



P³

OVERCOMING THE **PERSONALIZATION** VS. **PRIVACY PARADOX**

How to get ahead + stay ahead of the
changing marketing landscape.

JUNE 2018

jebbit



TABLE OF CONTENTS

INTRODUCTION

Foreword	3
The Personalization vs. Privacy Paradox	4

HOW DID WE GET HERE?

Personalization = ROI	7
A \$20 billion Industry	7
A Closer Look at the Merchandise	8
Is third-party data worth the money?	8
What Went Wrong	9
"Creepy" Personalization	9
Cambridge Analytica	10
GDPR	10

NEW CONSUMER EXPECTATIONS

Consumer Thoughts on Personalization	13
Personalization in Moderation	15
Control of Marketing Data	16
Transparency + Respect	16

GET AHEAD + STAY AHEAD

Rebuild Your Datasets	18
Throw out the bad data	19
Determine what you actually need	20
Source responsibly	20
Second-party data	21
First-party data	21
Engage in Two-way Dialogue	21
Declared data	22
Declared data + personalization	22

CONCLUSION

Conclusion	23
Additional Considerations	24

IMAGINE THIS...

You're shopping for a birthday gift for your mom. She's an avid bowler and while you don't care about bowling, you decide to buy her a new bowling bag online from a sporting goods store. Since you were automatically opted into the brand's email list when you made the purchase, you keep getting emails about bowling gear... which you would never, ever buy for yourself.

It's annoying, and you unsubscribe.

The next day, you log on to a new site and notice you're now getting ads for bowling gear. You have never visited the site before and are annoyed and slightly creeped out. How did they get that information?

You decide to no longer shop at the sporting goods store and to avoid the new site altogether.

We've all experienced something similar and although our response may not have been as extreme, there is a growing disconnect between consumers and marketers when it comes to personalization. Research shows:

..... **94%** of marketers believe personalization is critical to their "current and future success."

..... **92%** of US internet users are expressing concern about their online data privacy

As insights get deeper and pools of customer data expand, our ability to track customers across the internet gets more advanced.

It's time to talk about the difference between a great personalized experience and an invasion of privacy.

