Guarding and growing personal data value

Tim Cooper and Ryan LaSalle
Executive summary

Businesses collect massive volumes of data from individuals, using it to personalize customer offerings, innovate products and diversify into new markets. But increasingly customers are concerned about who is doing what with their data. Governments are rewriting the rules to protect privacy. And watchdogs are stepping up their scrutiny of data practices. How can organizations preserve and even increase the potential of personal data? Accenture believes five principles of corporate digital responsibility—stewardship, transparency, empowerment, equity and inclusion—can turn potential risks into opportunities for business differentiation and growth.

Why personal data is business critical

The use of personal data is a mainstream business activity. In an Accenture survey of nearly 600 businesses around the world, 79 percent of respondents said their companies collect data directly from individuals (through online customer accounts, for example) as well as from commercial or data-sharing partnerships (42 percent), connected devices (33 percent) and third-party data suppliers (33 percent). Businesses are using multiple channels to gather personal data due to the benefits it generates, for them and their customers. Chief among these advantages are the abilities to deliver better customer experiences (identified by 77 percent of respondents), enter new markets (52 percent) and make products more innovative (50 percent).

Business use of personal data at risk

Despite the benefits, there is a growing challenge to the business use of data from changes unfolding among businesses’ key stakeholders—including customers, regulatory bodies and watchdogs. Our research has identified a number of changes that are particularly important for organizations to understand if they hope to respond effectively.

There is a crisis of trust in data security: Customers will not do business with companies they do not trust with their data. The problem, though, is that customers’ trust in data security is weak. In Germany, for example, 71 percent of consumers are not confident in the security of their personal data. In addition, more than half of our survey respondents agree that their businesses are not doing enough to build trust with customers over the use of their data—a finding that applies to technology and non-technology companies alike. Poor data security can mean organizations lose customers, but that is not the only risk: fines, litigation costs, reputational damage and even a drop in share price can all accompany a data breach.

Customers are acting on their privacy concerns: Customer actions to protect their data could compromise the amount and quality of personal data that businesses can use. Seventy-nine percent of our survey respondents believe that their company’s customers are more aware of data privacy, and 67 percent believe that their customers are taking measures to protect that privacy (through moves such as changing passwords more frequently and opting out of some services). Moreover, many customers will avoid businesses that do not protect their privacy.

Customers are demanding a data dividend: Individuals are finding ways to gain greater benefits from allowing companies to use their data. Nearly 60 percent of our survey respondents from products and manufacturing companies report that their customers are actively monetizing their own data (for instance, by selling it to data intermediaries). As this practice becomes more commonplace, the era of universally “free” data collection could end and businesses will need to rethink their data-collection strategies.

New technologies and startups are helping more people go “off grid”: Growth in new privacy-enhancing technologies could reduce the quality of customer data and the speed at which businesses can analyze it. For instance, DuckDuckGo is a search engine that users can access anonymously. In early 2013, it handled about 1.7 million queries per day—by early 2015, that figure had reached more than 7 million.

Regulation is changing the rules of data collection: Governments are stepping up their regulatory response to concerns over data privacy. However, while our survey respondents agree that more stringent regulation will be disruptive, 72 percent of them believe that regulation can also help ensure clarity regarding the appropriate use of personal data.

Watchdogs are increasing the scrutiny of business data practices: A number of organizations are now scrutinizing the way businesses manage personal data. Fair Data in the United Kingdom and the Electronic Frontier Foundation in the United States are two examples. Such organizations are helping to draw a clearer distinction between companies that manage data ethically and those that do not, thereby influencing customers’ purchasing decisions.
Five principles for progress

How can businesses manage these threats? Accenture’s five principles of corporate digital responsibility provide a roadmap for action. However, our survey findings suggest that there are significant gaps between the importance businesses attach to these principles and the action they have already taken to implement them.

1. Digital stewardship: Ensuring that management of personal data is consistent with the expectations of those providing it. Identified as important by 90 percent of the businesses represented in our survey—with 74 percent also taking action—leading strategies here include upgrading the security of IT systems, establishing robust accountability structures across the company, and working with supply chain and industry partners to drive higher standards.

2. Digital transparency: Demonstrating openness in how businesses use personal data. Eighty-five percent of the businesses represented in our survey view transparency as important, yet only 65 percent report taking any action here. To get started, businesses can proactively show how they are using data internally, embrace industry-level self-regulation schemes and seek out independent accreditation.

3. Digital empowerment: Giving customers greater control over their data. Eighty-one percent of our survey respondents recognize this as important, yet only 55 percent say their businesses are taking action. Leading strategies include letting customers update any data held about them, strengthening customer controls over data sharing and proactively pushing data to help customers make better decisions (such as which foods would be healthiest for them).

4. Digital equity: Clarifying and potentially increasing the benefits customers receive in exchange for sharing their data. Seventy-two percent of the businesses in our study see this as important, but just 50 percent are developing strategies in this area. To implement this principle, companies must shift from a one-way data-collection mindset to a two-way transaction or “fair value” exchange mindset. They can foster such exchanges by providing consumers with monetary rewards for sharing data and by enhancing service functionality.

5. Digital inclusion: Using personal data to multiply positive societal outcomes. Though this principle is relatively nascent, 62 percent of participants in our survey view it as an important strategy for enhancing their company’s reputation for responsible data management. Half report that their businesses are taking action already, with leading companies addressing challenges in such areas as public health, urban planning and food wastage.

In this report, Accenture explores the five principles that determine a successful path to using personal data and identifies practical steps toward progress.
Introduction

The collection and analysis of personal data has unlocked significant benefits for organizations and customers alike. For organizations, these benefits include more innovative ways of reaching customers, as well as a greater ability to develop innovative products and enter new markets. For customers, the benefits include greater choice, increased convenience, higher discounts and more personalized consumption experiences. All of these advantages have been made possible by individuals’ willingness to share personal data through digital technologies.

But what if people stop sharing their data so freely? Businesses across all industries, in both developed and emerging economies, face this disruptive prospect. Customers have concerns about the security of their data, how it is being used and who is reaping the rewards from it. And they are acting on these concerns. In response, governments around the world have stepped up their legislative efforts, including passing new data-privacy laws. Moreover, startups are creating products and services aimed at reassuring customers, offering alternative ways to store, manage and monetize data. In addition, non-profits and civil society organizations are emerging, bringing greater scrutiny to previously opaque practices.

These trends will make it harder, and potentially more costly, for businesses to gather the volumes and quality of personal data to which they have become accustomed, compromising their ability to deliver the benefits they and their customers have enjoyed. Our research shows that businesses recognize the importance of addressing this challenge—but that they need to do more to translate this awareness into action.

In short, they must implement the five principles of corporate digital responsibility: stewardship, transparency, empowerment, equity and inclusion. They will need to strike a balance between protecting key data assets and finding new ways to share data appropriately. They may have to cede some control over the data they hold, in return for greater customer loyalty and the continued right to use that data. In many instances, they may need to move from a predominantly one-way model of data collection to a model that treats customers as equal partners in a two-way transaction. And increasingly they may need to find ways to use personal data to the benefit of society as a whole, while protecting private rights and concerns.
Why personal data is business critical

A data explosion is driving innovation and growth across the global economy. But the way businesses manage some of this data—in particular, data originating from individuals—is sparking controversy. From the selling of personal data to perceived intrusion into customers’ private lives, recent headlines have drawn attention to two clear facts. First, personal data is an asset but also can be a liability. Second, the appearance of malpractice in the use of personal data can prove just as damaging as actual malpractice. Given these realities, no business can afford to ignore the issue of responsible data management.

