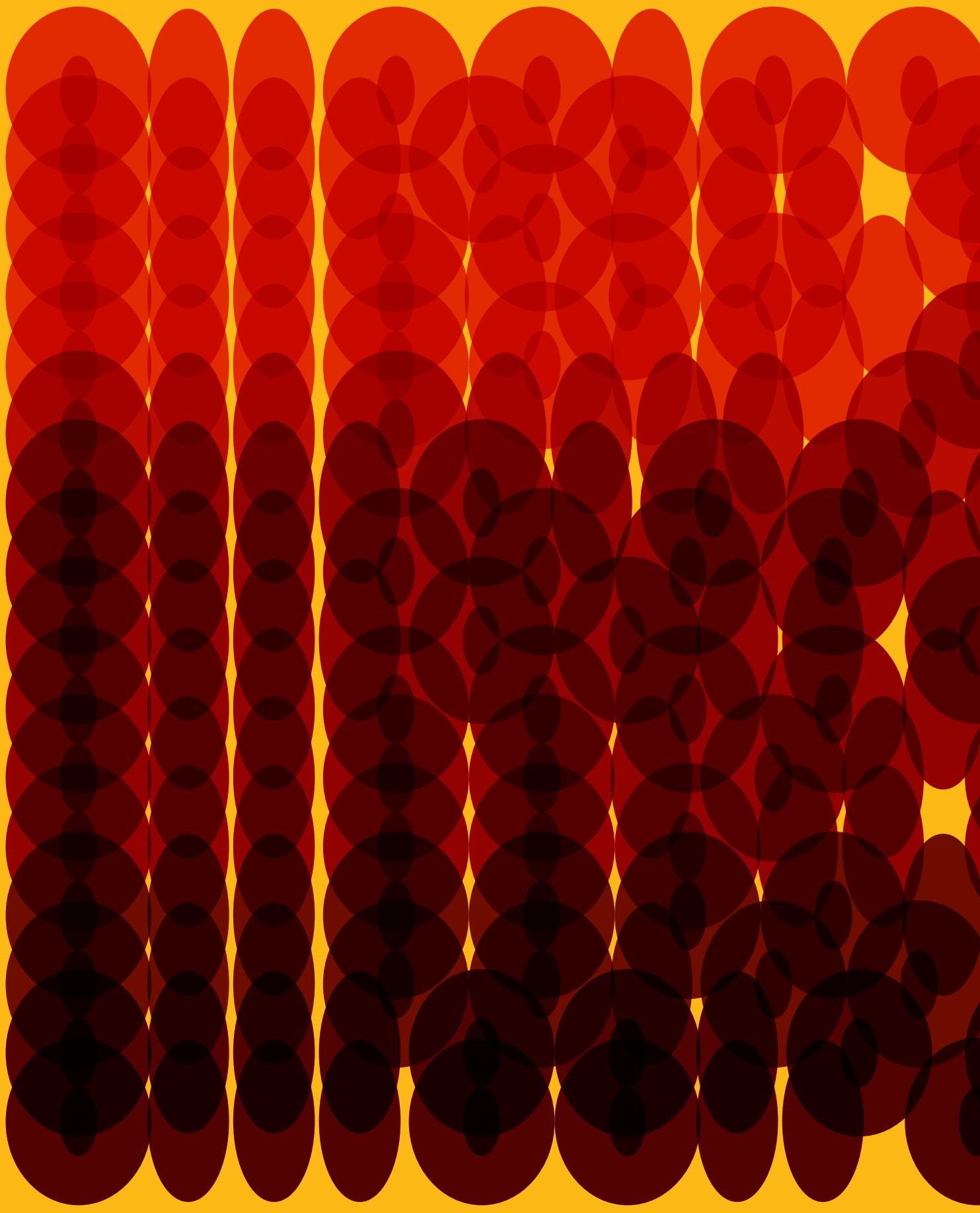


Timothy Morey is the vice president of innovation strategy at frog, a global product strategy and design firm. **Theodore "Theo" Forbath** is the global vice president of digital transformation at Cognizant. **Allison Schoop** is an associate strategy director at frog.

