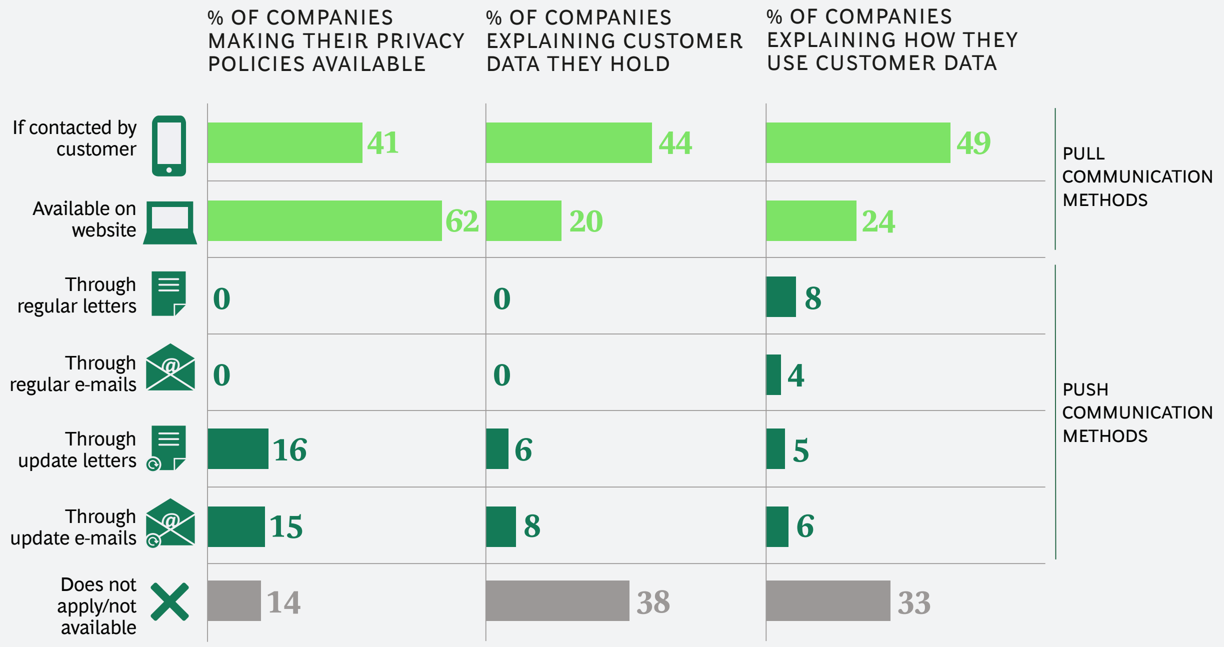
In the medium and long terms, however, the benefits of making this transition will be significant. Consumers are willing to accept a much wider use of their personal data than companies believe—but only if they are fully informed. In failing to understand and inform consumers, companies are currently being “recklessly conservative.”

A successful transition from opaque to transparent lies in a adopting a new set of engagement practices—moving from “pull” to “push.” Engagement practices today are overwhelmingly oriented toward pull behavior. They are designed to support consumers who will take the initiative to investigate and understand data use practices. (See Exhibit 22.) Unfortunately, few consumers do so, leaving the majority primed for distress when they are unpleasantly surprised by “new” data activities.

Good pull practices should not be eliminated. Rather, companies should add push-based practices, by which they take the initiative to bring information to consumers’ attention. This requires designing the right communications messages, processes, and distribution formats and vehicles. The appropriate bal-

Exhibit 22 | Companies Are Failing to Properly Engage Their Customers

Companies overwhelmingly rely on “pull” rather than “push” communication methods



Source: BCG Big Data and Trust Company Survey 2015.
Note: Survey questions: “With regard to communicating your company’s privacy policies to customers, which of the following statements are true?”; “With regard to engaging with customers about the data your company holds about them, which of the following statements are true?”; and “With regard to engaging with customers about how you use their data, which of the following statements are true?”

ance of push and pull methods will vary by company, industry, use case, or message. Always, though, a company's core goal must be to ensure that its data collection and use are fully understood by all relevant consumers—and other stakeholders.

Indeed, transparency is not just a consumer issue. Making data practices clear to a wider set of stakeholders also creates significant benefits. Regulators need to know—in advance—when a company is doing something new so that their actions are not shaped as reactions to consumer and financial press, for instance. Investors, industry associations, and commercial partners will also benefit from such transparency.

Clarity and transparency are good for the entire "data use ecosystem": when a company is open with regulators about its data practices, for instance, regulators are more likely to view new uses or consumer feedback positively because the transparency will provide them with valuable knowledge and insight into the complex and rapidly changing area of data usage and regulation. For example, we recently recommended that a financial services company implement a quarterly issues-oriented, nontransactional discussion with regulators. The goal is to give regulators a broad understanding of practices and issues on the horizon. Being involved in this way lets companies help drive the conversation instead of simply reacting to it.

Employing Purpose-Specific Notifications and Permissions. For each new use of data, a company should have an explicitly agreed-upon and purpose-specific approach to notification and permissions. In some cases, providing just a notification to consumers is sufficient. In others, an explicit opt-in response (which is not the same as signing a credit card application or clicking on a digital license agreement and thereby agreeing to something covered in the "fine print") will be needed.

