A Forrester Consulting Thought Leadership Paper Commissioned By Neustar

Differentiate With Privacy-Led Marketing Practices

As People Get Wiser, Respectful Collection And Use Of Customer Data Become Crucial

July 2013

FORRESTER®

Headquarters | Forrester Research, Inc.
60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | www.forrester.com

Table Of Contents

About Forrester Consulting
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.

Executive Summary

As scrutiny over personal data collection and sharing practices increases from both the media and government, marketers need to change their approach to audience targeting and find alternatives to "consumer data giants," in order to build and maintain trust with their customers.

In March 2013, Neustar commissioned Forrester Research to evaluate consumer attitudes and understanding of privacy and the marketing ecosystem's various uses of personal data. The study sought to determine whether marketers who take a permission-based, "privacy by design"-approach to the use of third-party data will build more loyalty and deeper engagement with their customers.[1]

In conducting a rigorous online study of more than 1,000 US adults, Forrester found that consumers perceive brands that take a respectful, protected approach to collecting and using customer data as being trustworthy.

Key Findings

Forrester's study yielded four key findings:

- Consumers are increasingly concerned about their personal data and are taking steps to protect it.
- Individuals are most frustrated by marketers "profiteering" from their personal data.
- Consumers are more loyal to, and willing to share data with, brands they trust.
- Marketers should take a privacy-led approach to customer data collection and use.

Consumer Data-Driven Models Carry Risks

Marketers in every industry depend on third-party data to help them paint a clearer picture of their customers' needs and lifestyles. Combine that demand with the volume of data that's actually available about people, and it's not a surprise that in the past decade, the third-party data vendor landscape has exploded. The two types of third-party data vendors that are best known today include:

- **Consumer data giants.** These firms function as a "central bank" of sorts for consumer data and build rich dossiers that include everything from demographic to behavioral data about specific individuals. In addition to selling individual attributes that marketers can append to their own customer database, they also sell data such as propensity-to-buy scores and highly descriptive lifestyle segments based on that data. They typically don't require clients to share data about their customers in order to purchase these third-party attributes.
- **Data cooperatives.** These organizations function as cooperative exchanges: Marketers must share data about their customers before gaining access to the insights from the cooperative. Typically, these providers help marketers find "lookalike" prospects — those whose buying behavior resembles that of their most valuable customers. While these firms don't typically provide data appends to the marketer's own database, they do provide lists (with name, address, email, and other PII) to their clients' list processing vendors.

The Traditional Models Face Serious Challenges

Although the data cooperative and data giant models have led to great success for many marketers, they now face some serious challenges. Their clients are increasingly sensitive to the problems the legacy third-party data model faces, which include:

- **Failure to move at market speed.** Marketers are trying desperately to keep up with the pace of changing customer behavior and expectations. That means extremely accurate, real-time recognition in every touchpoint (for example, at the call center or within social channels) and the ability to deliver insights and recommendations at the same rate. Many traditional data providers simply haven't been able to move from their legacy processes to deliver on these demands.
- **Regulatory and legislative scrutiny.** Within the US, both the Federal Trade Commission (FTC) and Congress have opened inquiries into the data brokerage industry. The FTC has authority to take action to prevent deceptive and unfair commercial practices, and both the FTC and Congress are considering whether there is a need for legislation. Meanwhile, states like California have moved ahead with their own proposed laws to protect consumer data rights.[2] Whether or not a federal privacy or personal data usage law is enacted, marketers are starting to think twice about their approach to collecting, buying, and storing customer data in perpetuity.
- **Negative publicity.** Every week, mainstream media outlets are publishing high-profile stories about data brokers and the use of personal information within the advertising industry.[3] Meanwhile, the Internet browser wars are heating up again as these services try to differentiate themselves as more respectful, or more protective, or more "intelligent" tools for consumers. Ultimately, this means that individuals are significantly more aware of the privacy implications of online tracking and profiling, and they're taking steps to learn more and protect themselves.

Alternative Models Exist

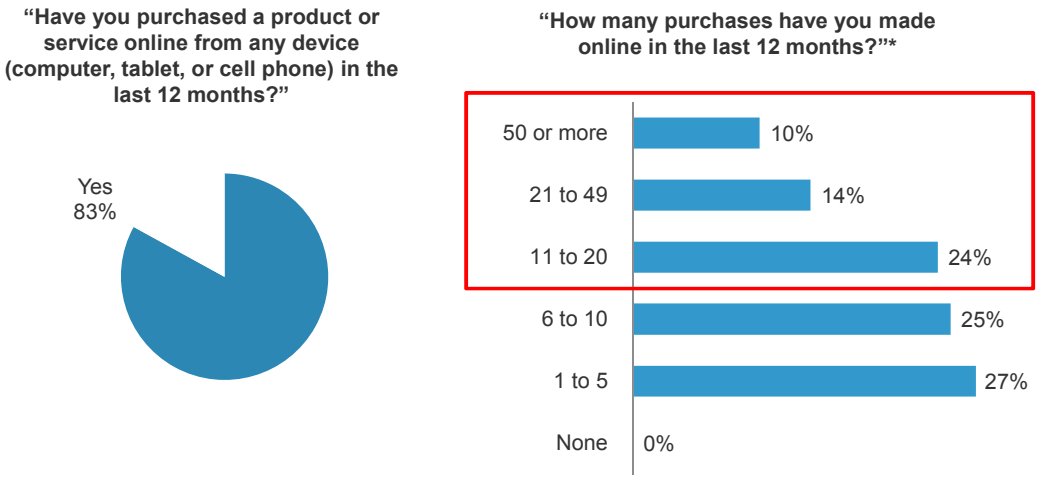
Some third-party data providers emphasize privacy and thereby reduce the risks to marketers:

- **Audience targeting providers.** These vendors take a different approach to third-party data by identifying audience attributes and enabling marketers to target customers without handing off PII.

