Promise and Permission:
The Role of Trust in the New Data Economy

By Tim Walters, PhD

THE CONTENT ADVISORY

Promise and Permission:
The Role of Trust in the New Data Economy

By Tim Walters, PhD

The combination of consumer resistance and regulatory constraints mark a fundamental turning point in how companies process data, create experiences, and build long-term relationships. In the emerging *new data economy*, marketers and other customer experience teams will be on the front lines of a competitive battle for the rich personal data required to fuel and sustain the relevant experiences consumers demand. As consumers assert more control over their data, they will tend to share it with companies that are both reliable data stewards and attractive partners in a mutual exchange of value. In short, the perceived trustworthiness of a company will be the decisive factor that determines whether consumers provide access to personal data. Marketers need to understand and master the dynamics of trust in personal data exchanges.

Welcome to the New Data Economy

The distinctive advantages of current big data practices are commonly designated as the "3 Vs" – namely, software and network innovations that allow large *volumes* and wide *varieties* of data to be processed at high *velocity*. Underlying these technical capabilities, however, is the presupposition that an organization can access and aggregate massive amounts of data, process it as they desire, and treat it as their own property – a corporate asset from which maximum business value can and should be extracted. Over the past decade, business models, software architectures, and marketing best practices have all been informed if not dictated by Tim O'Reilly's dictum, "The guy with the most data wins."[1]

> "The perceived trustworthiness of a company will be the decisive factor that determines whether consumers provide access to personal data. Marketers need to understand and master the dynamics of trust in personal data exchanges."

However, the era of abundant, freely available, and easily accessible data is coming to an end. (At least with regard to personal data, which is arguably the most valuable of all.) Regulatory restrictions on data collection and processing, combined with growing consumer resistance to invasive data practices, will make personal data far more scarce and cause a shift from big data to "beg data," as consumers' permission is required to process personal information. (See Figure 1.) In this new data economy, organizations will have to navigate fundamentally new requirements for both accessing and using personal data.

Figure 1

The New Data Economy

	FROM	TO
AVAILABILITY	**SUPER ABUNDANCE** Personal data is "digital exhaust" that can be vacuumed up at will and used without restriction.	**SCARCITY** Personal data is like the car that produces the exhaust – and you're only borrowing it.
CULTURE	**DATA PREDATORS** "The guy with the most data wins." (Tim O'Reilly)	**DATA SHEPHERDS** Data must be managed "sensitively and ethically." (ICO Commissioner Elizabeth Denham)
STRATEGY	**BIG DATA** Personal data is a corporate asset, from which business value is extracted.	**BEG DATA** Personal data is accessed via attractive value propositions that win consumers' permission.

A New Era of Data Scarcity

Multiple forces work in concert to create the new era of personal data scarcity:

- **Regulations restrict availability of data:** The General Data Protection Regulation (GDPR) significantly restricts how companies ("data controllers") can collect, use, and store (all of which are considered aspects of "processing") the personal data of anyone in the European Union (EU). Under the GDPR, affected companies may no longer vacuum up and store data simply because it might be of value in the future. Rather, they must state a specific processing purpose, use the acquired data only for that purpose, and delete it as soon as the purpose is accomplished. Moreover, the GDPR places new constraints on the use of third-party data, such as a purchased list. (For a detailed FAQ on the GDPR, see our previous whitepaper, "The Burdens and the Benefits of the GDPR: A Practical Guide for Marketers.[2]) Nor is the GDPR the only recent legislative intervention: similar rules are in place, proposed, or pending in Japan, Indonesia, and many other countries.[3]

- **Consumers acquire new rights:** Regulations such as the GDPR typically grant consumers ("data subjects") more control over how their data is used. For example, the GDPR requires companies to obtain consumers' permission to process personal data. (See the discussion of "permission generation" below). In addition, the GDPR expands so-called data subject rights beyond existing EU legislation, making it easier for consumers to object to processing, withdraw their data (the "right to be forgotten"), and to shift their data to another controller (the "right to data portability").[4]