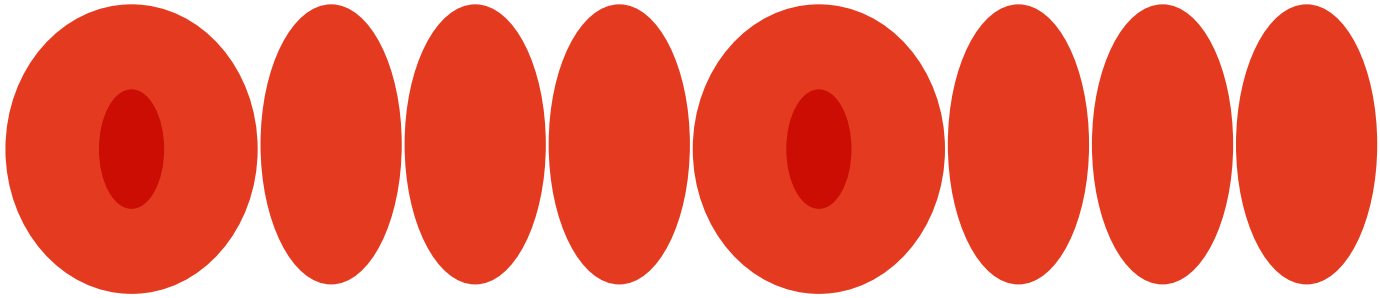
CUSTOMER DATA: DESIGNING FOR TRANSPARENCY AND TRUST

BY

TIMOTHY MOREY

THEODORE "THEO" FORBATH

ALLISON SCHOOP



WITH THE EXPLOSION OF DIGITAL TECHNOLOGIES, COMPANIES ARE SWEEPING UP VAST QUANTITIES OF DATA ABOUT CONSUMERS' ACTIVITIES, BOTH ONLINE AND OFF. FEEDING THIS TREND ARE NEW SMART, CONNECTED PRODUCTS—FROM FITNESS TRACKERS TO HOME SYSTEMS—THAT GATHER AND TRANSMIT DETAILED INFORMATION.

Though some companies are open about their data practices, most prefer to keep consumers in the dark, choose control over sharing, and ask for forgiveness rather than permission. It's also not unusual for companies to quietly collect personal data they have no immediate use for, reasoning that it might be valuable someday.

As current and former executives at frog, a firm that helps clients create products and services that leverage users' personal data, we believe this shrouded approach to data gathering is shortsighted. Having free use of customer data may confer near-term advantages. But our research shows that consumers are aware that they're under surveillance—even though they may be poorly informed about the specific types of data collected about them—and are deeply anxious about how their personal information may be used.

In a future in which customer data will be a growing source of competitive advantage, gaining consumers' confidence will be key. Companies that are transparent about the information they gather, give customers control of their personal data, and offer fair value in return for it will be trusted and will earn ongoing and even expanded access. Those that conceal how they use personal data and fail to provide value for it stand to lose customers' goodwill—and their business.

The Expanding Scope of Data

The internet's first personal data collectors were websites and applications. By tracking users' activities online, marketers could deliver targeted advertising and content. More recently, intelligent technology in physical products has allowed companies in many industries to collect new types of information, including users' locations and behavior. The personalization this data allows, such as constant adaptation to users' preferences, has become central to the product experience. (Google's Nest thermostat, for example, autonomously adjusts heating and cooling as it learns home owners' habits.)

The rich new streams of data have also made it possible to tackle complex challenges in fields such as health care, environmental protection, and urban planning. Take Medtronic's digital blood-glucose meter. It wirelessly connects an implanted sensor to a device that alerts patients and health care providers that blood-glucose levels are nearing troubling thresholds, allowing preemptive treatments. And the car service Uber has recently agreed to share ride-pattern data with Boston officials so that the city can improve transportation planning and prioritize road maintenance. These

Idea in Brief

THE PROBLEM
Though consumers worry about how their personal data is gathered and used, they're surprisingly ignorant of what data they reveal when they're online, and most companies opt not to enlighten them. This dynamic erodes trust in firms and customers' willingness to share information.

THE SOLUTION
Companies need to design products and services with transparency and data privacy in mind. They must provide customers with appropriate value in exchange for data, educate them about how it is collected, and allow them to have control over it.