Privacy And Personal Data Concerns Are Ubiquitous

As the media and regulators shine an ever-brighter light on behavioral advertising data, consumers are becoming increasingly concerned with how their data is being used by the companies they do business with. And these concerns are not limited to novice online shoppers and older consumers. In fact, the vast majority of respondents (83%) have made at least one purchase online in the past 12 months, and 48% purchase *monthly or more*. And, the customers we surveyed aren't new to eCommerce, either: Nearly a third has been shopping online for over a decade (see Figure 1).

Figure 1
Majority Of Online Adults Have Made Purchases Online



Base: 1,053 US online adults
*Base: 877 US online adults who have purchased online in the last 12 months

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

With their growing concerns, these consumers are taking steps to educate and protect themselves in ways we've never seen before. We found that:

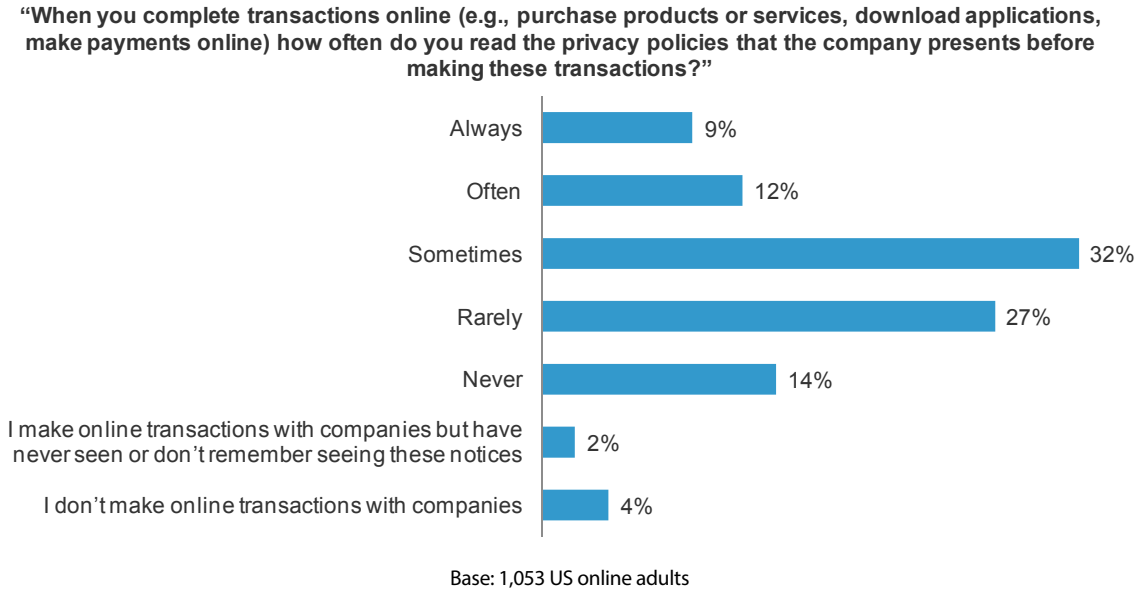
- **A majority reads privacy policies — and then acts on them.** Our research shows that more than half of consumers "sometimes to always" read privacy policies before completing an online transaction (see Figure 2). While this figure is significant in and of itself, things get even more interesting when we asked whether those individuals who read policies have ever changed their behavior — specifically, whether they had opted out of a transaction — as a result. The verdict? More than one-third said they had (see Figure 3).

- **They're adopting tools and technology to protect their data.** For years, many consumer data giants, data cooperatives, audience targeting providers, and marketers have leveraged the gap between what consumers say about privacy concerns, and what they actually do to protect their privacy. But our research suggests that a behavioral shift is underway: Nearly a third of our respondents have embraced the use of tools such as ad blockers (27%), do not track plug-ins or browser settings (18%), and even third-party tracking tools (13%) (see Figure 4).

- **They're more cautious about interacting with online advertising.** Widely-used interactive marketing tactics are becoming an increasing source of concern for consumers. For example, nearly 60% of our survey participants reported that they have actually avoided clicking on an ad for a product that they were otherwise interested in because they were concerned about being tracked. Even that old standby, email marketing, isn't immune: More than half of respondents are "concerned" or "very concerned" about the data that will be captured or how they will be tracked if they open promotional emails.