THE PERSONALIZATION VS. PRIVACY PARADOX

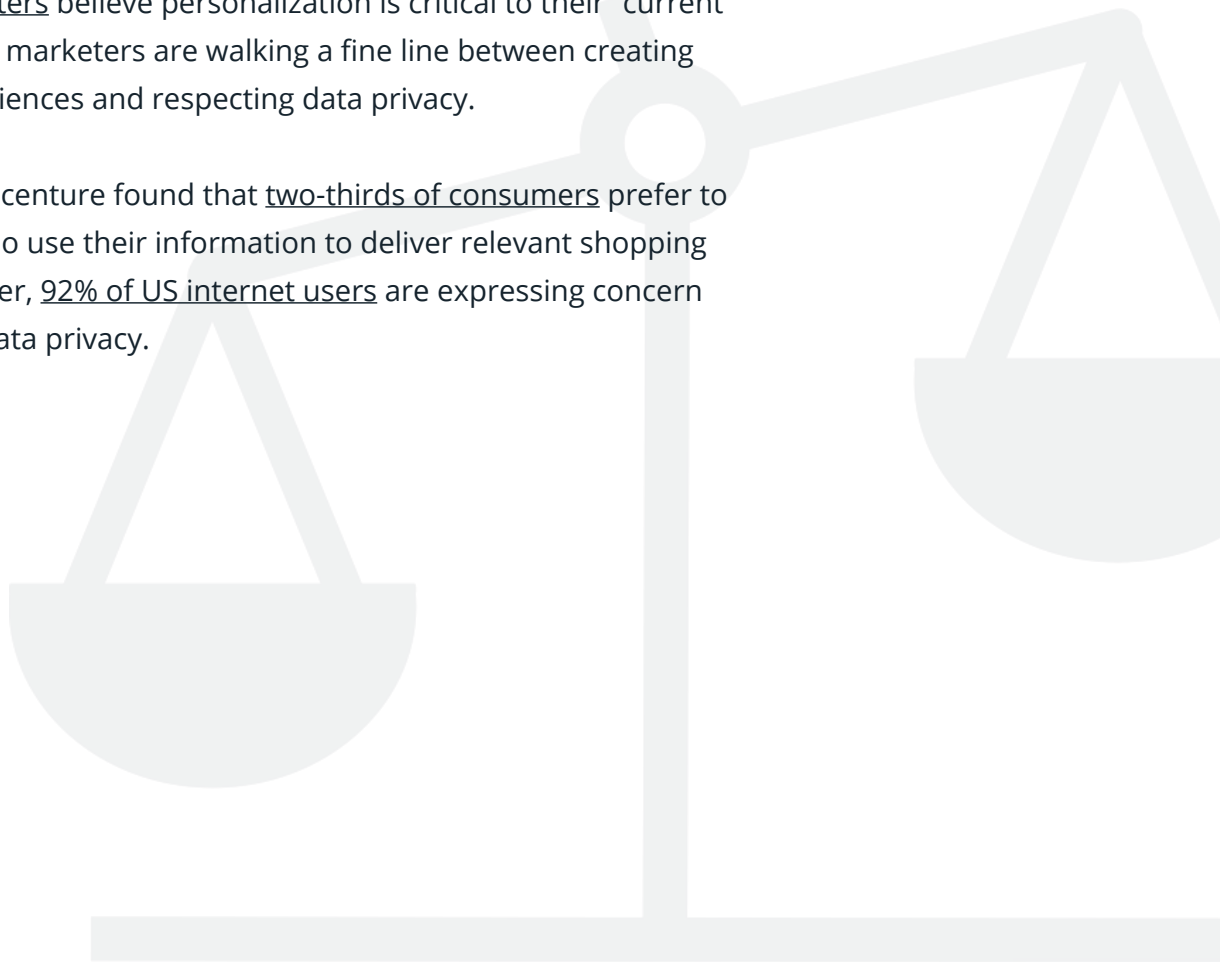
In 2012, Charles Duhig wrote an article for The New York Times Magazine titled, "[How Companies Learn Your Secrets](#)". The article explained how Target statisticians were able to predict if consumers were pregnant based on shopping history and other algorithms.

Activating their assumption, coupons were sent to a pregnant teen and found by her father, resulting in an angry dispute with the Target store.

This famous personalization horror story details what can go wrong when marketing efforts invade personal privacy. The example illustrates that even if the data activated is accurate, if not freely given by the customer, personalization can have deleterious results.

While [94% of marketers](#) believe personalization is critical to their "current and future success," marketers are walking a fine line between creating individualized experiences and respecting data privacy.

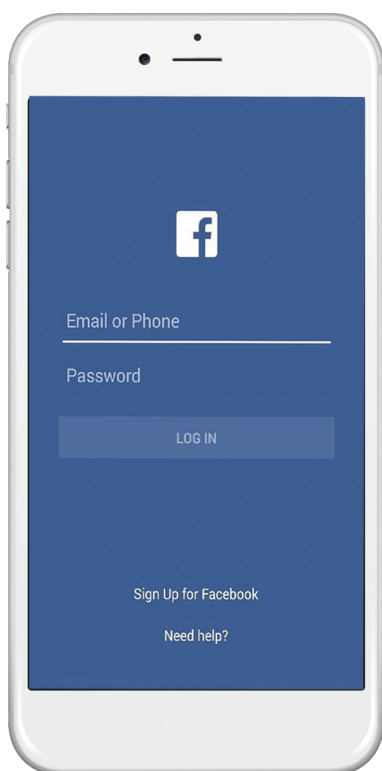
A recent study by Accenture found that [two-thirds of consumers](#) prefer to buy from brands who use their information to deliver relevant shopping experiences. However, [92% of US internet users](#) are expressing concern about their online data privacy.