To understand the challenges and opportunities of personal data use facing organizations today, Accenture undertook primary and secondary research, as well as seeking the views of academic experts (see About the research, page 29). What is clear is that data management has become even more critical following the disruptive impact of digital technology on traditional methods of data collection. Three new features on the data landscape—a new data life cycle, a wider spectrum of data-collection channels and more integrated business benefits—demand closer attention.
**New data life cycle**

Digital technology has transformed the way businesses collect and use data (see Figure 1). To gauge public opinion, companies no longer need to knock on doors. Instead, they can swiftly process millions of comparable data points collected through online behavioral tracking tools, such as cookies. Cloud computing has further transformed the data life cycle by making data accessible almost anywhere and at any time, saving people from having to carry around heavy files and papers.

Figure 1. Digital technology has transformed the business data life cycle

At each stage of the business data life cycle—from collection to disposal—digital technology has transformed traditional “analog” approaches to data management.

<table>
<thead>
<tr>
<th><strong>ANALOG</strong></th>
<th><strong>DIGITAL</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection</strong></td>
<td><strong>Face-to-interface</strong></td>
</tr>
<tr>
<td>Face-to-face</td>
<td>Data is collected via different tracking technologies, such as sensors, GPS and website cookies.</td>
</tr>
<tr>
<td>Consumer data is collected primarily through direct surveys, interviews and focus groups.</td>
<td></td>
</tr>
<tr>
<td><strong>Aggregation</strong></td>
<td><strong>Sample-based</strong></td>
</tr>
<tr>
<td>Data is segmented into groups, usually by socioeconomic characteristics (e.g., income level, demographics). It is difficult to combine data in different formats.</td>
<td><strong>Individual-based</strong></td>
</tr>
<tr>
<td></td>
<td>Data is analyzed on an individual basis, with standardized formats helping to build a 360-degree profile of each consumer.</td>
</tr>
<tr>
<td><strong>Analysis</strong></td>
<td><strong>Retrospective</strong></td>
</tr>
<tr>
<td>Basic levels of historical analysis are used to identify needs of certain groups from sample-based data.</td>
<td><strong>Predictive</strong></td>
</tr>
<tr>
<td></td>
<td>Companies use more advanced statistical modeling, such as predictive analytics, to build a fuller consumer profile and predict future purchases.</td>
</tr>
<tr>
<td><strong>Monetization</strong></td>
<td><strong>Indirect</strong></td>
</tr>
<tr>
<td>Revenue is generated indirectly by using insight into customer needs to develop new products and services.</td>
<td><strong>Direct</strong></td>
</tr>
<tr>
<td></td>
<td>Data has intrinsic value and can be sold to third parties (in anonymized format).</td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td><strong>Physical</strong></td>
</tr>
<tr>
<td>Storage is physical (e.g., in files) and space-consuming. Retrieval of data is often costly and inconvenient.</td>
<td><strong>Virtual</strong></td>
</tr>
<tr>
<td></td>
<td>Users can now access data anywhere with an internet connection and at low cost.</td>
</tr>
<tr>
<td><strong>Disposal</strong></td>
<td><strong>Single-step</strong></td>
</tr>
<tr>
<td>Permanent deletion of data involves destroying the single physical device on which the data is stored.</td>
<td><strong>Multi-step</strong></td>
</tr>
<tr>
<td></td>
<td>To permanently delete data, numerous platforms and databases must be targeted individually.</td>
</tr>
</tbody>
</table>

Source: Accenture Institute for High Performance.
Wider spectrum of data-collection channels

The shift to a digital economy has introduced new channels through which businesses can harness data. The most popular channel for collecting data is individuals themselves (for example, by gathering personal data from online customer accounts). Indeed, nearly 80 percent of the businesses represented in our survey use this approach (see Figure 2).

In addition, businesses are accessing personal data from other organizations: through commercial or data-sharing arrangements (identified by 42 percent of survey respondents), from third-party data suppliers (companies that collect and sell anonymized data) and from data intermediaries (companies that store and often monetize personal data on behalf of individuals).

Figure 2. Businesses gather personal data through multiple channels

Our survey findings suggest that businesses collect personal data mainly from individuals, but also from other organizations and through connected devices (for example, wearable technologies).

Q: From which of the following sources does your company routinely collect data?

- Directly from individuals themselves: 79%
- Directly from other organizations (e.g., through commercial or data-sharing agreement): 42%
- Purchase from third-party data suppliers: 33%
- From connected devices: 33%
- From personal-data intermediaries: 30%

Source: Accenture personal data survey 2014.
More integrated business benefits

Businesses are exploring diverse channels in order to realize the integrated benefits that personal data can deliver to them and their customers. Three benefits are particularly valuable:

1. **Customer innovation**: Online marketplace Alibaba recorded sales of US$9.3 billion in just one day in 2014. To achieve this feat, it had laid the groundwork by using algorithms to predict and display personalized recommendations to its customers.1 When Singles Day (a key event in China’s shopping calendar) came around, Alibaba customers had a ready-made list of discounted, tailored products waiting for them to buy. Alibaba understood the importance of using personal data to deliver more tailored customer experiences—the number one benefit identified by businesses in our survey (see Figure 3).

2. **Product innovation**: In addition to tailoring existing goods and services more closely to customers’ tastes, personal data helps companies develop entirely new offerings aimed at meeting specific customer needs. For example, Volvo worked with startup MyndPlay to analyze how drivers respond emotionally to car designs. To conduct this analysis, the companies monitored volunteers’ brain signals as they viewed different car designs and images. Analysis of the data inspired Volvo to launch the concept car Coupe—the company’s first initiative to build an emotional connection with consumers.

3. **Market innovation**: Many companies that collect personal data are well-positioned to use these insights to enter new markets. For instance, numerous retail businesses now offer financial services, aided by their insight into customers’ spending patterns and personal profiles. Several major supermarkets in the United Kingdom (ASDA, Marks & Spencer, Sainsbury’s) offer personal finance services. In a similar vein, personal data can be a significant source of direct revenue generation. About 33 percent of the businesses represented in our survey earn revenue from selling anonymized data. The benefits that businesses have realized from personal data are considerable, but they are also now being challenged.

---

**Figure 3. Personal data unlocks key business benefits**

Personal data helps companies deliver many benefits—in particular, developing more personalized services, driving next-generation products and unlocking new markets.

Q: What are the key benefits your company realizes from the use of personal data?

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>77% Ability to deliver better customer experiences/personalized services</td>
<td></td>
</tr>
<tr>
<td>53% Enhanced customer loyalty</td>
<td></td>
</tr>
<tr>
<td>52% Ability to uncover opportunities in new markets</td>
<td></td>
</tr>
<tr>
<td>52% Advertising that is more targeted to individuals’ interests</td>
<td></td>
</tr>
<tr>
<td>50% Better/more innovative products</td>
<td></td>
</tr>
<tr>
<td>47% Ability to offer commercially viable discounts and sale schemes</td>
<td></td>
</tr>
<tr>
<td>41% Increased profitable revenue</td>
<td></td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
In focus: What is personal data?