Figure 2

Majority Of Online Adults Have Made Purchases Online

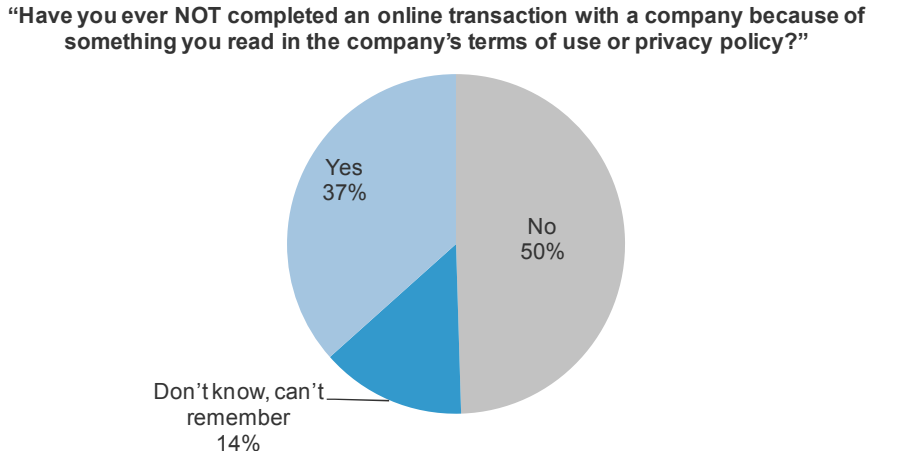


Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 3

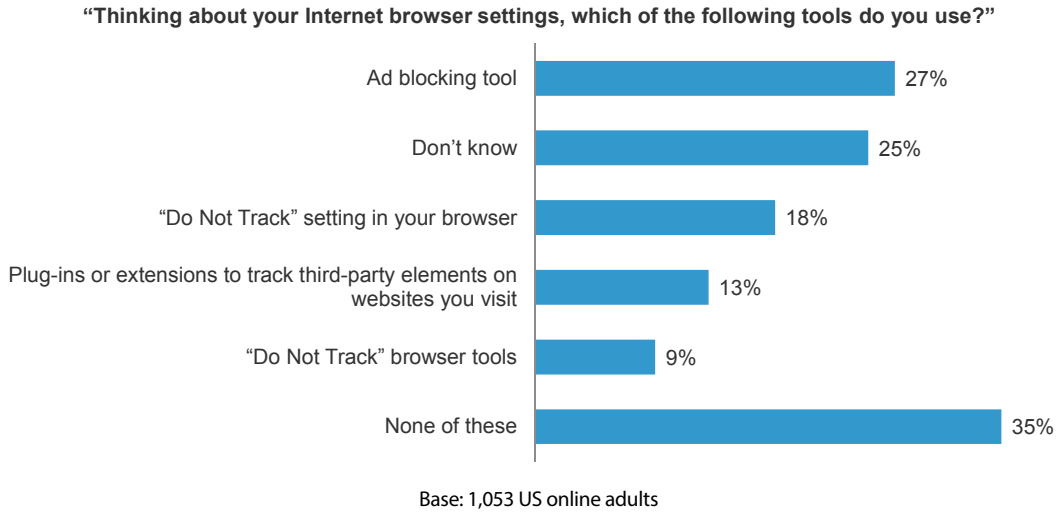
Consumers Are Protecting Their Data



Base: 843 US online adults who have read privacy policies when purchasing online

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 4
Consumers Are Protecting Their Data



Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

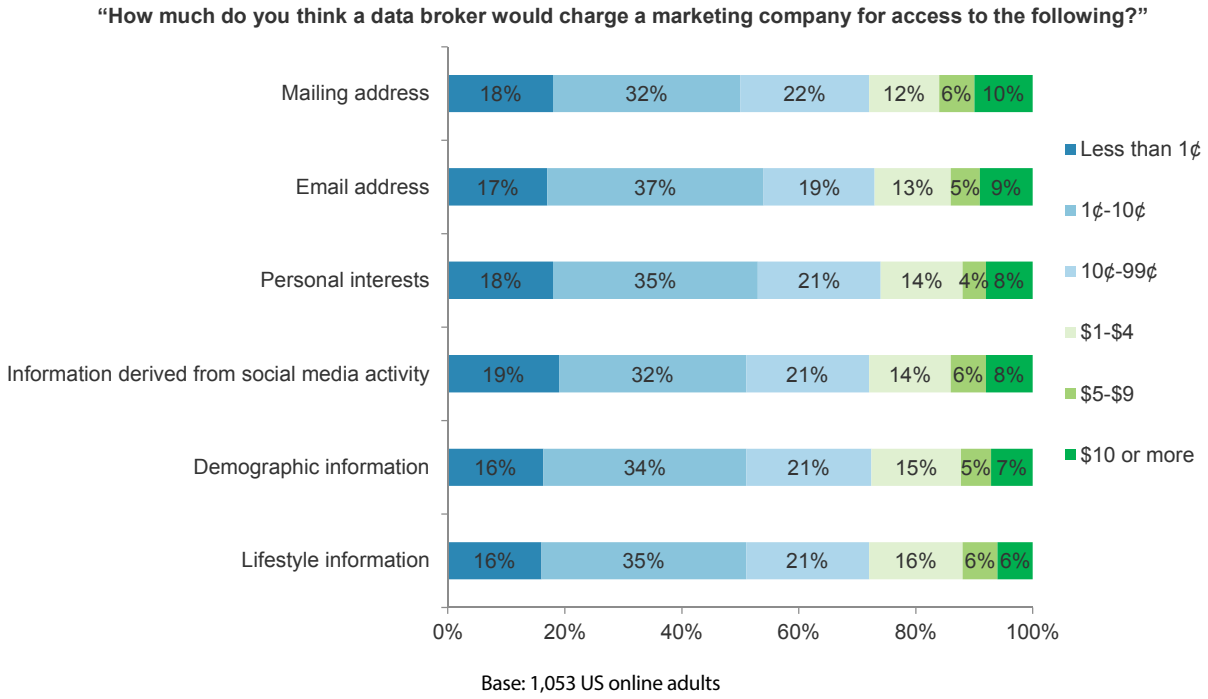
Perceptions About Personal Data Reflect Increased Sophistication