In terms of landscape, Europe recently enacted the [General Data Protection Regulations \(GDPR\) Act](#), which has already had big implications for how brands, even here in the United States, can market to consumers.

New 'data rights', such as the right to be forgotten and the right to obtain consent before an E.U. citizen's data is used, will bring forward new challenges to how companies sell and advertise their products.

In the midst of GDPR, large data breaches have also heightened consumer awareness of how their data is collected, used, and protected.

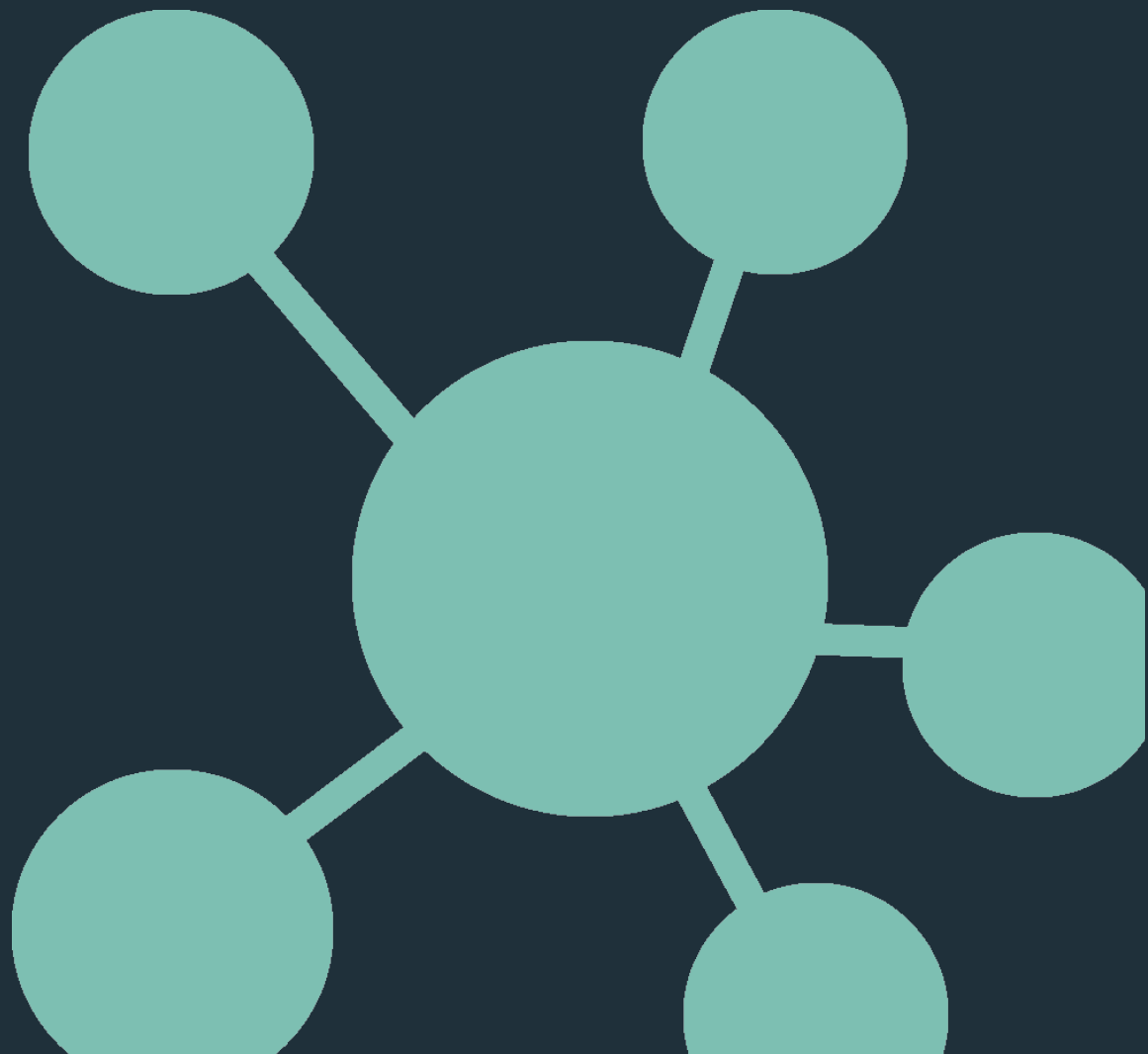


Whether it is Cambridge Analytica gaining access to private information on up to [87 million Facebook users](#), or the large-scale data breaches at [Equifax](#) or [Yahoo](#), Americans are now more [concerned about data privacy](#) than their income.

It's time for marketers to face the changing landscape.

In this report, we will explore how we got here, what the new consumer expectations are, and what smart marketers can do to get ahead.

HOW DID
WE GET HERE?





HOW DID WE GET HERE?

CONSUMERS WANTED PERSONALIZATION
AND BRANDS DELIVERED.

What began as a way to deliver personalized content resulted in “creepy” advertisements and raised concerns about both personal data privacy and data security.

PERSONALIZATION = ROI

Consumers expect personalization. Adobe found 67% of consumers think it's important for brands to automatically adjust content based on their current context and a whopping 42% get annoyed when their content isn't personalized.

Naturally, with numbers like those brands set out to deliver and have seen great results.

McKinsey research revealed that personalization can deliver five to eight times the ROI on marketing spend and lift sales by 10% or more.

FUELING PERSONALIZATION LED TO A \$20 BILLION DATA ECONOMY

It is estimated that by 2019, marketing data and analytics sales will reach \$187 billion, worldwide. In 2017 alone, US companies spent over \$20 billion on audience data and data management solutions.

However, while companies have continued to spend vast amounts on data solutions, there appears to be a lack of quality control. IBM estimates that the yearly cost of poor quality data, in the US alone, is \$3.1 trillion.