Personal data can be as seemingly innocuous as a date of birth or as sensitive as a detailed medical history (see Figure 4). As digital technologies continue to infuse our lives, what constitutes “sensitive” data today has become a broad question. In a 2014 survey of consumers in the United Kingdom and the United States, most respondents identified their national insurance number, health records and home address as sensitive personal data. But now these have been joined by data such as internet protocol (IP) or Mac address and location data recorded on mobile phones.2

Figure 4. There are many different types of personal data

Formal definitions of personal data have been updated to reflect the digital age.

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Official records</td>
<td>Name, social security number</td>
</tr>
<tr>
<td>Demographic information</td>
<td>Age, gender, race</td>
</tr>
<tr>
<td>User-generated content</td>
<td>Blogs, tweets</td>
</tr>
<tr>
<td>Online activity</td>
<td>Online searches, website browsing</td>
</tr>
<tr>
<td>Social contacts</td>
<td>Facebook friends, Twitter followers, phone book contacts</td>
</tr>
<tr>
<td>Data recorded on smart personal devices</td>
<td>Location data on smartphones, physical conditions recorded on fitness wearables</td>
</tr>
</tbody>
</table>

Source: OECD.

Personal data now makes up about 75 percent of all digital data created.3 In the United States, for example, a typical white-collar worker creates as many as 5,000 megabytes of personal data each day—roughly the size of two high-definition movies.4 While individual data points may have relatively little value in themselves, the potential for them to be linked—and the insights that companies can gain from making those connections—can be particularly lucrative.
Business use of personal data at risk

Businesses have to date largely enjoyed the fruits of personal data while facing relatively few challenges. But that period of relative calm is changing. New risks are emerging to the strategies that have enabled businesses to create benefits for themselves and their customers from the use of personal data. From many quarters—customers, governments, startups, non-governmental organizations (NGOs)—pressures are emerging that, left unaddressed, could severely constrain companies’ ability to gather data and generate value from it.
There is a crisis of trust in data security

Consumers have little confidence in organizations’ ability to keep personal data secure. In a recent Accenture survey, for example, more than half (55 percent) of consumers across 23 countries report that they are not confident in the security of their personal data. Mistrust is particularly acute among participating consumers who live in Germany, with 71 percent not confident in the security of their data (see Figure 5).

Businesses acknowledge this lack of trust. More than half of our survey respondents believe that their business is not doing enough to build trust with customers around data use (see Figure 6 for a country breakdown). The perceived deficit in action also varies across industries. Significantly, trust is the greatest concern in the industry at the forefront of technological change: the IT industry.

Business implications: Businesses will need to step up their efforts to win back customer trust. Customers will avoid companies they do not trust to keep their data secure. In a 2014 global survey by SafeNet, nearly two-thirds of the consumers who responded said they would stop or avoid using a company that had experienced a data breach. In addition, fines for data breaches, already significant, are rising quickly: A data breach in the United States costs 15 percent more in 2014 than it did in 2013. Yet the indirect cost of a breach may be even greater. The reputational damage and loss of business opportunities that can follow a data breach sometimes amount to billions of dollars and can even result in a fall in share price.
Customers are acting on their privacy concerns

Not only are customers concerned about the ability of businesses to keep their data secure, but they are also worried about the way in which that data is being used. Seventy-nine percent of our survey respondents report that their customers are more aware of the issue of data privacy—and 67 percent say their customers are taking action to protect their privacy (such as changing passwords more frequently and opting out of some services). Customers of consumer products and manufacturing companies are particularly vigilant, but reported action varies across different industries (see Figure 7). Attitudes also vary across countries: 81 percent of the survey respondents in China see their customers taking action, versus 59 percent in France.

Business implications: As customers take privacy protection into their own hands, the volume and quality of personal data that businesses can access could be compromised. This impact will likely only increase as consumer action catches up with awareness. Companies that fail to respond effectively to this trend may pay a high price. According to the TRUSTe Consumer Confidence Index, nine in ten internet users in the United Kingdom and the United States would avoid doing business with companies that do not protect their privacy.7

Part of the challenge for businesses is that privacy is an inherently personal concept. It evolves over time and is being shaped by technology advancement itself. For businesses looking to adapt to their customers’ changing concerns about privacy, it is clear that a “one-size-fits-all” approach to protecting privacy will not suffice.

Figure 7. Customer awareness of data privacy is translating into action

Customer awareness of data privacy is high across all industries. And a significant proportion of businesses report that their customers are taking active measures to protect their privacy (for example, changing passwords, opting out of some services).

Q: Looking back over the last three years, to what extent do you agree or disagree with the following statements? (Percentage of respondents who agree or strongly agree)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Awareness (%)</th>
<th>Protection (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>73</td>
<td>86</td>
</tr>
<tr>
<td>Products</td>
<td>77</td>
<td>85</td>
</tr>
<tr>
<td>IT &amp; technology</td>
<td>73</td>
<td>83</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>58</td>
<td>80</td>
</tr>
<tr>
<td>Retail/wholesale</td>
<td>59</td>
<td>80</td>
</tr>
<tr>
<td>Resources</td>
<td>62</td>
<td>77</td>
</tr>
<tr>
<td>Health &amp; public service</td>
<td>59</td>
<td>73</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>59</td>
<td>70</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
Customers are demanding a data dividend

The era of one-way, universally "free" data collection is over. Business executives know this; they believe that their customers have not only become more aware of the potential monetary value of their data, but also are taking action to monetize it (see Figure 8). What is the explanation for this development? Customers do not feel they have been receiving their fair share of the benefits that come from providing personal data. In a study by telecommunications company Orange, 67 percent of European consumers surveyed believe that organizations benefit the most from using their personal data. Only 6 percent identify themselves as the main beneficiary.8

Business implications: As individuals become more aware of the potential to monetize their data—and as channels for doing so become more accessible—they will be able to operate as their own digital enterprises, treating their data as a business would manage its intellectual property. For example, intermediaries such as Datacoup enable users to sell their data by connecting their social media and debit and credit card accounts to businesses that want to gather quality data about their target customers. A week after Datacoup’s launch, the platform had already gathered interest from 15,000 individuals and 20 data buyers.9 As these startups become more popular, they could increase the costs of accessing personal data for businesses while creating a clearer choice for customers deciding between companies that reward them for sharing data and those that do not.

Figure 8. Customers are moving to monetize their personal data

Businesses know that their customers are more aware of the value of their data. A significant share of customers is reportedly taking action to increase the monetary value they receive from sharing their data.