- **Growing consumer resistance to data practices:** Worldwide, consumers' dissatisfaction with and opposition to intrusive, surveillance-based marketing practices has been increasing for years. Currently, some 1.7 billion ad- and tracking blockers are in use globally. Over 90% of US adults feel they have "lost control of their data." (See Figure 2.)[5]

Figure 2

Consumer Revolt Against Data Surveillance

~1.7 Billion ad tracking block users worldwide

91% Of US adults "agree" or "strongly agree" that consumers have lost control over their data

68% Of US and UK consumers don't trust how their data is being used

80% In a global survey gave "If they used my data without me knowing" as the number one reason they abandon a provider

- **Data misdeeds fuel consumer anxiety – and further regulation:** The seemingly unstoppable parade of high profile data breaches (Equifax, Yahoo, and Uber in 2017, for example) can only make consumers more reluctant to part with personal data. Moreover, consumer awareness of the systematic misuse of data has been growing steadily since the Snowden revelations in 2013. More recently, the Facebook – Cambridge Analytica scandal dominated headlines just as public awareness about the GDPR was peaking in the spring of 2018 – and was followed by calls for additional data protection regulations in the US and elsewhere.[7]

Together, these forces add up to a significant reduction in the amount of personal data that companies can access and process. As it becomes more scarce, personal data will grow in value – and create a new competitive battlefield.

The Looming Battle for Personal Data

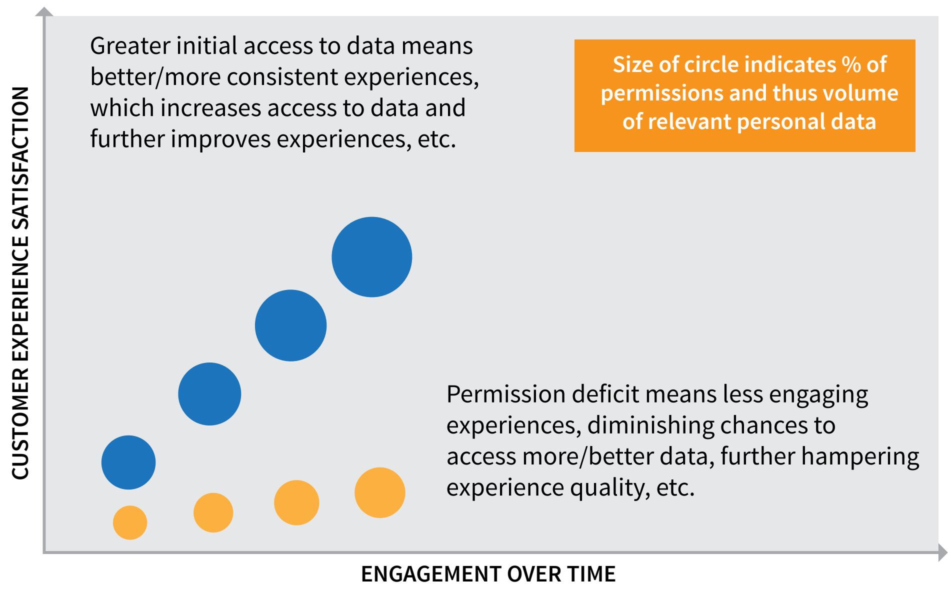
Whether in response to regulatory obligations or (far better!) out of a desire to relieve consumer anxiety about data risks, the new data economy makes it advisable if not necessary to transparently inform consumers about processing purposes and to obtain their approval.

(For marketers and CX teams operating under the GDPR, this will normally take the form of the consumer's *active permission* when granting consent, or their *passive permission* when they do not exercise the right to object to processing under legitimate interest.[8])

As it is quite evident that consumers will not respond favorably to *every* request for their data, marketing's primary task must shift from demand generation to *permission generation* – i.e., devising experiences and value propositions that increase the positive responses to requests for permission to process data.[9] The resulting customer interactions could produce a dynamic that divides business competitors into a few "haves" and many "have nots." (See Figure 3.)