BEST PRACTICE
Disney devised electronic wristbands that give park visitors access to attractions and hotel rooms and allow them to charge food. Disney uses the bands to collect data on customers but clearly spells out its practices and privacy policies. The trade-offs are transparent to the customers, who find the convenience and other benefits the bands offer worthwhile.

and countless other applications are increasing the power—and value—of personal data.

Of course, this flood of data presents enormous opportunities for abuse. Large-scale security breaches, such as the recent theft of the credit card information of 56 million Home Depot customers, expose consumers' vulnerability to malicious agents. But revelations about companies' covert activities also make consumers nervous. Target famously aroused alarm when it was revealed that the retailer used data mining to identify shoppers who were likely to be pregnant—in some cases before they'd told anyone.

At the same time, consumers appreciate that data sharing can lead to products and services that make their lives easier and more entertaining, educate them, and save them money. Neither companies nor their customers want to turn back the clock on these technologies—and indeed the development and adoption of products that leverage personal data continue to soar. The consultancy Gartner estimates that nearly 5 billion connected "things" will be in use in 2015—up 30% from 2014—and that the number will quintuple by 2020.

Resolving this tension will require companies and policy makers to move the data privacy discussion beyond advertising use and the simplistic notion that aggressive data collection is bad. We believe the answer is more nuanced guidance—specifically, guidelines that align the interests of companies and their customers, and ensure that both parties benefit from personal data collection.

Consumer Awareness and Expectations

To help companies understand consumers' attitudes about data, in 2014 we surveyed 900 people in five countries—the United States, the United Kingdom, Germany, China, and India—whose demographic mix represented the general online population. We looked at their awareness of how their data was collected and used, how they valued different types of data, their feelings about privacy, and what they expected in return for their data.

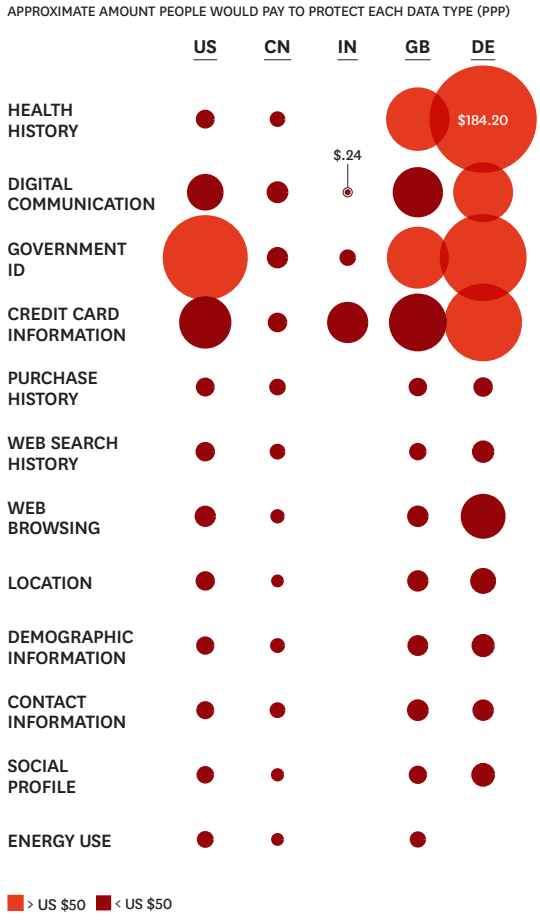
To find out whether consumers grasped what data they shared, we asked, "To the best of your knowledge, what personal information have you put online yourself, either directly or indirectly, by your use of online services?" While awareness varied by country—Indians are the most cognizant of their data trail and Germans the least—overall the survey revealed an astonishingly low recognition of the specific types of information tracked online. On average, only 25%

IN THE DARK ABOUT DATA

While most people are broadly aware that companies collect data on them, they're surprisingly uninformed about the specific types of data they give up when they go online.

PUTTING A PRICE ON DATA

Surveys of consumers in the United States, China, India, Great Britain, and Germany reveal that they value some types of information much more highly than others.



of people knew that their data footprints included information on their location, and just 14% understood that they were sharing their web-surfing history too. (See the exhibit "In the Dark about Data.")