Q: Looking back over the last three years, to what extent do you agree or disagree with the following statements? (Percentage of respondents who agree or strongly agree)

<table>
<thead>
<tr>
<th>Category</th>
<th>Agree or Strongly Agree</th>
<th>Disagree or Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products</td>
<td>77%</td>
<td>59%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>76%</td>
<td>58%</td>
</tr>
<tr>
<td>Financial services</td>
<td>75%</td>
<td>46%</td>
</tr>
<tr>
<td>IT &amp; technology</td>
<td>73%</td>
<td>56%</td>
</tr>
<tr>
<td>Retail/wholesale</td>
<td>69%</td>
<td>50%</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>63%</td>
<td>51%</td>
</tr>
<tr>
<td>Resources</td>
<td>60%</td>
<td>47%</td>
</tr>
<tr>
<td>Health &amp; public service</td>
<td>54%</td>
<td>39%</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
New technologies and startups are helping more people go “off grid”

New technologies and startups are giving people alternative ways to protect their personal data, beyond good housekeeping measures such as changing passwords. DuckDuckGo is a search engine that users can access anonymously. In early 2013, it handled about 1.7 million queries per day. Following the Snowden revelations of government surveillance, the number of daily queries doubled in the second half of 2013, and in early 2015 queries had reached more than 7 million.10

Some consumers are also choosing to use mobile devices that enable them to control what personal data can be accessed. Devices such as the Blackphone and the Indie Phone, both launched in 2014, are good examples. The Blackphone encrypts all users’ phone calls, emails, texts and internet browsing.11 The Indie Phone provides users with a central repository for all their data, and app developers must ask for permission to access the data.12

Startups, too, are getting in on the act. As a leading online storage vault for personal information, Personal.com enables subscribers, who pay an annual fee of just US$29.99,13 to store and manage their data in a vault with the same level of security as the United States military.14 Ghostery helps customers block organizations from tracking their web-browsing activities and now boasts more than 20 million users.15

Business implications: As these technologies, devices and startups become more common, the speed at which businesses can use and analyze customers’ data may be significantly reduced. Extracting information from encrypted data takes an estimated 1 quintillion times longer than from open data.16 To sustain their current access to customers’ data, businesses may have to work harder to convince people that their data is in safe hands. They may also need to adapt to customers who wish to go “off grid” but continue to use their services.

Regulation is changing the rules of data collection

Against a backdrop of growing consumer concern, many governments are reviewing regulation to protect data. In 1993, four countries had data-privacy regulations. By late 2013, this number had reached 101 (see Figure 9).17 This means that 66 percent of the world’s population was covered by data-protection regulation in 2013, up from 42 percent in 1993.18 In some cases, these regulations are placing more restrictive provisions on businesses than before. For example, some countries are moving toward data localization, requiring personal data about any of their citizens to be held domestically rather than stored or managed abroad. Russia has set a timetable to introduce data localization in late 2015.19 As a result of the new law, it is reported that large technology companies might have to pay as much as US$200 million to build a data center in Russia,20 compared with US$43 million in the United States.21

Figure 9. The global rise of data-protection regulation—and European Union influence

The number of countries with data-protection regulation has soared over the past 20 years. In particular, the European Union’s standards have been adopted by or affect many non-EU countries.

Source: Accenture analysis of secondary sources.
Governments are also defining procurement rules to promote stricter data diligence in the wider economy. For example, suppliers of IT services to the German government must now explicitly guarantee that they will not give third parties access to confidential data.\textsuperscript{22}

As digital technologies grow more sophisticated, policymakers are keeping pace. In late 2014, the European Commission adopted an opinion calling for consent for device fingerprinting (by which new technologies are used to uniquely identify mobile devices and applications) to be put on the same legal footing as the use of cookies on the internet.\textsuperscript{23}

Enhanced regulation could exert a significant impact on businesses. Indeed, the companies we surveyed rank it as the number-one disruptor (see Figure 10).

*Figure 10. Businesses see stricter government regulation as the number-one disruptor*

When asked about a number of potential future scenarios, the majority of businesses represented in our survey see stricter data-protection regulation (such as data localization) as the most disruptive.

Q: Which of the following events will be most disruptive to your company’s ability to realize value from the collection and analysis of personal data in the next three years? (Please rank top three according to level of importance)

<table>
<thead>
<tr>
<th>Event</th>
<th>Brazil</th>
<th>China</th>
<th>France</th>
<th>Germany</th>
<th>India</th>
<th>United Kingdom</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals charging for use of their data becomes global norm</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Governments implement stricter data protection regulations (e.g., requiring in-country physical data storage)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Significant customer backlash against online price discrimination</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>High-profile instances of cyber-crime/data breaches</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>New technologies and products let individuals avoid creating an online footprint</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
Increased cost of compliance could be one obvious outcome. A study by the UK Ministry of Justice estimated that proposed EU data protection rules would impose a net cost of between £100 million and £360 million each year on the UK economy. However, more harmonized legislation may make the business environment more transparent: Respondents in nearly three-quarters of the businesses represented in our survey agree that regulation will help enhance clarity regarding the appropriate use of data (see Figure 11 for a country breakdown). However, at the industry level, some respondents are less convinced. In retail, for example, only 56 percent believe that more regulation will help.

**Business implications:** As the regulatory picture changes around the world, businesses need to monitor the latest developments and model their potential impact. However, it is not just a one-way street. Regulation can also establish a clearer framework within which businesses can operate. Should standards harmonize globally, businesses operating across national borders in particular would likely benefit from greater regulatory clarity and certainty.

**Watchdogs are increasing the scrutiny of business data practices**

Alongside government regulation, civil society organizations are stepping up the scrutiny of how businesses manage personal data. Consider Fair Data, a scheme launched in the United Kingdom in 2013 with members in more than 60 countries. Fair Data accredits companies that adhere to 10 core principles that reflect existing ISO standards and data-protection legislation, such as the obtaining of consent before collecting data, efficient data security measures and access rights for data subjects. The accreditation is available to consumer organizations, business-to-business companies and government bodies.

Similarly, the Electronic Frontier Foundation (EFF), a nonprofit digital-rights group based in the United States, has recently been putting greater emphasis on evaluating the data practices of major internet companies. EFF’s published scorecards assess companies’ commitment to protecting customer interests when third parties seek access to their data. EFF has been a major initiator of the Do Not Track movement—a technology and policy proposal that addresses third-party tracking of internet users’ browsing activities.

**Business implications:** In the same way many consumers look for Fairtrade food labels, customers will evaluate companies’ data practices to determine from which businesses they want to buy. In a survey by Evidon of consumers in the United Kingdom, 54 percent feel better about brands that are transparent in their data practices, and 48 percent suggest that they would be more likely to purchase these brands. By engaging proactively with data-rights organizations, businesses can help give credence to their assessments and more clearly distinguish themselves from rivals.

On a number of fronts, businesses are facing a challenge to the status quo of personal data collection. Left unaddressed, these challenges carry significant repercussions: loss of customers, reduced supply of high-quality data, increased costs, even a fall in a company’s share price. To avoid these negative impacts, businesses need to take action now.

---

**Figure 11. Business appetite for regulation varies by economy**

Emerging economies seem to favor more data-related regulation than their developed-economy counterparts, perhaps reflecting the relative infancy of the relevant institutions in emerging economies.

Q: To what extent do you agree or disagree with the statement “More regulation will help ensure there is greater clarity around appropriate use of data”? (Percentage of respondents who agree or strongly agree)

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>83%</td>
</tr>
<tr>
<td>France</td>
<td>81%</td>
</tr>
<tr>
<td>Brazil</td>
<td>76%</td>
</tr>
<tr>
<td>India</td>
<td>76%</td>
</tr>
<tr>
<td>Germany</td>
<td>69%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>66%</td>
</tr>
<tr>
<td>United States</td>
<td>61%</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
Five principles for progress

What can businesses do about the threats to the use of personal data? To prepare for and adapt to changing customer attitudes, strengthening government regulation and new sources of scrutiny, Accenture has developed five principles for corporate digital responsibility that can help guide the way.
1. Digital stewardship
Ensuring that management of personal data is consistent with the expectations of those providing it
Companies that ensure their data-management approaches are secure and reflect customers’ notions of privacy can differentiate themselves from the competition and secure new business. For example, following Microsoft’s introduction of new security measures, the company’s suite of enterprise cloud services was the first to win approval from the Article 29 Working Party—a group of data protection authorities in the European Union—for meeting their privacy standards. This helped the company make significant headway in the cloud services market. Similarly, Deutsche Telekom worked with email providers WEB.DE, T-Online and GMX to launch the secure end-to-end email communication service “Email made in Germany.” This initiative stores user data within Germany, responding to customers’ fear of external surveillance of their data. The parent company of GMX and WEB.DE saw a six-figure increase in new joiners at the time of the Snowden revelations between June and August 2013.