Figure 3

Permission Generation Creates a Have/Have Not Dynamic



Those organizations that receive a relatively larger number of positive responses to the initial request for data will be able to produce smarter, more relevant experiences – leading to greater customer satisfaction and engagement, thus increasing their changes of accessing additional data to fuel even better experiences, and so on. In contrast, those that lag behind at the outset will struggle to create attractive experiences – subsequently diminishing their access to data and further hampering their competitive position, etc.

The potential for these data-experience positive feedback loops – building on one level of data access to improve experiences and amplify the chances of further access – illustrates what we intuitively understand: *Consumers are more willing to share data with companies that they trust.* Trust is the strategic high ground in the coming battle for personal data.

Coming to Terms With Trust in Personal Data Exchanges

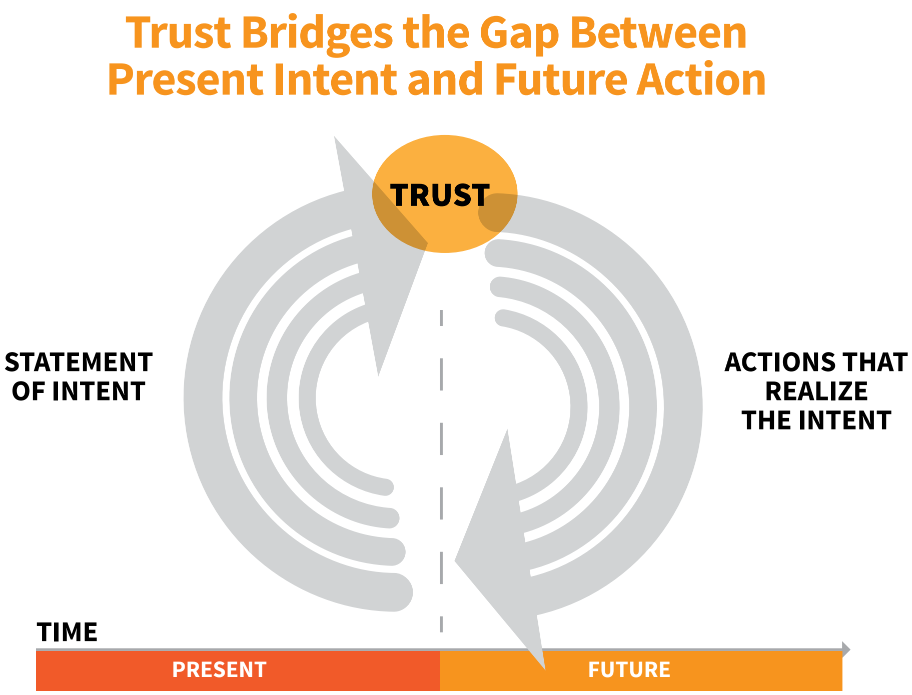
Trust is undeniably the basis of successful customer relationships. Edelman's 2015 Trust Barometer study found that 63% of people who lack trust in an organization will refuse to buy products and services from it and 37% have shared negative comments online.[10] Yet despite the recent corporate embrace of trust – in one survey of business leaders, 83% agreed that "trust is the cornerstone of the digital economy" – there has been very little analysis of the meaning and role of trust in realm of data collection and processing.[11]

Analyses of trust often center on two elements that are thought to be indispensable for a trust relationship to occur: the first is uncertainty and the second is vulnerability.[12]

> Consumers are more willing to share data with companies that they trust. Trust is the strategic high ground in the coming battle for personal data.

- **Uncertainty** means that I choose to trust you (or alternatively not to) only in situations in which I cannot be certain how you are going to act. (See Figure 4.) Trust is always pertinent only with regard to a future that is unpredictable. (Although it is often – perhaps necessarily – rooted in the past, trust is essentially oriented toward an uncertain future.) If your behavior is entirely predictable and preprogramed, trust is irrelevant.