It's not as if consumers don't realize that data about them is being captured, however; 97% of the people surveyed expressed concern that businesses and the government might misuse their data. Identity theft was a top concern (cited by 84% of Chinese respondents at one end of the spectrum and 49% of Indians at the other). Privacy issues also ranked high; 80% of Germans and 72% of Americans are reluctant to share information with businesses because they "just want to maintain [their] privacy." So consumers clearly worry about their personal data—even if they don't know exactly what they're revealing.

To see how much consumers valued their data, we did conjoint analysis to determine what amount survey participants would be willing to pay to protect different types of information. (We used purchasing parity rather than exchange rates to convert all amounts to U.S. dollars.) Though the value assigned varied widely among individuals, we are able to determine, in effect, a median, by country, for each data type.

The responses revealed significant differences from country to country and from one type of data to another. (See the exhibit "Putting a Price on Data.") Germans, for instance, place the most value on their personal data, and Chinese and Indians the least, with British and American respondents falling in the middle. Government identification, health, and credit card information tended to be the most highly valued across countries, and location and demographic information among the least.

We don't believe this spectrum represents a "maturity model," in which attitudes in a country predictably shift in a given direction over time (say, from less privacy conscious to more). Rather, our findings reflect fundamental dissimilarities among cultures. The cultures of India and China, for example, are considered more hierarchical and collectivist, while Germany, the United States, and the United Kingdom are more individualistic, which may account for their citizens' stronger feelings about personal information.

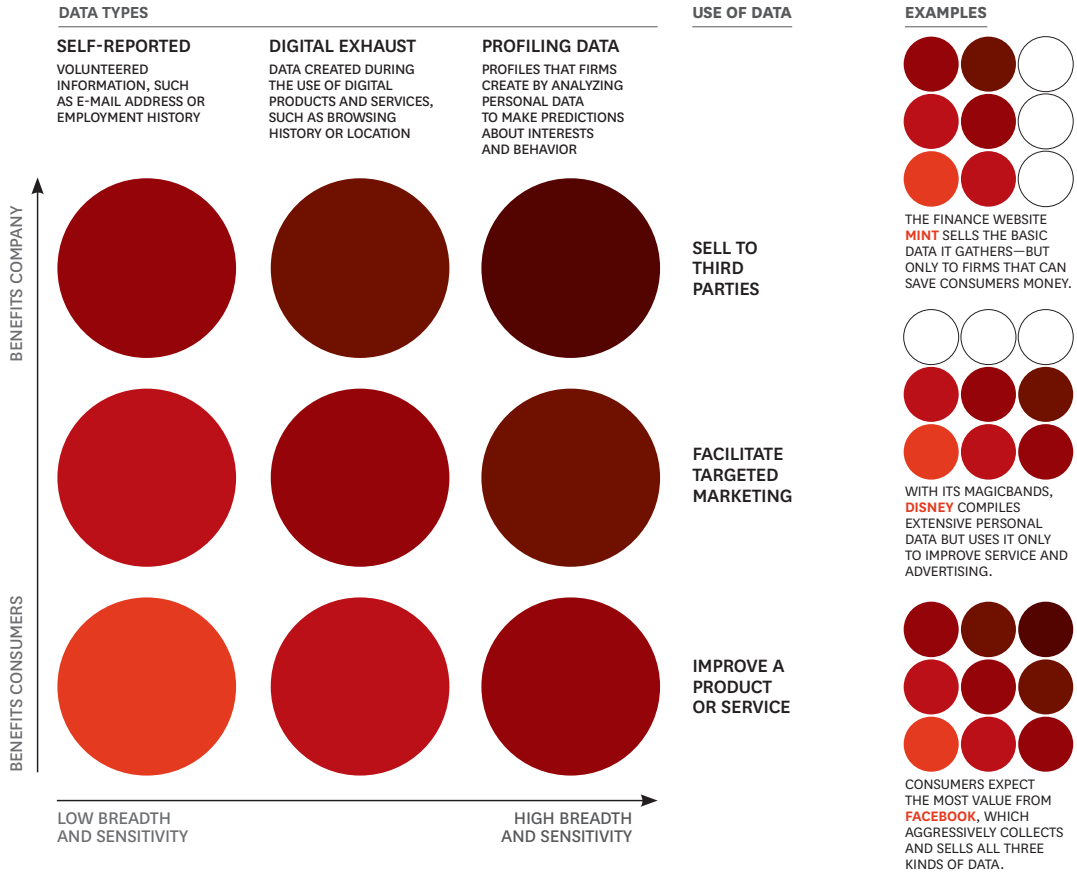
The Need to Deliver Value

If companies understand how much data is worth to consumers, they can offer commensurate value in return for it. Making the exchange transparent will be increasingly important in building trust.