2. Digital transparency
Demonstrating openness in how businesses use personal data
Companies can foster transparency by proactively showing customers and other organizations how they are using data and storing it internally. Nectar, a loyalty program in the United Kingdom, offers its 18 million customers full visibility of data collection and use. Consequently, Nectar was singled out by the UK Information Commissioner’s Office as an exemplar of transparency.

3. Digital empowerment
Giving customers greater control over their data
Digital empowerment has two components: allowing customers to update data held about them, and using data analytics to help customers make better decisions. Companies that master these components can not only improve customer satisfaction, but also unlock new sources of revenue. For example, CNH Industrial, a global manufacturer of agriculture and construction equipment, analyzes data on farmers’ activity collected from sensors in its products and uses the data to advise farmers on how to maximize crop yield.

4. Digital equity
Clarifying and potentially increasing the benefits customers receive in exchange for sharing their data
Companies can strengthen digital equity by providing greater monetary or service-in-kind benefits to customers in return for their data, as well as by simply improving the visibility of such benefits. For example, Kreditech is a German startup whose business model is built on assessing credit risks. The company gives out small loans on the basis of personal data from social networks or e-commerce retail accounts. Since its launch in 2012, Kreditech has issued 1.5 million loans, rewarding customers for sharing more information about themselves.

5. Digital inclusion
Using personal data to multiply positive societal outcomes
Many companies have datasets that, shared appropriately with organizations such as charities and NGOs, can create significant value for society. In 2013, telecommunications company Orange worked with a think tank to map economic activity in Côte d’Ivoire using data on mobile signals and call patterns. Though initially designed to align urban development efforts with the country’s economic needs, the effort also enables Orange to use the findings to refine its business operations in Côte d’Ivoire—and potentially commercialize the project’s methodology in other markets.
The benefits of corporate digital responsibility

Different firms may find some of these principles to be more important than others, given the inherent variety in business models and industry dynamics. But together, the principles set out the key tenets of how businesses can use personal data responsibly. Ranging from the foundational and often mandatory to the discretionary or aspirational, they share the twin objectives of better risk management and enhanced value creation (summarized in Figure 12).

Figure 12. Corporate digital responsibility delivers important benefits

By pursuing strategies that align with the five principles of corporate digital responsibility, businesses can realize a number of primary and secondary benefits.

<table>
<thead>
<tr>
<th>Stewardship</th>
<th>Transparency</th>
<th>Empowerment</th>
<th>Equity</th>
<th>Inclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved cost control and risk mitigation</td>
<td>Enhanced customer loyalty and market share</td>
<td>Better product differentiation and brand</td>
<td>New revenue streams</td>
<td></td>
</tr>
</tbody>
</table>

Primary benefits

Secondary benefits

The gap between principle and practice

While corporate digital responsibility principles can deliver significant benefits to companies, do business leaders recognize their importance? According to our research, the answer is yes across all dimensions (see Figure 13).

However, there is a gap between levels of importance attached to these principles and actions being taken to implement them. For example, while 81 percent of our survey respondents agree that giving customers greater control over their data is important, only 55 percent say their businesses are taking action to provide this control.

In the sections that follow, we identify leading examples of companies that are putting corporate digital responsibility principles into action. We also offer practical steps for getting started, with an eye toward helping businesses close the gap between perceived importance and action.

Figure 13. Gaps exist between perceived importance of and action taken on corporate digital responsibility principles

Businesses agree that the principles of corporate digital responsibility matter, but their actions to address them are falling short.

Q: Over the next three years, to what extent will the following strategies be important ways in which businesses can strengthen their reputation for the responsible use of data—and to what extent is your company already taking action in each of these areas?

Source: Accenture personal data survey 2014.

Source: Accenture Institute for High Performance.
In focus: Who leads the way?

In our survey results, we identified a group of businesses that we call corporate digital responsibility (CDR) leaders. Such companies:

- Are taking action across all five principles of corporate digital responsibility: stewardship, transparency, empowerment, equity and inclusion; and
- Have a board-level chief data or privacy officer or equivalent.

Twenty-two percent of our respondents met these two criteria, amounting to 130 businesses in all. Proportionally, more companies from the IT and technology industry made the grade than from any other industry, reflecting the maturity of personal data use in this sector (see Figure 14).

Figure 14. The proportion of CDR leader companies varies across industries

While IT and technology companies might be expected to have more advanced data-management practices, surprisingly, health and public-service organizations account for the smallest proportion of CDR leaders.

Proportion of companies in each industry sample that meet key CDR criteria

<table>
<thead>
<tr>
<th>Industry</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT &amp; technology</td>
<td>36%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>30%</td>
</tr>
<tr>
<td>Resources</td>
<td>26%</td>
</tr>
<tr>
<td>Products</td>
<td>25%</td>
</tr>
<tr>
<td>Financial services</td>
<td>22%</td>
</tr>
<tr>
<td>Retail/wholesale</td>
<td>17%</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>15%</td>
</tr>
<tr>
<td>Health &amp; public service</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.

Company size also makes a difference. Twenty-four percent of large companies (those with more than 500 employees) in our sample are CDR leaders, compared with 11 percent of small and medium-sized enterprises (those with 500 or fewer employees). This may suggest that smaller organizations find it harder to manage the costs associated with enhanced data-management capabilities.

Finally, geography matters. Companies operating in emerging economies are more likely to be CDR leaders than are their developed-market counterparts (see Figure 15).

Figure 15. Some countries have greater proportions of CDR leader companies than others

Reported levels of action on CDR principles are higher from businesses operating in emerging economies than from those in developed markets.

Proportion of companies in each country sample that meet key CDR criteria:

<table>
<thead>
<tr>
<th>Country</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>44%</td>
</tr>
<tr>
<td>India</td>
<td>29%</td>
</tr>
<tr>
<td>Brazil</td>
<td>27%</td>
</tr>
<tr>
<td>United States</td>
<td>22%</td>
</tr>
<tr>
<td>France</td>
<td>18%</td>
</tr>
<tr>
<td>Germany</td>
<td>14%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>13%</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
Steps to success

Turning the five principles of corporate digital responsibility into tangible actions will not be easy. However, by observing leading practices from companies around the world, as well as by drawing on Accenture’s own expertise, we have identified the following strategies and actions that provide a basis for getting started.
1. Digital stewardship

Managing data in a way that is consistent with stakeholder expectations is a challenge for all businesses, particularly given the ongoing threat of hacking. Building internal capabilities is clearly critical, but leading companies also seek to collaborate with industry partners to co-create secure platforms and drive standards across the ecosystem.