As consumers become "perpetually connected," they're starting to understand that there's an implicit tradeoff in many of their interactions with brands and services: data in exchange for value. As this mind shift occurs, so does the consumers' awareness of different data types, risks, and what they perceive as "appropriate use." We found that:

- **Consumers differentiate between data types and their perceived value.** We asked respondents how much they thought a piece of data about them might be sold for. Across the board, most believe that a piece of data (any data) is sold for less than a dime. But, there are some interesting nuances that don't necessarily align with reality. For example, consumers "valued" mailing address most highly, while demographic and psychographic information (such as lifestyle and personal interests) are perceived as being least expensive (See Figure 5).
- **Respondents' perceived value of a piece of data is tied to its *sensitivity*, not to its ubiquity.** For example, an overwhelming majority of individuals think that their PII (that is, data which identifies them and makes them "contactable") is readily available to marketers for purchase; this is also the data they this is more expensive. On the other hand, far fewer believe that data like political affiliation, marital status, and ethnicity (which is actually more difficult to acquire, and is more expensive in the data marketplaces), is generally available (see Figure 6).

Figure 5

Consumers' Perception Of Data Costs Skew Higher For PII

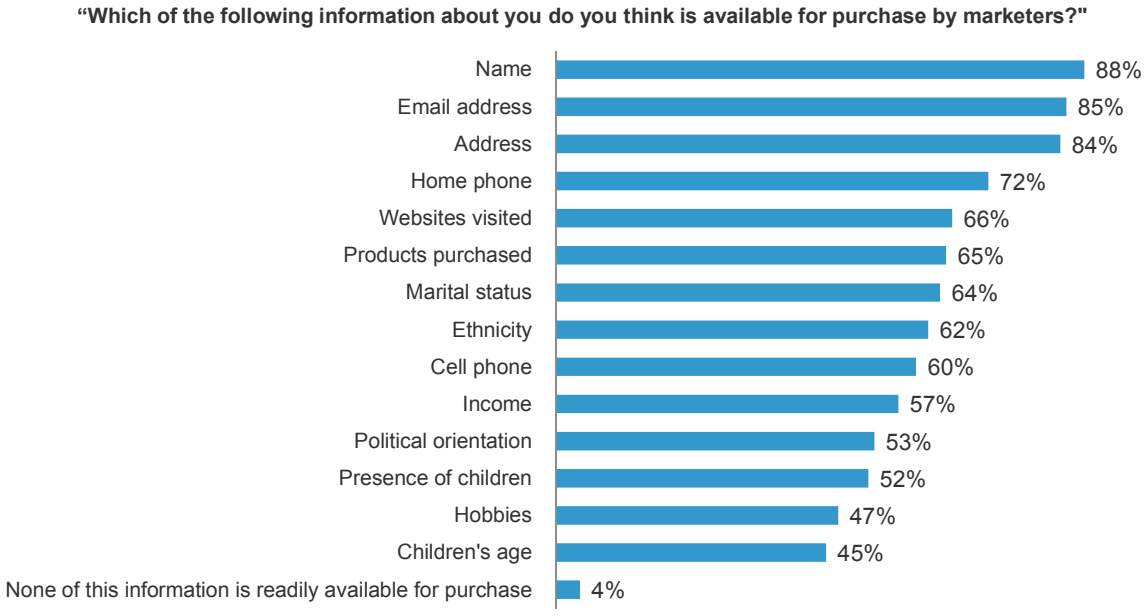


Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 6

Respondents' Perceived Value Of Data



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

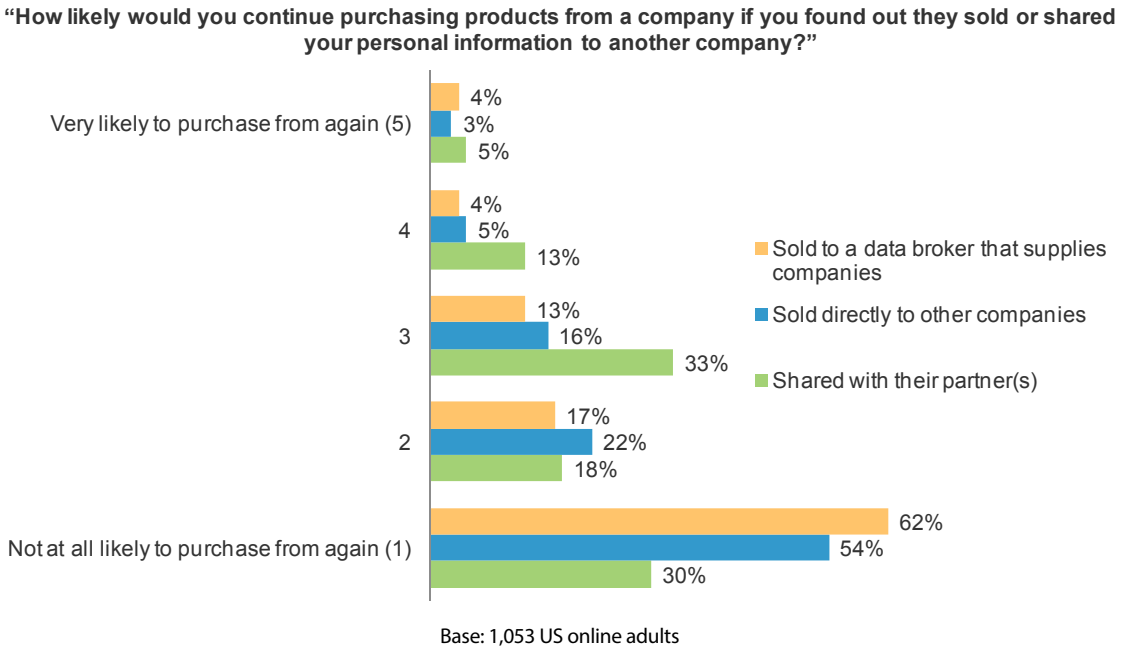