A lot depends on the type of data and how the firm is going to use it. Our analysis looked at three categories: (1) *self-reported data,* or information people volunteer about themselves, such as their e-mail addresses, work and educational history, and age and gender; (2) *digital exhaust,* such as location data and browsing history, which is created when using mobile devices, web services, or other connected technologies; and (3) *profiling data,* or personal profiles used to make predictions about individuals' interests and behaviors, which are derived by combining self-reported, digital exhaust,

SWAPPING VALUE FOR DATA

The value people put on data rises as its breadth and sensitivity increase and its use shifts benefits toward companies. And the more people value data, the more they expect companies to provide in return for it.



and other data. Our research shows that people value self-reported data the least, digital exhaust more, and profiling data the most.

We also examined three categories of data use: (1) *making a product or service better,* for example, by allowing a map application to recommend a route based on a user's location; (2) *facilitating targeted marketing or advertising,* such as ads based on a user's browsing history; and (3) *generating revenues through resale*, by, say, selling credit card purchase data to third parties.

Our surveys reveal that when data is used to improve a product or service, consumers generally feel the enhancement itself is a fair trade for their data. But consumers expect more value in return for data used to target marketing, and the most value for data that will be sold to third parties. In other words, the value consumers place on their data rises as its sensitivity and breadth increase from basic information that is voluntarily shared to detailed information about the consumer that the firm derives through analytics, and as its uses go from principally benefiting the consumer (in the form of product improvements) to principally benefiting the firm (in the form of revenues from selling data). (See the exhibit "Swapping Value for Data.")

Let's look now at how some companies manage this trade-off.

Samsung's Galaxy V smartphone uses digital exhaust to automatically add the contacts users call most to a favorites list. Most customers value the convenience enough to opt in to the feature—effectively agreeing to swap data for enhanced performance.

Data Laws Are Growing Fiercer

In a landmark case in September 2014, Germany ordered Google to stop violating its Federal Telemedia Act and Federal Data Protection Act. Under fire was Google's practice of compiling individual user data from its various services into detailed user profiles without users' consent.

Google was already facing fines from six other European countries for breaking the European Union's rules on privacy, but Germany's decision to force the company to change its practices to comply with the country's particular data protection laws set a new precedent. Among the list of required measures was a directive that Google meet Germany's stringent privacy options, in particular, providing a "right to forget" service through which people could remove any personal information they did not want online. This marked a new era for global web-based businesses.

As the *New York Times* has reported, many countries now default to Europe's data protection rules, adopting passages from the EU's strict regulations almost word for word. At the same time, they add regional legal interpretations. Brazil requires that tech companies get direct permission from users before sharing their data with online advertisers and marketers; South Africa forbids the transmission of people's personal data to countries that don't replicate its privacy laws; and South Korea grants individuals the right to access at any time the online information that companies hold about them. The United States is exceptional in that its personal data laws are not clearly defined and not enforced by any independent governing body except in the case of data related to health care or minors. However, as Google's experiences show, U.S.-based companies that operate internationally may be forced to comply with more-stringent data laws elsewhere.

Google's predictive application Google Now harnesses profiling data to create an automated virtual assistant for consumers. By sifting through users' e-mail, location, calendar, and other data, Google Now can, say, notify users when they need to leave the office to get across town for a meeting and provide a map for their commute. The app depends on more-valuable types of personal data but improves performance enough that many users willingly share it. Our global survey of consumers' attitudes toward predictive applications finds that about two-thirds of people are willing (and in some cases eager) to share data in exchange for their benefits.