Fostering a culture of stewardship:
Weaving responsible management of data into an organization’s culture is vital for mitigating security risks. Ongoing employee training and regular tests to help people recognize and prevent security risks have proven effective in controlling the costs of data breaches. A global study by Symantec and the Ponemon Institute finds that the appointment of a C-level information security professional, a strong security posture and an incident management plan can all help reduce significantly the costs associated with a data breach. Indeed, ensuring board-level responsibility for data security and privacy can also powerfully signal a company’s commitment to data stewardship. A significant proportion of the resources and the IT and technology companies represented in our survey have a board-level chief data or privacy officer (or equivalent), but fewer than one-half of the health and public-service organizations do (see Figure 16).

Co-creating secure platforms:
Given the interconnected nature of the digital economy, businesses need to work across sectors to effectively protect customer data and manage security risks. For example, retail is particularly vulnerable to cybersecurity risks, and many recent data breaches have resulted from insecure encryption of credit card data. Loss of bank-card data in retail breaches carries a high price for financial institutions, too—almost US$1 million per organization in legal proceedings and lost business opportunities. In an effort to minimize future risks from the retail sector, credit card companies American Express, Discover, JCB, MasterCard, UnionPay and Visa, supported by dozens of banks, are collaborating to develop a new payments system.

The new system uses tokenization: conversion of a credit card number into a unique value that, by itself, holds no value to hackers.

Driving standards across the ecosystem:
Establishing robust data-security standards can enhance customers’ trust in companies and lead to the creation of new service offerings. Existing schemes—such as the Payment Card Industry Security Standards, ISO27001 on information security and the code of practice for protection of personally identifiable information in public clouds—are important standards that businesses can emulate. In addition, companies can participate in collaborative initiatives that help reduce risks across their ecosystem. For example, the Cyber-security Information Sharing Partnership is a joint industry-government initiative that provides a secure forum for companies to share knowledge on cyber-breaches. The information is analyzed by a team of security specialists from both the public and private sectors, providing member companies with regular threat and vulnerability assessments. Since the partnership’s launch in 2013, 750 organizations have now signed up for it.

Five steps to get started:
1. Compile and maintain a company-wide data inventory to record key assets, levels of sensitivity and data owners.
2. Establish clear data-governance structures with board-level responsibility.
3. Put a company-wide, locally tailored data-protection policy in place with business-unit champions and regular employee training.
4. Conduct regular resilience tests to model the impact of cyber-attacks, and put contingency plans in place.
5. Assess and monitor suppliers’ data-handling standards, updating procurement rules as needed.

Figure 16. The majority of businesses in many industries have board-level chief data or privacy officers

Health and public service organizations often handle the most sensitive types of personal data, yet in our survey they report the lowest proportion of chief data or privacy officers.

Q: Does your company currently have a board-level chief data officer or chief privacy officer or equivalent?

<table>
<thead>
<tr>
<th>Resources</th>
<th>Yes</th>
<th>No</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT &amp; technology</td>
<td>77%</td>
<td>9%</td>
<td>13%</td>
</tr>
<tr>
<td>Products</td>
<td>76%</td>
<td>19%</td>
<td>5%</td>
</tr>
<tr>
<td>Telecommunications &amp; media</td>
<td>76%</td>
<td>17%</td>
<td>7%</td>
</tr>
<tr>
<td>Financial services</td>
<td>64%</td>
<td>23%</td>
<td>10%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>56%</td>
<td>34%</td>
<td>13%</td>
</tr>
<tr>
<td>Retail/wholesale</td>
<td>50%</td>
<td>22%</td>
<td>28%</td>
</tr>
<tr>
<td>Health &amp; public service</td>
<td>49%</td>
<td>30%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Accenture personal data survey 2014.
2. Digital transparency

Leading companies are using digital technology and old-fashioned collaboration skills to increase openness across the data life cycle, embrace industry self-regulation and seek out independent accreditation.

Increasing openness across the data life cycle: Businesses need to be clear about their internal data practices to build and maintain trust with consumers throughout the data life cycle, from data collection to disposal. Simplifying terms of consent and privacy statements would help address customer concerns. Researchers at Carnegie Mellon University found that it would take 76 working days to read all of the privacy policies that a typical internet user encounters each year.\textsuperscript{41} To improve transparency for consumers, in 2014 Facebook shortened the length of its privacy policy by two-thirds and introduced explanatory graphics and interactive videos.\textsuperscript{42} Beyond such moves, businesses can also build intuitive and accessible dashboards of personal-data usage. For example, Google's data dashboard summarizes a user's data across Google products (such as Gmail and YouTube) and enables users to manage privacy settings for each service.

Embracing industry self-regulation: By establishing a dialogue on standards, organizations can implement industry-level self-regulation schemes that minimize potential regulatory disruption (depending on where they operate). For example, online advertising agencies in the United States initiated a self-regulatory program whereby they defined seven principles for making online advertising more consumer-friendly. Participating agencies commit to deploying multiple mechanisms to clearly inform consumers about the companies' data-collection practices, as well as to limit the retention of consumer data gathered for online advertising purposes.\textsuperscript{43}

Seeking out independent accreditation: Accreditation makes it easier for customers to identify organizations that collect, use and retain personal data in an ethical manner. For example, the Fair Data mark will be available only to those businesses that sign on to the scheme's principles and that have been audited. These principles include gaining appropriate consent for gathering personal data, giving customers access to their own data and not passing data on to other companies.\textsuperscript{44}

Five steps to get started:
1. Map the flow of personal data across its life cycle, from collection to disposal.
2. Open up different elements of the life cycle to user scrutiny (for example, through data dashboards and explicit data-disposal agreements).
3. Establish clear, intuitive privacy terms, conditions and policy statements.
4. Consider regular publication of a transparency report detailing third-party data requests.
5. Work with watchdogs to gain external accreditation.

3. Digital empowerment

To give customers more sovereignty over their data, businesses need to strengthen customer controls over data and help customers make better decisions.

Strengthening customer controls: By providing customers with clear, intuitive opt-in choices, organizations can help them control their data more effectively. ElevenPaths, a company created by Telefónica, launched the Latch app, which helps users strengthen the security of their digital identities. Latch has a digital switch that means users can turn their personal accounts (social media, email, bank accounts, credit and debit cards) on and off over the internet during given timeframes. This reduces their exposure to services that might generate sensitive information and increases data security for both consumers and businesses.\textsuperscript{45} Since its launch in 2013, the app has been downloaded more than 500,000 times.\textsuperscript{46}

Helping customers make better decisions: Businesses can also use data analytics to offer customers “decision services.” Bupa, a healthcare company, partnered with Australia’s George Institute for Global Health to launch the mobile phone app FoodSwitch, which helps consumers make better food choices. Users scan bar codes of packaged foods with their smartphones, and the app recommends a list of healthier substitutes. They can also save and share their food switches through social media. With a database of 17,000 packaged foods, FoodSwitch had been downloaded 400,000 times in Australia by mid-2013.\textsuperscript{47}

Five steps to get started:
1. Develop capabilities to facilitate real-time adjustment of privacy settings and sharing preferences.
2. Anticipate customers’ uptake of decision services by analyzing existing data—and craft strategies for meeting demand for such services.
3. Develop in-house capabilities or partner with analytics service providers to turn data inventories into insights valuable to customers.
4. Understand the economic trade-offs of increased customer empowerment (such as reductions in overdraft charges versus enhanced customer loyalty).
5. Assess the impact of using an “opt in” rather than “opt out” model of data collection.
4. Digital equity

To build a stronger two-way relationship with customers and their data, companies can enhance financial incentives for people to share their personal data, deliver benefits in real time and develop new applications of core capabilities.