Just let that sink in.

So why does bad data cost so much?

Let's look at the data being bought and sold.

A CLOSER LOOK AT THIRD-PARTY DATA

The \$20 billion data economy is based on the buying, selling and management of third-party audience data.

Third-party data is information collected by an entity that does not have a direct relationship with the consumer.

Data vendors will often aggregate unrelated sources to compile third-party data sets - including information such as home addresses, voter registrations, birth dates, and credit scores, and combine that with data inferred from cookies, such as online browsing, click trails, and searches.

Third-party data can help marketers achieve great scale due to the massive amounts of information available. However, it is also available to all marketers, and therefore not a competitive advantage.

Because third-party data comes from an entity without a direct relationship with consumers, it is also the biggest offender in privacy disputes and runs a greater risk of inaccuracy.

Is third-party data worth the money?

With poor data quality costing businesses over \$3 trillion each year, we wanted to take a look at the accuracy of third-party data. To do so, we asked 100 individuals to access a well regarded third-party data vendor's registry on their personal computers and record the accuracy of their digital footprints.

What we found is that data being purchased and sold through this vendor was only 34% accurate.

This means that brands choosing to activate this data run a high risk of impersonal, inaccurate and irrelevant marketing at a tremendous cost.

34%

We found that data being purchased and sold through this third-party data vendor was only 34% accurate.

What participants had to say about their data accuracy:

"I feel like I have an alter ego who exists in this data registry. Overall hysterical."

"I'm listed in 3 different age brackets, none of which are my own."

"They have me covered as pretty much every age possible and every income bracket possible. I also apparently buy a lot of very generic things like cereal and milk... There were a TON of car-related hobbies and interests which **couldn't be farther from the truth.**"

WITH SO MUCH DATA, WHAT WENT WRONG?