- **Over a third are concerned about data-sharing practices.** When we asked about their greatest concerns as they relate to online privacy, first place went to identity theft. But second most worrying to consumers is that their data might be permanently recorded and made accessible to others; a quarter worries that their data and behaviors might be shared with advertisers (see Figure 7).
- **However, people are far more tolerant of data-sharing between partner companies than they are of any form of data-selling.** In fact, while only 30% of respondents said they'd stop shopping with a company that *shared* data, more than twice that number (62%) would stop shopping if they knew for certain that the retailer sold the consumer's personal information to a data broker (see Figure 8).
- **Consumers have clear — but unmet — expectations for data retention.** When given a choice about the duration of data retention, 58% of respondents thought that a company should delete their personal data six months after their most recent transaction (see Figure 9). In fact, just over half reported that they have actually requested that their data be deleted from at least one customer file, primarily because they no longer shopped with that company. Unfortunately, however, over half of them don't believe that the retailer actually complied with their request (see Figure 10).

Figure 7
Top Concerns Around Personal Privacy

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 8

Consumers Are More Accepting Of Data-Sharing Between Partners

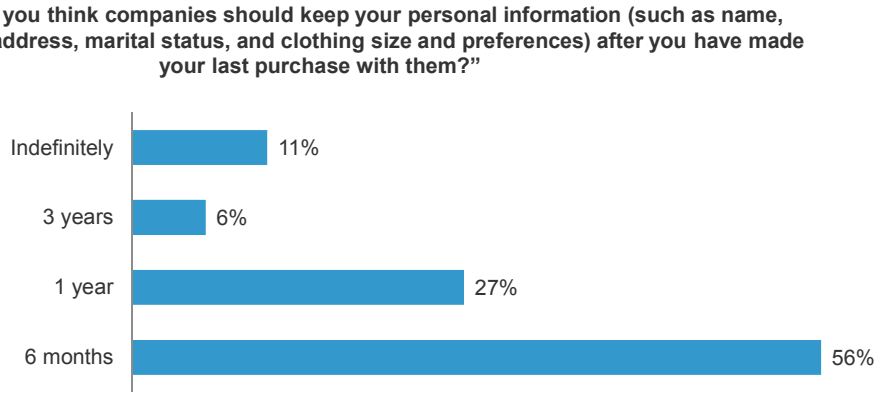


Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 9

Consumers Want Their Data Deleted After Six Months

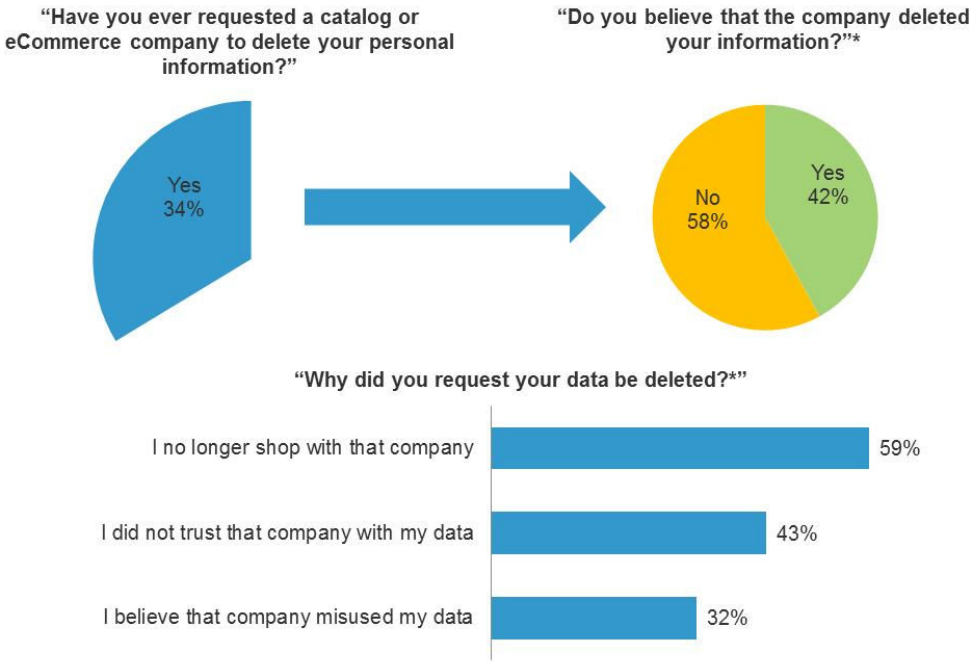


Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 10

One-Fifth Of Consumers Believe Their Data Has Been Misused Or A Company Can't Be Trusted With Their Data