Figure 4



- **Vulnerability** plays on multiple registers in a trust relationship. First, it designates that trust is a factor in situations that involve risk and exposure. A broken promise is disappointing; misplaced trust can leave you (feeling) betrayed, if not actually harmed. On the other hand, vulnerability also highlights how the fortunes of the two parties (the trustor and the trustee) can be intertwined for mutual reliance and mutual benefit.

Consider, then, how these elements apply to the relationship between a consumer and an organization that wants to process his or her personal data. The company can reduce uncertainty by clearly explaining how the data will be used, shared, and secured. Still, *uncertainty* cannot be eliminated entirely; the consumer has to trust the organization *now* to do *in the future* (only) what it says it will do.

Moreover, allowing access to personal data makes one extremely vulnerable. Abuse of the consumer's trust could expose them to financial harm, reputational damage, or even the theft of their very identity. At the same time, the company takes on all of the regulatory and reputational risks associated with handling personal data. (Of course, it is difficult to compare personal and corporate risks. Still, it is known that data misuse can have a significant financial impact on an organization.[13]) On a more positive note, building and maintaining trust can lead to a long-term relationship that benefits both parties.

> Vulnerability is a necessary aspect of any trust situation. A broken promise is disappointing; misplaced trust can leave you feeling betrayed, if not actually harmed."

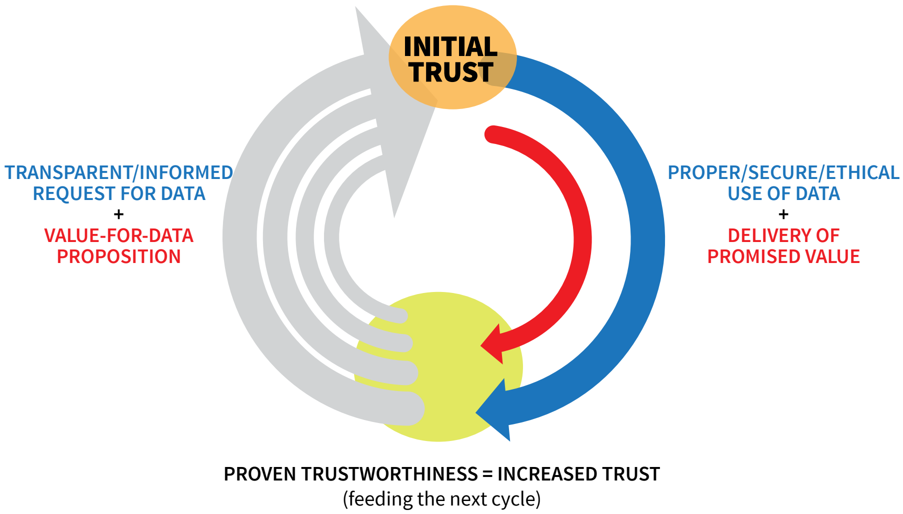
Beyond Security, the Attractive Value Proposition

Data security is a primary source of anxiety and suspicion for consumers. According to a recent Harris poll, 78% of US respondents say that a company's ability to keep their data private is "extremely important," while nearly as many (73%) think businesses focus on profit over consumers' security needs.[14] To compete successfully for personal data, organizations must aggressively and transparently address these concerns. (The GDPR envisions a variety of certifications and seals to indicate a company's verified commitment to data security and other aspects of compliance.[15])

But the new data economy adds another layer to this dynamic. As consumers assert control and ignite a competition for their personal data, they will consider not only whether firms will use it properly and securely. The additional factor will be what value they receive in exchange for parting with their data. These *value-for-data propositions* will used by consumers to differentiate and evaluate the numerous requests for personal information. The perceived trustworthiness of the requester – i.e., the consumer's calculation of the firm's ability to keep their promise and *deliver the stated value in the future* – then becomes the decisive element that determines which firms gain access to more personal data earlier in the engagement lifecycle and begin to leverage the data-experience positive feedback loops. (See Figure 5.)