Disney likewise uses profiling data gathered by its MagicBand bracelet to enhance customers' theme park and hotel experiences and create targeted marketing. By holding the MagicBand up to sensors around Disney facilities, wearers can access parks, check in at reserved attractions, unlock their hotel doors, and charge food and merchandise. Users hand over a lot of data, but they get convenience and a sense of privileged access in return, making the trade-off worthwhile. Consumers know exactly what they're signing on for, because Disney clearly spells out its data collection policies in its online MagicBand registration process, highlighting links to FAQs and other information about privacy and security.

Firms that sell personal information to third parties, however, have a particularly high bar to clear, because consumers expect the most value for such use of their data. The personal finance website Mint makes this elegant exchange: If a customer uses a credit card abroad and incurs foreign transaction fees, Mint flags the fees and refers the customer to a card that doesn't charge them. Mint receives a commission for the referral from the new-card issuer, and the customer avoids future fees. Mint and its customers both collect value from the deal.

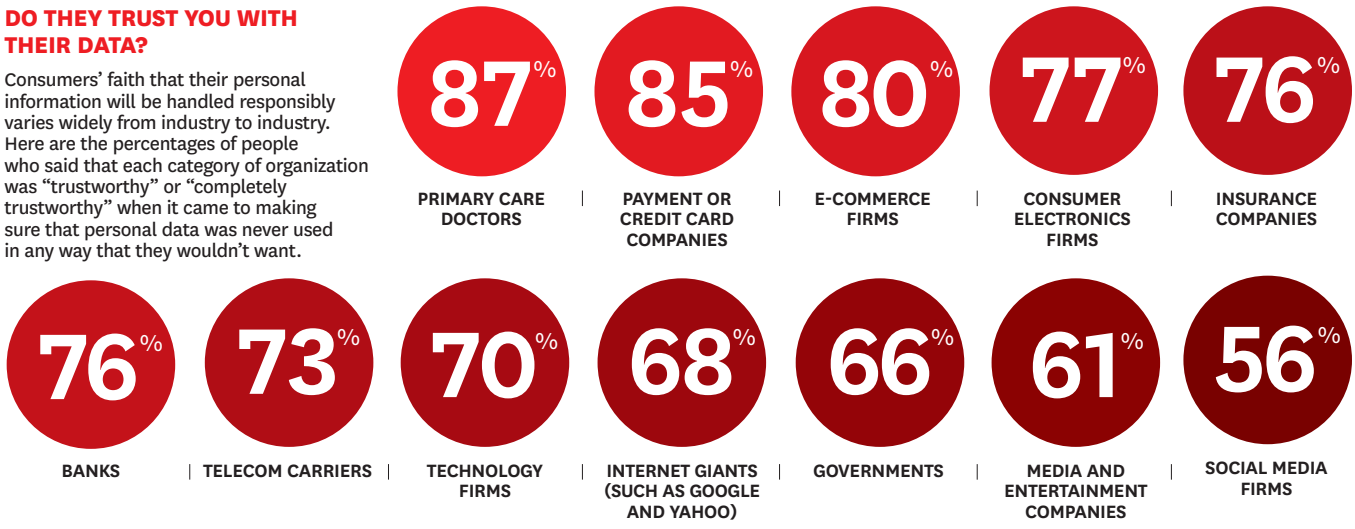
Trust and Transparency

Firms may earn access to consumers' data by offering value in return, but trust is an essential facilitator, our research shows. The more trusted a brand is, the more willing consumers are to share their data.

Numerous studies have found that transparency about the use and protection of consumers' data reinforces trust. To assess this effect ourselves, we surveyed consumers about 46 companies representing seven categories of business around the world. We asked them to rate the firms on the following scale: *completely trustworthy* (respondents would freely share sensitive personal data with a firm because they trust the firm not to misuse it); *trustworthy* (they would "not mind" exchanging sensitive data for a desired service); *untrustworthy* (they would provide sensitive data only if required to do so in exchange for an essential service); and *completely untrustworthy* (they would never share sensitive data with the firm).

After primary care doctors, new finance firms such as PayPal and China's Alipay received the highest ratings on this scale, followed by e-commerce companies, consumer electronics makers, banks and insurance companies, and telecommunications carriers. Next came internet leaders (such as Google and Yahoo) and the government. Ranked below these organizations were retailers and entertainment companies, with social networks like Facebook coming in last. (See the exhibit "Do They Trust You with Their Data?")