Base: 1,053 US online adults

*Base: 355 US online adults who requested that a company delete their personal information

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Consumers Trust Brands That Treat Personal Data Respectfully

In our survey, we ran a fully randomized A/B split test of respondents to understand whether there was a perceived difference between methods of third-party data usage. Our first scenario was designed to test consumer reactions to the traditional consumer data giant model of third-party data acquisition. The second tested reactions to a privacy-led model of customer data handling. Each participant in the study *saw only one* of the following two scenarios:

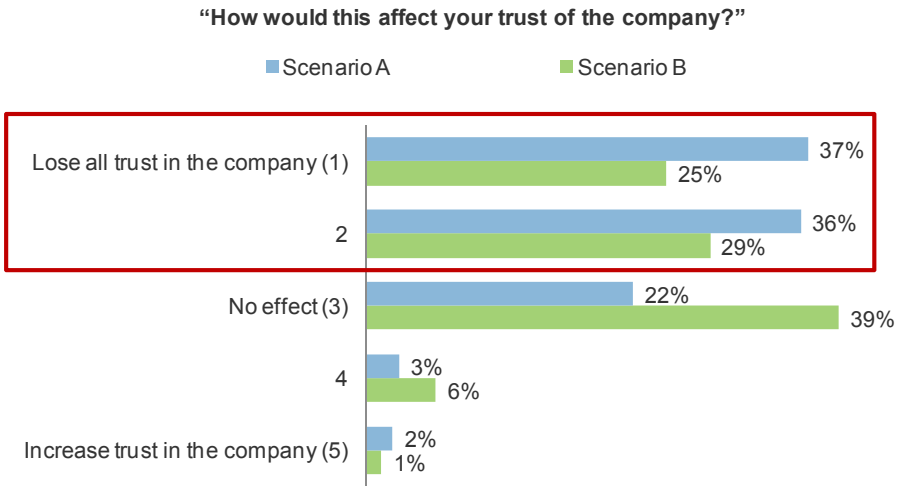
- **Scenario A:** Imagine that a company wants to send you marketing materials and tailor them to your interests and needs. It purchases data from a third party to learn about your household income, whether you have children, what kind of lifestyle you lead, and/or what political party you're affiliated with. It uses that data to decide on the kinds of offers to send you, the kinds of products you might like, etc. The company may store this data for use for multiple uses.

- **Scenario B:** Imagine that a company wants to send you marketing materials and tailor them to your interests and needs. The company acquires a list, from a third party, of people who it believes will be interested in its product based on aggregated information about the person's household. The company does not have access to identifiable information about the household or the individual.

Our findings don't bode well for third-party data acquisition models, especially as an increasing number of firms become more transparent about their practices in an attempt to differentiate with privacy. While we found that the majority of customers in both groups (about 73%) were frustrated by their lack of control about how their data was used, we also found that:

- **Traditional data-buying models erode customer trust.** In the traditional model of data acquisition, nearly three-quarters of individuals negatively perceived the trustworthiness of the company. By contrast, just over half said that they'd lose trust in the company taking the privacy-led approach.
- **A company's trustworthiness affects people's willingness to buy.** We found that those individuals exposed to Scenario A were significantly less likely to buy from that company again (41%) compared with those who saw Scenario B (27%). And when asked whether they'd be willing to recommend the company to a friend or family, a full 40% of Scenario A customers responded "not at all likely" compared with only a quarter of Scenario B customers (see Figures 11 and 12).

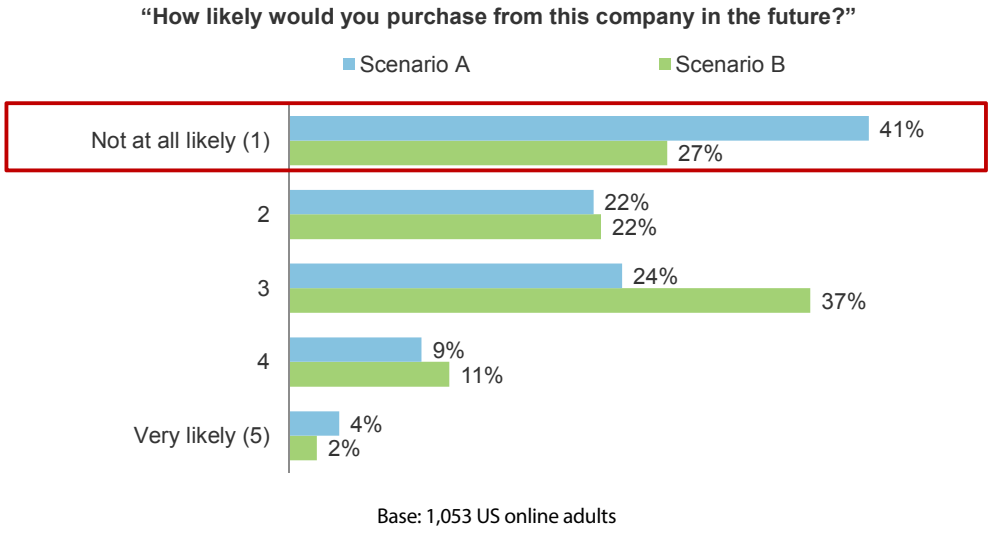
Figure 11
Customer Lose Trust In Companies That Hoard Personal Data