Figure 5

Trust Fuels Positive Feedback Loops



A Virtuous Cycle of Increasing Trust

This secure and mutually beneficial data exchange raises two issues. First, the obvious question is, where does the (initial) trust come from to ignite the first cycle? In a commercial relationship, trust is normally located near the end of the long "customer lifecycle" that runs from initial consideration to research, purchase, and use. Trustworthiness is typically earned only after the consumer has used the product or service happily and reliably. But in order to access personal data and build desirable experiences, marketers need to "move trust upstream" – i.e., to devise ways to motivate consumers to enter a trust based relationship at or near the beginning of the engagement lifecycle. In the new data economy, this could be accomplished in several ways, such as:

- **Leverage the company's brand and reputation:** Would you be more receptive to a data request from Apple or Comcast? Subaru or Spirit Airlines?

- **Deploy content marketing:** By definition, a well-functioning content marketing program provides valuable, brand-agnostic information prior to the beginning of any sales cycle. (Petfinder's pet adoption service (now owned by Nestle Purina) and General Mill's tablespoon.com recipe site exemplify this approach.[16]) By building an engaged, appreciative audience in this way, an organization can create reserves of "trust credits" that can be deployed in data requests.[17]

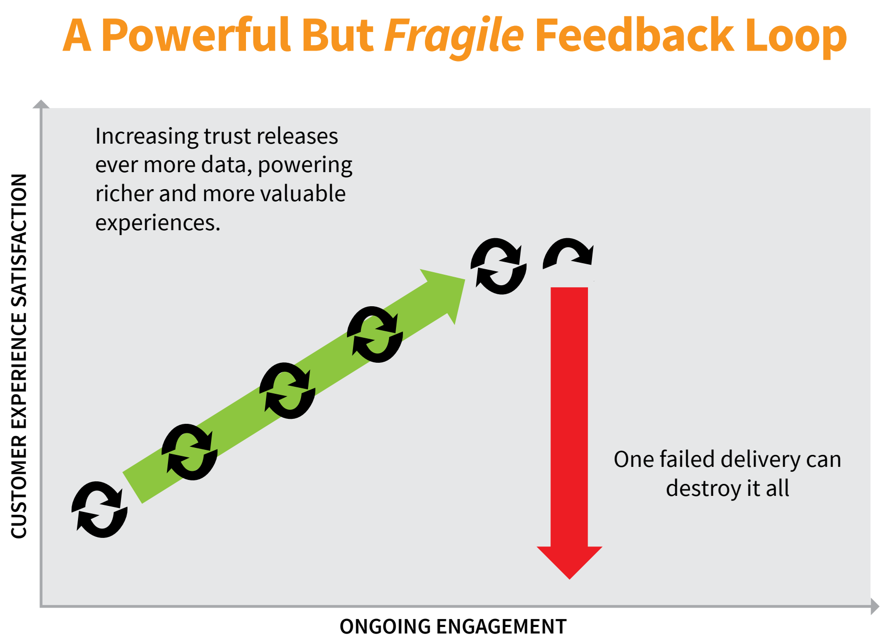
- **Start with small stakes:** Reduce the consumer's anxiety and vulnerability by first asking for relatively innocuous personal data. For example, in exchange for my email address, you'll send me a newsletter with that valuable, brand-agnostic content marketing content. I know that it's easy enough to unsubscribe, plus I can easily validate whether the content is valuable and decide whether to engage more deeply (and provide additional personal data).

Second, note that the delivery of the promised value in Figure 5 “weighs” more than proper and secure use of the data. This is because, thanks to regulations such as the GDPR, compliant and ethical data processing will (eventually) be table stakes. More importantly, whereas secure data use reduces exposure and vulnerability for the consumer, the value-for-data proposition speaks to the positive benefit(s) they receive from choosing to enter a relationship with a particular provider – thus accentuating the value of their data and their sense of control over how it is deployed.