Enhancing financial incentives:
By increasing the visibility of benefits (monetary or in-kind services) that customers can receive by sharing their personal data, businesses can differentiate their offerings and enhance customer loyalty. The social network tsū, launched in 2014, is a good example. Like typical social media platforms, tsū earns its revenue through on-site advertising—but the company shares 90 percent of its advertising revenue with users to attract people who demand greater value from their social content and the network.48

Delivering benefits in real time:
American Eagle, Best Buy, JCPenney, Macy’s, Target and other US-based retailers have partnered with shopkick, a smartphone app with 6 million users, to track and communicate with consenting shoppers in real time through location data. Rather than using GPS, shopkick creates a highly accurate inaudible signal unique to each store that can be automatically picked up by a smartphone’s internal microphone. Shopkick users share their location data with retailers, which then offer them rewards and discounts for walking into their stores. The gains have been mutual—in 2013, Shopkick drove more than US$500 million in revenue for its retail partners.49

Developing new applications of core capabilities: Organizations enjoying high levels of customer trust due to data security can drive new growth by providing data-management services. For example, Australia’s Commonwealth Bank offers its online banking customers a digital safety deposit box. Customers can use the box to store any type of digital file. The box is hosted on the bank’s cloud storage platform—with unlimited storage capacity. Customers can use it to save important documents such as payslips, contracts, scanned copies of passports and product warranties.50

Five steps to get started:
1. Map the flow of data-related benefits (tangible and intangible) between the organization and its customers.
2. Use analytics to assess customers’ perceptions of the fairness of benefit distribution.
3. Communicate more clearly the benefits customers can get at each point in their transactions with the organization.
4. Partner with service providers to find novel ways to enhance the customer experience.
5. Explore opportunities to offer data-management services.

5. Digital inclusion

A number of leading companies are enhancing digital inclusion by identifying and enabling societal application of data and proactively using data to inform public-policy debate.

Identifying and enabling societal application of data: Data gathered by corporations can be a boon for organizations seeking to tackle social problems in such areas as public health, urban planning and food wastage. In 2014, Johnson & Johnson agreed to give all of its clinical trial data to Yale University to help advance science and medicine, positioning itself favorably with consumers and medical professionals alike.51 Also in 2014, Twitter launched Data Grants to share tweet data with selected researchers to solve health and social issues ranging from urban flooding in Jakarta to food-borne gastrointestinal illness.52 Working with Gnip, the world’s largest social-data provider, researchers will also receive support in identifying, refining and delivering data needed for research. By identifying the right partners that would benefit from a company’s data assets, and by ensuring appropriate permissions protocols surrounding data sharing, companies can enhance their reputation and identify new growth opportunities.53

Informing public policy: By driving research and generating insights from data on public-policy challenges, businesses can help inform debate. Nest, a home automation company acquired by Google and best known for producing smart thermostats, is an example. Nest makes internet-connected smoke alarm and carbon monoxide monitors for households. Through its product, it collects real-time data about fires and carbon monoxide events from millions of users.54 In 2014, Nest produced a white paper analyzing field data on carbon monoxide events in Canada, the United Kingdom and the United States. Fire-service professionals and consumers are using the information to enhance their understanding of carbon monoxide leaks, which claim thousands of lives each year. Government bodies are using the analysis to improve regulatory codes and standards.55

Five steps to get started:
1. Identify assets from data inventories that have potential for wider societal application.
2. Assess whether social impact would be best achieved through in-house data analysis, collaboration with partners or open innovation.
3. Ensure consent from data providers, and establish sharing protocols that protect individual and corporate privacy.
4. Enhance in-house skills needed to work with external partners.
5. Identify alignment of social-impact strategies with commercial potential.
### Figure 17. A summary checklist for action

<table>
<thead>
<tr>
<th>Principle</th>
<th>Leading strategies</th>
<th>Steps to get started</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stewardship</td>
<td>Fostering a culture of stewardship</td>
<td>1. Compile and maintain a company-wide data inventory to record key assets, levels of sensitivity and data owners.</td>
</tr>
<tr>
<td></td>
<td>Co-creating secure platforms</td>
<td>2. Establish clear data-governance structures with board-level responsibility.</td>
</tr>
<tr>
<td></td>
<td>Driving standards across the ecosystem</td>
<td>3. Put a company-wide, locally tailored data-protection policy in place with business-unit champions and regular employee training.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Conduct regular resilience tests to model the impact of cyber-attacks, and put contingency plans in place.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Assess and monitor suppliers’ data-handling standards, updating procurement rules as needed.</td>
</tr>
<tr>
<td>Transparency</td>
<td>Increasing openness across the data life cycle</td>
<td>1. Map the flow of personal data across its lifecycle, from collection to disposal.</td>
</tr>
<tr>
<td></td>
<td>Embracing industry self-regulation</td>
<td>2. Open up different elements of the lifecycle to user scrutiny (for example, through data dashboards and explicit data-disposal agreements).</td>
</tr>
<tr>
<td></td>
<td>Seeking out independent accreditation</td>
<td>3. Establish clear, intuitive privacy terms, conditions and policy statements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Consider regular publication of a transparency report detailing third-party data requests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Work with watchdogs to gain external accreditation.</td>
</tr>
<tr>
<td>Empowerment</td>
<td>Strengthening customer controls</td>
<td>1. Develop capabilities to facilitate real-time adjustment of privacy settings and sharing preferences.</td>
</tr>
<tr>
<td></td>
<td>Helping customers make better decisions</td>
<td>2. Anticipate customers’ uptake of decision services by analyzing existing data—and craft strategies for meeting demand for such services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Develop in-house capabilities or partner with analytics service providers to turn data inventories into insights valuable to customers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Understand the economic trade-offs of increased customer empowerment (such as reductions in overdraft charges versus enhanced customer loyalty).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Assess the impact of using an ”opt in” rather than ”opt out” model of data collection.</td>
</tr>
<tr>
<td>Equity</td>
<td>Enhancing financial incentives</td>
<td>1. Map the flow of data-related benefits (tangible and intangible) between the organization and its customers.</td>
</tr>
<tr>
<td></td>
<td>Delivering benefits in real-time</td>
<td>2. Use analytics to assess customers’ perceptions of the fairness of benefit distribution.</td>
</tr>
<tr>
<td></td>
<td>Developing new applications of core capabilities</td>
<td>3. Communicate more clearly the benefits customers can get at each point in their transactions with the organization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Partner with service providers to find novel ways to enhance the customer experience.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Explore opportunities to offer data-management services.</td>
</tr>
<tr>
<td>Inclusion</td>
<td>Identifying and enabling societal application of data</td>
<td>1. Identify assets from data inventories that have potential for wider societal application.</td>
</tr>
<tr>
<td></td>
<td>Informing public policy</td>
<td>2. Assess whether social impact would be best achieved through in-house data analysis, collaboration with partners or open innovation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Ensure consent from data providers and establish sharing protocols that protect individual and corporate privacy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enhance in-house skills needed to work with external partners.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Identify alignment of social–impact strategies with commercial potential.</td>
</tr>
</tbody>
</table>
Where next?