A firm that is considered untrustworthy will find it difficult or impossible to collect certain types of data, regardless of the value offered in exchange. Highly



trusted firms, on the other hand, may be able to collect it simply by asking, because customers are satisfied with past benefits received and confident the company will guard their data. In practical terms, this means that if two firms offer the same value in exchange for certain data, the firm with the higher trust will find customers more willing to share. For example, if Amazon and Facebook both wanted to launch a mobile wallet service, Amazon, which received good ratings in our survey, would meet with more customer acceptance than Facebook, which had low ratings. In this equation, trust could be an important competitive differentiator for Amazon.

Approaches That Build Trust

Many have argued that the extensive data collection today's business models rely on is fraught with security, financial, and brand risks. MIT's Sandy Pentland and others have proposed principles and practices that would give consumers a clear view of their data and control over its use, reducing firms' risks in the process. (See "With Big Data Comes Big Responsibility," HBR, November 2014.)

We agree that these business models are perilous and that risk reduction is essential. And we believe reasoned policies governing data use are important. But firms must also take the lead in educating consumers about their personal data. Any firm that thinks it's sufficient to simply provide disclosures in an end-user licensing agreement or present the terms and conditions of data use at sign-up is missing the point. Such moves may address regulatory requirements, but they do little if anything to help consumers.

Consider the belated trust-building efforts under way at Facebook. The firm has been accused of riding roughshod over user privacy in the past, launching services that pushed the boundaries on personal data use and retreating only in the face of public backlash or the threat of litigation. Facebook Beacon, which exposed users' web activities without their permission or knowledge, for example, was pulled only after a barrage of public criticism.

More recently, however, Facebook has increased its focus on safeguarding privacy, educating users, and giving them control. It grasps that trust is no longer just "nice to have." Commenting in a *Wired* interview on plans to improve Facebook Login, which allows users to log into third-party apps with their Facebook credentials, CEO Mark Zuckerberg explained that "to get to the next level and become more ubiquitous, [Facebook Login] needs to be trusted even more. We're a bigger company now and people have more questions. We need to give people more control over their information so that everyone feels comfortable using these products." In January 2015 Facebook launched Privacy Basics, an easy-to-understand site that explains what others see about a user and how people can customize and manage others' activities on their pages.

Like Facebook, Apple has had its share of data privacy and security challenges—most recently when celebrity iPhoto accounts were hacked—and is taking those concerns ever more seriously.

Using Humor to Teach About Data Privacy

Britain's Channel 4 does an excellent job of educating its viewers about its data collection and privacy policy. On a dedicated website, the TV station details the type of information gathered and how it's used, and summarizes the policy in a short, entertaining video with comedian Alan Carr. As he deadpans, "We'll ask you for your name, e-mail, and a few other details. Now, I know what you're thinking. Why should you give us your name and inside-leg measurement? What will we do with that information?" He then explains that viewers maintain complete control of their data, that it will never be sold, and that it can be erased from the system at their request at any time.

The video, which has been watched millions of times, is one component of Channel 4's vigorous Viewer Promise program. According to Steven Forde, the channel's director of viewer relationship management, these efforts have built trust and encouraged data sharing: Eleven million viewers have registered on the site. Eighty percent of them volunteer their address details, though they're not required to, and fewer than 0.01% opt out of targeted advertising.

WWW.CHANNEL4.COM/4VIEWERS/VIEWER-PROMISE/OURPROMISE

Particularly as Apple forays into mobile payments and watch-based fitness monitoring, consumer trust in its data handling will be paramount. CEO Tim Cook clearly understands this. Launching a "bid to be conspicuously transparent," as the *Telegraph* put it, Apple recently introduced a new section on its website devoted to data security and privacy. At the top is a message from Cook. "At Apple, your trust means everything to us," he writes. "That's why we respect your privacy and protect it with strong encryption, plus strict policies that govern how all data is handled....We believe in telling you up front exactly what's going to happen to your personal information and asking for your permission before you share it with us."