It is clear that companies need to do this more effectively.

For instance, The Global Privacy Enforcement Network surveyed more than 1,200 smartphone apps in 2014 and found that 85% did not disclose data uses and that many requested broad permission for data uses without explaining why or how the data would be used.

Measuring and Publishing Metrics About Consumer Trust. As with all significant change and key operating activities, progress toward becoming a trusted data steward cannot be made without active measurement. And, in the context of transparency, key metrics should be shared with consumers and other stakeholders. (Few companies are doing this, as Exhibit 18 showed previously.) Doing so is a way to begin to differentiate a company's data practices and create a sustainable competitive advantage.

Transparency is not just a consumer issue. Consider all stakeholders.

Companies should start by creating metrics so that they can monitor trust, by tracking stakeholder perceptions, regularly and routinely. Metrics should be tailored to a company's unique dynamics but should generally cover:

- Overall faith in a company's data stewardship
- Willingness to allow the company to pursue new uses
- Understanding of a company's data practices
- Areas of significant sensitivity and concern

These metrics will serve several functions. They will help determine how consumers are responding to current efforts and which approaches to notifications and permissions work best for particular consumer segments. They can feed into a permissible-use framework by revealing trends among different demographics. For example, trust data might indicate that millennials trust a company more than Generation-Xers do, indicating that opt-out permissions are a better methodology for the former group whereas opt-in permissions are more appropriate for the latter. Because they can deliver such insights, trust metrics can help senior executives set policy direction.

In general, this set of practices is the aspect of data stewardship that companies today are the furthest from mastering. Currently, only 6% of companies have internal consumer trust metrics and actively measure consumer trust, according to our survey, and just 4% publish their trust metrics regularly.

In the absence of these metrics, companies are flying blind. If you don't know how you are being perceived, it is inherently impossible to know what to change. Thus blinded, a company will have little chance of becoming a trusted data steward and is in jeopardy of tripping unforeseen landmines and suffering reputational and performance damage.

The Responsibilities and Rewards of Trust

Companies must choose which direction to take when it comes to managing consumer data and trust.

Failing to establish good stewardship of consumer data puts companies on a vicious cycle, wherein poor management leads to the loss of trust and revenue and a downward trend in financial performance.

Conversely, companies can enter a virtuous cycle by establishing best practices and—crucially—a fundamentally revised mindset about privacy and data stewardship in order to win trust. In this virtuous cycle, managing consumer data well and actively engaging with stakeholders regarding data use engenders consumer trust. Trusting consumers allow more data to be used (our survey showed that consumers are at least five times as likely to share data with companies they trust), and so on.

Companies that choose this track and earn the trust of well-informed consumers will be able to create more value from consumer data. They can access more data for current uses and pursue new uses that are not available to less-trusted competitors. We believe that this creates sustainable competitive advantage because good data stewardship enhances brand value, because the capabilities that must be built to achieve it are not easily replicated, and because standards will only get higher over time, allowing front-runners to get far ahead of the pack as they establish new marketplace norms.

The choice seems clear, and the time to make it is now.

FOR FURTHER READING

The Boston Consulting Group has offers additional publications on the issue of consumer data and trust, including the following:

The Trust Advantage: How to Win with Big Data
A Focus by The Boston Consulting Group, November 2013

Unlocking the Value of Personal Data: From Collection to Usage
A report by The Boston Consulting Group and the World Economic Forum, February 2013

The Value of Our Digital Identity
A report by The Boston Consulting Group in the Liberty Global Policy Series, November 2012

NOTE TO THE READER

About the Authors

John Rose is a senior partner, managing director, and fellow in the New York office of The Boston Consulting Group. He is a fellow at the BCG Henderson Institute. His focus is the risks that companies face from the use of consumer data and the steps they can take to create sustainable competitive advantage through effective data stewardship. **Alexander Lawrence** is a project leader in the firm's New York office. Before joining BCG, he worked as an attorney specializing in mergers and acquisitions. **Elias Baltassis** is a director in BCG's Paris office and the leader of the data and analytics team in Europe. Prior to joining BCG, he was a partner with a leading strategy consulting firm and a founding member and managing director of a leading pure-play big data company.

Acknowledgments

The authors thank Katherine Andrews, Mickey Butts, Gary Callahan, Catherine Cuddihee, Kim Friedman, and Abby Garland for their editorial, production, and design contributions.

For Further Contact

John Rose
Senior Partner and Managing Director
BCG New York
+1 212-446-2800
rose.john@bcg.com

Alexander Lawrence
Project Leader
BCG New York
+1 212-446-2800
lawrence.alexander@bcg.com

Elias Baltassis
Director
BCG Paris
+33 1 40 17 10 10
baltassis.elias@bcg.com

© The Boston Consulting Group, Inc. 2018. All rights reserved.

For information or permission to reprint, please contact BCG at:
E-mail: bcg-info@bcg.com
Fax: +1 617 850 3901, attention BCG/Permissions
Mail: BCG/Permissions
The Boston Consulting Group, Inc.
One Beacon Street
Boston, MA 02108
USA

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com.

Follow The Boston Consulting Group on Facebook and Twitter.

3/18

BCG

The Boston Consulting Group

bcg.com