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure 12
Consumers Prefer To Shop With Companies That Take A Privacy-Led Approach To Data



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

What It Means: Privacy Will Be A Brand Differentiator

Most marketers still consider privacy something they have to deal with in order to get to the primary task at hand. But businesses that choose to lead with privacy will begin changing the dialogue — as they become more vocal about their approach, they will force privacy to become a market differentiator. We believe that:

- **Privacy policies will become increasingly simple and graphical.** Already, industry working groups are testing ways to visually display privacy policies. While broad-scale adoption is likely a few years away, consumers will start expecting sites to reveal their data collection, use, sharing, and retention practices in simple, at-a-glance dashboards.
- **Traditional data vendors and service providers will have to adapt.** As consumer expectations for transparency increase, traditional data brokers will increasingly experiment with permission-based exchanges where consumers and marketers can create mutually beneficial sharing agreements. Similarly, marketing services providers will need to adopt new processes for handling customer data — whether it's first party or third party.
- **Misuse and abuse of data will impact profitability.** Today, we can quantify the cost of remedying data breaches. In the future, companies will also be liable for breaching privacy, and those costs will be significant. Companies that breach privacy by collecting inappropriate data, sharing data without permission, or failing to protect and purge data as promised will: 1) incur hefty fines; 2) lose consumer trust; and 3) lose critical business partnerships as a result of their poor practices.

KEY RECOMMENDATIONS: MARKETERS SHOULD LEAD WITH PRIVACY

It seems that privacy and personal data practices are at a tipping point. Within the next half decade, the traditional models of third-party data brokerage will likely be upended, and consumers will move their business to the brands that prove their trustworthiness. Marketers that want to get ahead of the curve and begin differentiating with privacy must:

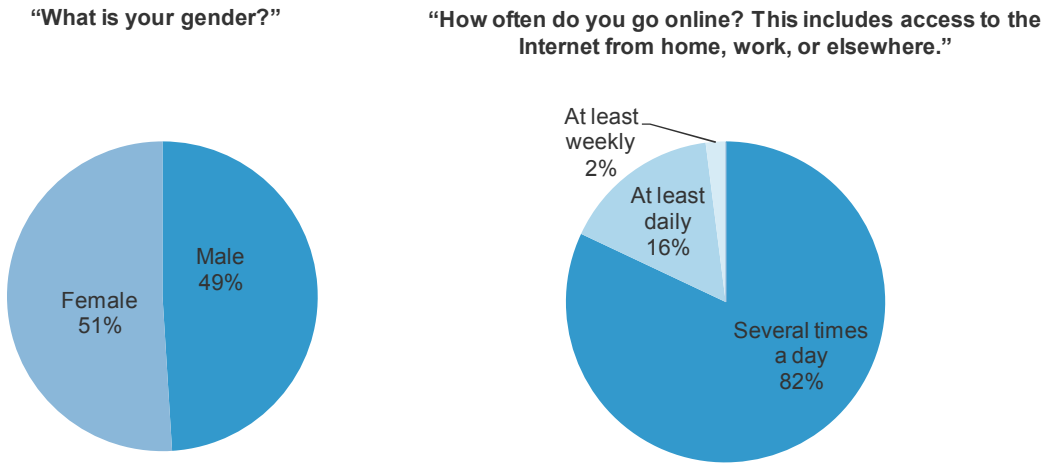
- **Embrace solutions designed with privacy in mind.** Most legacy data providers — consumer data giants, cooperatives, and audience targeters — have systems and processes that aren't designed to support privacy-led marketing. Providing individuals with simple options to control how their data is used for ad-targeting is a good example.
- **Evaluate technology and data vendors on their approach to consumer data.** Moving toward privacy-led marketing means stress-testing the privacy practices of all your customer data vendors — whether they're data management, analytics, or campaign management. For example, can access to PII data be limited? Can sensitive identity data be held in separate repositories from less sensitive transaction detail data?
- **Turn privacy from a cost center into a differentiating opportunity.** Even if fear tactics by advocates don't lead to new regulations, our research shows that people prefer to interact with businesses that treat their data with respect and don't attempt to profiteer from it. This potential upside is an important line item to highlight as you make a case for privacy-led marketing in your own organization.

Appendix A: Methodology

In March 2013, Neustar commissioned Forrester Research to evaluate consumer attitudes and understanding of privacy and the marketing ecosystem's various uses of personal data. The study sought to determine whether marketers who take a permission-based, privacy by design-modeled approach to the use of third-party data will build more loyalty and deeper engagement with their customers. The survey was fielded in March 2013. Respondents are 1,053 US-based online adults. Respondents received a small incentive for their participation.