On the site, Apple describes the steps taken to keep people's location, communication, browsing, health tracking, and transactions private. Cook explains, "Our business model is very straightforward: We sell great products. We don't build a profile based on your email content or web browsing habits to sell to advertisers. We don't 'monetize' the information you store on your iPhone or in iCloud. And we don't read your email or your messages to get information to market to you. Our software and services are designed to make our devices better. Plain and simple." Its new stance earned Apple the highest possible score—six stars—from the nonprofit digital rights organization Electronic Frontier Foundation, a major improvement over its 2013 score of one star.

Enlightened Data Principles

Facebook and Apple are taking steps in the right direction but are fixing issues that shouldn't have arisen in the first place. Firms in that situation start the trust-building process with a handicap. Forward-looking companies, in contrast, are incorporating data privacy and security considerations into product development from the start, following three principles. The examples below each highlight one principle, but ideally companies should practice all three.

Teach your customers. Users can't trust you if they don't understand what you're up to. Consider how one of our clients educates consumers about its use of highly sensitive personal data.

This client, an information exchange for biomedical researchers, compiles genomic data on anonymous participants from the general public. Like all health information, such data is highly sensitive and closely guarded. Building trust with participants at the outset is essential. So the project has made education and informed consent central to their experience. Before receiving a kit for collecting a saliva sample for analysis, volunteers must watch a video about the potential consequences of having their genome sequenced—including the possibility of discrimination in employment and insurance—and after viewing it, must give a preliminary online consent to the process. The kit contains a more detailed hard-copy agreement that, once signed and returned with the sample, allows the exchange to

include the participant's anonymized genomic information in the database. If a participant returns the sample without the signed consent, her data is withheld from the exchange. Participants can change their minds at any time, revoking or granting access to their data.

Give them control. The principle of building control into data exchange is even more fully developed in another project, the Metadistretti e-monitor, a collaboration between frog, Flextronics, the University Politecnico di Milano, and other partners. Participating cardiac patients wear an e-monitor, which collects ECG data and transmits it via smartphone to medical professionals and other caregivers. The patients see all their own data and control how much data goes to whom, using a browser and an app. They can set up networks of health care providers, of family and friends, or of fellow users and patients, and send each different information. This patient-directed approach is a radical departure from the tradition of paternalistic medicine that carries over to many medical devices even today, with which the patient doesn't own his data or even have access to it.

Deliver in-kind value. Businesses needn't pay users for data (in fact, our research suggests that offers to do so actually reduce consumers' trust). But as we've discussed, firms do have to give users value in return.

The music service Pandora was built on this principle. Pandora transparently gathers self-reported data; customers volunteer their age, gender, and zip code when they sign up, and as they use the service they tag the songs they like or don't like. Pandora takes that information and develops a profile of each person's musical tastes so that it can tailor the selection of songs streamed to him or her; the more data users provide, the better the tailoring becomes. In the free version of its service, Pandora uses that data to target advertising. Customers get music they enjoy at no charge and ads that are more relevant to them. Consumers clearly find the trade satisfactory; the free service has 80 million active subscribers.

In designing its service, Pandora understood that customers are most willing to share data when they know what value they'll receive in return. It's hard to set up this exchange gracefully, but one effective approach is to start slowly, asking for a few pieces of low-value data that can be used to improve a service. Provided that there's a clear link between the data collected and the enhancements delivered, customers will become more comfortable sharing additional data as they grow more familiar with the service.

IF YOUR company still needs another reason to pursue the data principles we've described, consider this: Countries around the world are clamping down on businesses' freewheeling approach to personal data. (See the sidebar "Data Laws Are Growing Fiercer.")

There is an opportunity for companies in this defining moment. They can abide by local rules only as required, or they can help lead the change under way. Grudging and minimal compliance may keep a firm out of trouble but will do little to gain consumers' trust—and may even undermine it. Voluntarily identifying and adopting the most stringent data privacy policies will inoculate a firm against legal challenges and send consumers an important message that helps confer competitive advantage. After all, in an information economy, access to data is critical, and consumer trust is the key that will unlock it. ▼

HBR Reprint R1505H

"The new computer is great, but we can't get rid of the old one. It knows too much."

PAUL KALES