Conclusion: Putting Trust to Work In the New Data Economy

Clearly, the virtuous cycles can work only as long as the organization continues to reward trust by *consistently* delivering on the propositions they make on data usage and consumer value. A single failure could evaporate all accumulated trust and end the relationship permanently.

Figure 6



> In order to access personal data and build desirable experiences, marketers need to ‘move trust upstream’ – i.e., devise ways to motivate consumers to enter a trust-based relationship at or near the beginning of the engagement lifecycle.

Marketers have often been called "the promise makers" – with sales, support, product management, and the rest of the organization serving as the promise keepers.[18] Until now, a gap between these two elements was suboptimal but not uncommon. The indignities of air travel are never depicted in the ads, and no Big Mac has ever looked as good coming out of the clamshell as it does on television. But with consumers parceling out scarce personal data on the basis of data-for-value propositions, any gap between the marketing promise and the delivered value must be identified and eliminated. Silos, fragmentation, and non-integrated processes – which demonstrably have hampered real improvements in customer experiences for years – are transformed into existential threats on the battlefield of data access in the new data economy. In particular, firms must:

- **Understand and control the personal data they process:** This isn't just a compliance requirement of the GDPR and other regulations. It's about not only knowing what data you have where, but precisely how you use it, and – crucially – what benefit(s) it produces (or could produce) for both the organization *and* the consumer.

- **Carefully match data requests and benefits:** The companion mistake to overpromising the benefits you can deliver the consumer is to *over reach* when requesting data – asking for more than you need risks provoking suspicion and mistrust. (And it's a violation of the GDPR as well.)

- **Coordinate data and business processes to nurture trust:** Early stage data-for-value propositions (such as valuable newsletter content in exchange for an email) should be fairly easy to identify and fulfill. But as the relationship progresses and the requested personal data becomes richer and more extensive, the value exchange will necessarily grow more complex and precarious. To reliably deliver the promised benefits and preserve the firm's trustworthiness, marketers and customer experience teams will need to orchestrate numerous data flows and business processes.

In the new data economy, personal data becomes a scarce, and therefore extremely valuable, resource. Organizations that can instill trust – and nurture it by consistently delivering reciprocal value in exchange – will have access to more and better data, fueling superior customer experiences and business success.

> In order to access personal data and build desirable experiences, marketers need to 'move trust upstream' – i.e., devise ways to motivate consumers to enter a trust-based relationship at or near the beginning of the engagement lifecycle.

Notes

1. O'Reilly was specifically discussing location data, but the insight is obviously generalizable. See the 2012 interview, available at https://www.socialmediatoday.com/content/video-timoreilly-guy-most-data-wins.

2. This whitepaper is available from The Content Advisory at www.contentadvisory.net/research/.

3. See for example, "Brazil Moving Forward With GDPR-Inspired Data Protection Bill," at https://iapp.org/news/a/brazil-moving-forward-with-gdpr-inspired-data-protection-bill/ and "The Data Protection Landscape In APAC," at https://www.fortinet.com/blog/industrytrends/the-data-protection-landscape-in-apac-.html.

4. For a more detailed discussion of data subject rights under the GDPR, see the whitepaper cited in note 2. See also the Financial Times article, "Companies Under Strain From GDPR Requests," available at https://www.ft.com/content/31d9286a-7bac-11e8-8e67-1e1a0846c475.

5. Sources for Figure 2, in order of appearance: Already in 2016 – before public awareness of the GDPR and mass anxiety about the Facebook-Cambridge Analytical scandal – the Global Web Index determined that on average, 37% of mobile users deploy ad blockers. Today, with some 4.6 billion mobile phone users worldwide, that means that over 1.7 billion people are currently blocking ads and tracking – a number greater than the population of the Western Hemisphere. For the GWI study on blocker usage, see "37% of mobile users are blocking ads," available at https://blog.globalwebindex.com/chart-of-the-day/37-of-mobile-users-areblocking-ads; Pew Internet report, available at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/#shared; Gigya privacy survey, available at info.gigya.com/rs/672-YBF-078/images/201704-Gigya-DSPrivacy_ Survey_Report-web.pdf; SAP/Hybris consumer survey report, available at https://www.hybris.com/en/gmc55-the-global-2017-sap-hybris-consumer-insights-report.