Appendix B: Demographics

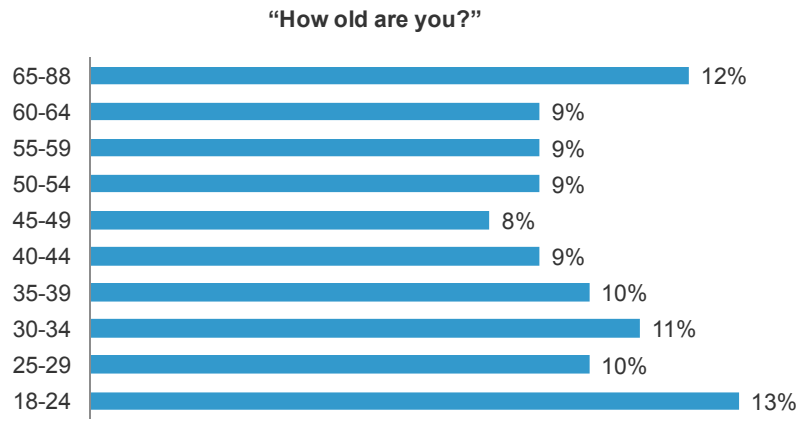
Figure A
Gender And Frequency Of Online Access



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

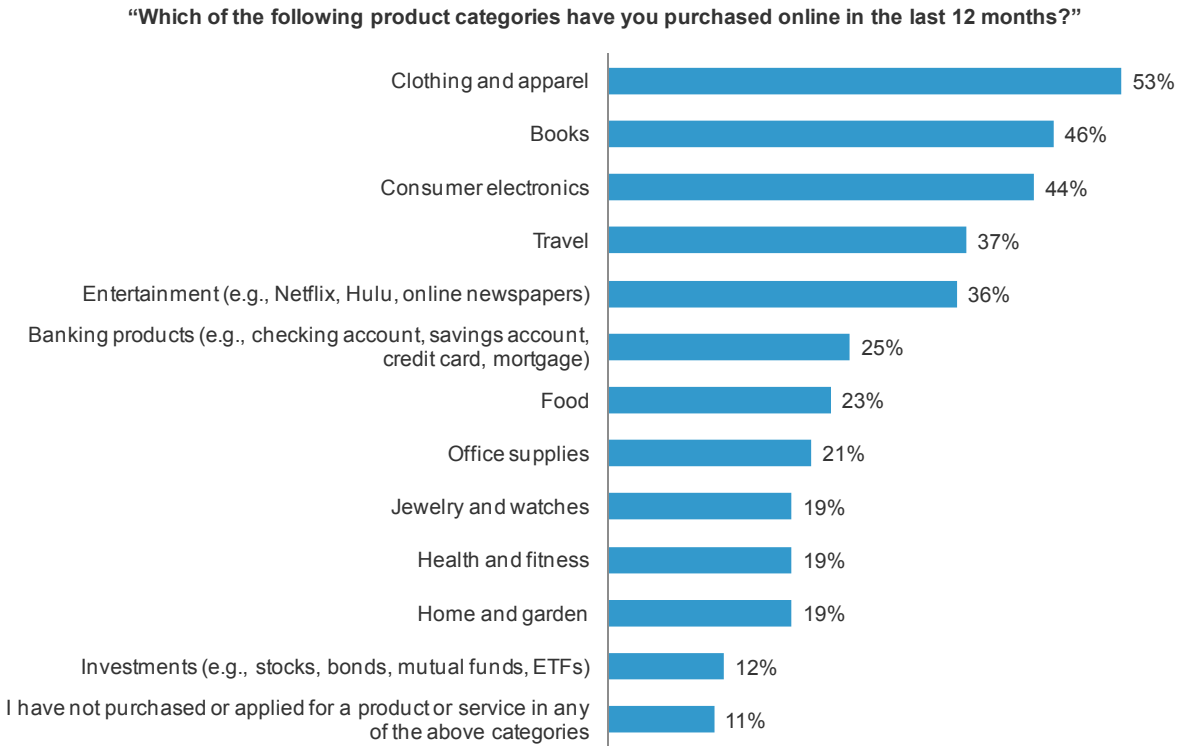
Figure B
Age Breakdown Of Respondents



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Figure C
Types Of Purchases In The Past 12 Months



Base: 1,053 US online adults

Source: A commissioned study conducted by Forrester Consulting on behalf of Neustar, March 2013

Appendix C: Endnotes

[1] "Privacy by Design" is a framework developed within the Information and Privacy Commission of Ontario, Canada. Its goals are "ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage." In March 2012, the US Federal Trade Commission called for organizations to begin adopting the PbD framework. More details can be found at http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[2] California's "Right To Know Act of 2013" (AB-1921), sponsored by Assemblywoman Bonnie Lowenthal, would require organizations that retain data about customers to provide a copy of that information to the customer upon request. The full text of the proposed bill can be found at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1291

[3] See Natasha Singer's series on consumer database marketing for The New York Times, including the "What They Know" series at http://topics.nytimes.com/top/reference/timestopics/people/s/natasha_singer/index.html