Gathering and analyzing personal data has helped businesses develop better products and services for their customers. But this activity is likely to become increasingly difficult if companies do not make major changes to their approach. Emerging risks—posed by shifts in customer attitudes and behaviors, government regulations, alternatives presented by startups and greater scrutiny from NGOs—could reduce the supply and quality of personal data that businesses can access. Putting corporate digital responsibility principles into practice can help companies manage these risks and transform them into opportunities for growth and competitive differentiation. But our research shows that organizations have a long way to go before these principles are fully implemented. The need to take action sooner rather than later, though, is paramount. More disrupters are heading our way. Savvy companies will start preparing now for these tests—before their rivals can.

Adapting to the Internet of Things

Embedded technologies that connect and share intelligence with people and the external environment—the Internet of Things (IoT)—could present significant challenges for businesses seeking to manage data responsibly. In the same way that companies handling large amounts of sensitive data can become targets for hackers, the many “nodes” of data concentration that characterize the IoT may also be prone to cybercrime. Ensuring transparency in data handling could become more complex as the IoT grows more sophisticated, especially with an increase in network automation. Businesses may have difficulty understanding and controlling how personal data is used—particularly if they do not own the assets through which such data is channeled. Enhancing the equity of the IoT system could help. Consumers are likely to feel more comfortable with a more sophisticated IoT if they believe they can benefit from it. Similarly, empowering consumers to control what happens to their data should help build trust. Businesses will need to balance automation of the IoT system with enabling consumers to adjust privacy settings on smart devices, even post-sale.

Proliferating questions about responsible business

Questions about what constitutes responsible business activity in a digital economy are likely to grow in number and complexity. For example, how will businesses manage the increased transparency of online pricing systems that discriminate on the basis of location or income? What role do businesses have in closing the digital divide between the “tech-haves” and “tech have-nots”? What parameters should govern the use of sentiment trackers and the potential for mood manipulation that accompanies them? Corporate digital responsibility principles can help businesses address immediate challenges related to such questions while also preparing for future disruption.

The story of using personal data is the story of technology itself. As with any new technological development or leap in scientific capability, progress tests the boundaries of consumer understanding and comfort. As digital technologies open up new avenues for improving economic health and personal well-being—from neuroscience and artificial intelligence to cognitive computing—navigating inherently personal customer attitudes will be a key determinant of success for businesses. But by developing strategies that align with corporate digital responsibility principles—stewardship, transparency, empowerment, equity and inclusion—businesses can take a more disciplined approach to managing future disruption. The future of the digital economy—and the benefits it delivers to human beings and organizations—relies on businesses doing so swiftly and effectively.
About the research

Three research elements underpin this study:

1. **An online survey** of 578 business professionals across seven economies and multiple industries (see Figures 18 and 19). Conducted by Kadence International between July and August 2014, the survey targeted and screened for individuals with a high level of exposure to the issues surrounding personal data, such as those working in customer service, business development, marketing and sales. Eighty percent of the respondents came from large enterprises (those with more than 500 employees) and 20 percent from small and medium-sized enterprises (those with 500 or fewer employees).

![Figure 18. Breakdown of respondents by geography](image)

- France: 18%
- Germany: 17%
- United States: 16%
- India: 14%
- United Kingdom: 14%
- Brazil: 11%
- China: 10%

![Figure 19. Number of respondents by industry](image)

- Products*: 111
- Financial services: 91
- Health & public service: 83
- IT & technology: 59
- Telecommunications & media: 59
- Retail/wholesale: 54
- Resources: 53
- Manufacturing: 50
- Other: 18

*Products = automotive, consumer goods and services, industrial equipment, logistics and distribution, tourism, and transportation

2. **Interviews** with eight academic experts. They are: Dr. Orla Lynskey (The London School of Economics and Political Science); Professor Ian Brown (Oxford Internet Institute); Dr. Mark Coté (King’s College London); Professor Christopher Millard (Queen Mary University of London); and Dr. Marie Griffiths, Dr. Gordon Fletcher, Dr. Maria Kutar and Dr. Aleksej Heinze (all of the Centre for Digital Business, Salford Business School, United Kingdom).

3. **Secondary research**, including literature reviews, case studies and industry-leading practice undertaken by Accenture specialists.
References

4Ibid.
10DuckDuckGo corporate website.
14Personal.com corporate website.
15Ghostery corporate website.
25“Datacoup corporate website.
31“Boom Triggered by NSA; German Email Services Report Surge in Demand,” Spiegel Online International, August 26, 2013.
35Kreditech corporate website.
39Cyber-security Information Sharing Partnership website.
43Fair Data website.
44“ElevenPaths website.
45ElevenPaths website.
46“Letch Google Play page.
50Commonwealth Bank of Australia corporate website.
51“Johnson & Johnson Announces Clinical Trial Data Sharing Agreement with Yale School of Medicine,” PR Newswire, January 30, 2014.
52“Twitter’s Data Grants Will Be Used to Research Food Poisoning, Cancer, Happiness,” Gigaom, April 17, 2014.

Further reading


About the Authors
Tim Cooper is a London-based senior manager in Accenture Strategy’s Sustainability practice, where he leads the global capability on digital responsibility.
Ryan LaSalle is managing director of growth and strategy for Accenture Security and is based in Washington, D.C.
Kuangyi Wei is an associate manager at the Accenture Institute for High Performance.

Contact
For more information about this report, please contact:
tim.e.cooper@accenture.com
ryan.m.lasalle@accenture.com

Acknowledgements
The authors would like to thank the following individuals for their contributions to this study:
Julian Allen, Allan Alter, Samira Azzam, Renee Byrnes, Phil Davies, Dan Elron, Gwen Harrigan, Benjamin Hayes, Laurie Henneborn, Paul Johnson, Peter Lacy, David Light, Archie Maitland, Raghav Narsalay, Paul Nunes, Armen Ovanessoff, Anton Pichler, Kevin Richards, Matthew Robinson, Jade Siu, Niaz Souti, Mark Spelman, Florian Thoma, Jan-Boris Wojtan, Alan Woodhouse and Barbara Wynne.

About the Accenture Institute for High Performance
The Accenture Institute for High Performance develops and communicates breakthrough ideas and practical insights on management issues, economic trends and the impact of new and improving technologies. Its worldwide team of researchers works in collaboration with Accenture’s strategy, digital, technology and operations business leaders to demonstrate, through original, rigorous research and analysis, how organizations become and remain high performers.

About Accenture Security
Accenture Security offers holistic strategies and solutions to help clients prevent, intercept and remediate security risks, providing the resilience required to drive, high performance and growth. With a focus on outcomes and the tight integration of security strategies with business goals, Accenture innovates with advanced, intelligent solutions that preempt, detect and respond to threats with agility. Accenture has more than 20 years of experience helping corporations and governments across the globe use security to both defend organizations against malicious threats and empower them to operate new business processes and drive innovation while maintaining acceptable levels of risk.

About Accenture Strategy
Accenture Strategy operates at the intersection of business and technology. We bring together our capabilities in business, technology, operations and function strategy to help our clients envision and execute industry-specific strategies that support enterprise wide transformation. Our focus on issues related to digital disruption, competitiveness, global operating models, talent and leadership help drive both efficiencies and growth. For more information, follow @AccentureStrat or visit www.accenture.com/strategy

About Accenture
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2016 Accenture
All rights reserved.
Accenture, its logo, and High performance. Delivered. are trademarks of Accenture.