6. Edward Snowden's revelations of mass surveillance by the U.S. and other governments – as well as the complicity of many telecommunications, technology, and internet firms – came to light in the summer of 2013. At the end of 2013, a survey by mobile provider Orange found that consumer trust in a range of vertical sectors suffered a substantial net decline compared to late 2012. See http://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf.

7. For example, see the discussion of California's Consumer Privacy Act 2018 at https://www.cpomagazine.com/2018/07/13/tech-companies-ready-to-battle-new-californiadata-privacy-law/.

8. For a more detailed discussion of consent and legitimate interest under the GDPR, see the whitepaper cited in note 2.

9. In the spring of 2018, PageFair placed a simple mockup consent request in an article and asked readers if they would consent to data processing; nearly 80% said they would refuse to provide personal data. "Research Result: What Percentage Will Consent to Tracking For Advertising?" at https://pagefair.com/blog/2017/new-research-how-many-consent-totracking/. Moreover, research shows that consumers are generally "consent poor." In a 2015 survey, 70% of over-55s, 51% of those aged 35-54 and 27% of consumers aged 18-34 said they give consent less than 20% of the time. See "Why Age Matters When Marketing Consent," available at https://www.consumerintelligence.com/articles/why-age-matters-whenmarketing- consent.

10. A summary of Edelman's 2015 Trust Barometer report is available at https://www.scribd.com/doc/252750985/2015-Edelman-Trust-Barometer-Executive-Summary.

11. The metric is from Accenture's 2016 Technology Vision Survey of 3,100 business and IT leaders. See https://www.accenture.com/nz-en/insight-technology-trends-2016. For an additional perspective on the role of trust in business affairs, see the World Economic Forum's report "Rethinking Personal Data: A New Lens For Strengthening Trust," available at http://reports.weforum.org/rethinking-personal-data/;

12. See "Differentiating Trust and Trustworthiness: A Sociologist's Perspective," available at http://www.kellogg.northwestern.edu/trust-project/videos/carruthers-ep-1.aspx.

13. See "The Financial Impact of Data Breaches Is Just the Beginning," available at https://www.information-age.com/data-breaches-financial-impact-123470254/.

14. In late March 2018, The Harris Poll conducted a survey of 10,000 consumers in the US and six other countries. See https://www.prnewswire.com/news-releases/new-survey-finds-deepconsumer- anxiety-over-data-privacy-and-security-300630067.html.

15. See the whitepaper, "Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms," available at https://iapp.org/media/pdf/resource_center/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

16. See www.tablespoon.com and www.petfinder.com.

17. See for example, "GDPR: The Biggest Gift to Content Marketers in a Decade," available at https://contentmarketinginstitute.com/2018/06/gdpr-content-marketers/.

18. For an engaging discussion of marketers as promise makers, see Robert Rose and Carla Johnson, "Experiences: The 7th Era of Marketing" (2015). Information and sample chapters are available at http://7theraofmarketing.com/.

The Content Advisory Inc.

We teach companies how to build audiences and see the future of strategic content through trend forecasting, research, education, and brand consulting.

A trusted audience is the most valuable asset any company will manage. For years, brands have had to rely on third-party media and measurement to reach the audiences who can drive strategic business value. We know that marketers now have the disruptive power to create or acquire owned-media experiences and build these valuable audiences for themselves. The Content Advisory is committed to accelerating this shift and fundamentally transforming the practice of marketing.

For more information please visit www.contentadvisory.net.

THE CONTENT ADVISORY