To recap: Brands recognized the need to personalize their content - they bought lots of third-party data, activated it, and were seeing increases in ROI on their marketing spends. So, what went wrong?

Personalization tactics got invasive, data became less secure, and consumers took notice.

"CREEPY" PERSONALIZATION

Seventy-five percent of consumers say most forms of personalization are at least somewhat creepy. Going back to the Target example, when personalization gets too personal, people are not happy.

So what types of personalization should marketers avoid?

According to a recent survey by Accenture, consumers find the following personalization tactics the “creepiest:”

- **Text from a brand or retailer when walking by a store (41%)**
- **Mobile notification after walking by a store (40%)**
- **Ads on social site for items browsed on a brand website (35%)**

This means many of the personalization methods based on location and retargeting are not as effective as marketers once thought.

In fact, they can have the complete opposite effect, with 22% of consumers saying they will leave a brand after being creeped out.



CAMBRIDGE ANALYTICA

Of course you can't talk about data use without addressing the Cambridge Analytica scandal.

In 2016, Cambridge Analytica, an English political consultancy, was able to steal private information from 87 million Facebook users.

That data was then used to tailor ads designed to sway the 2016 presidential election.

The controversy occurred amidst growing discontent around how consumer behavioral data is being used to deliver content to consumers.

As a result, Cambridge Analytica has become the poster case for misuse of consumer data and has since spurred legislation proposals similar to GDPR in the United States.

It remains to be seen if legislation such as the CONSENT Act will move forward, but Facebook and many other companies have been mending their data policies as a result.

GDPR

A recent study revealed that more Americans are concerned about data privacy than their income and sixty-six percent of Americans want companies to be more transparent about how their data is used.

These sentiments are echoed globally and the embodiment can be seen with the passage of the E.U. General Data Protection Regulation (GDPR).

GDPR has renewed concerns over consumer privacy in the collection and activation of third-party data. Beginning May 25, 2018, companies now have to obtain consent from consumers to contact them for marketing purposes, share or sell data to third parties, and for any uses that the consumer "would not reasonably expect."

Post-GDPR, using third-party data to personalize content will be increasingly difficult and will force marketers to reevaluate their current data strategies and data sets.

NEW CONSUMER EXPECTATIONS





NEW CONSUMER EXPECTATIONS

PERSONALIZATION IN THE AGE OF THE CONSUMER

According to [Forrester](#), we are seven years into the Age of the Customer, an age defined by consumers placing elevated expectations on every interaction they have with brands.

As of 2018, recent studies by [Adlucent](#) and [The Economist Intelligence Unit](#) reveal consumers not only want personalization, they want transparency and control of their marketing data.

While [60% expect brands](#) to provide relevant online experiences, a resounding [96% of consumers](#) want brands to be more transparent about the collection and use of their personal data.

Amidst growing data privacy concerns and after enduring years of “creepy” and inaccurate personalization, consumers’ expectations have evolved. Recognizing and adjusting to these new expectations is critical to future success.

HOW DO CONSUMERS FEEL ABOUT **PERSONALIZATION** **IN 2018?**

Much of the data surrounding how consumers feel about personalization was taken prior to Cambridge Analytica. We wanted to gauge how consumers are feeling given the current landscape.

To do so, we surveyed 100 individuals and found that while personalization is still an expectation, customers are quicker to break ties with brands who implement it poorly.

Two out of three respondents said they have had “creepy” personalized experiences and **58% have broken ties** with a brand as a result.

When it comes to their personal data, 40% want tighter control, while 26% want complete ownership of who can use it.

Overall, the numbers are showing that personalization can make or break relationships and consumers are wanting a tighter grip over who can collect and use their data.

HOW CONSUMERS FEEL ABOUT PERSONALIZATION IN 2018

We surveyed 100 individuals and found that personalization can make or break relationships and consumers are wanting a tighter grip over who can collect and use their data.

100
Participants



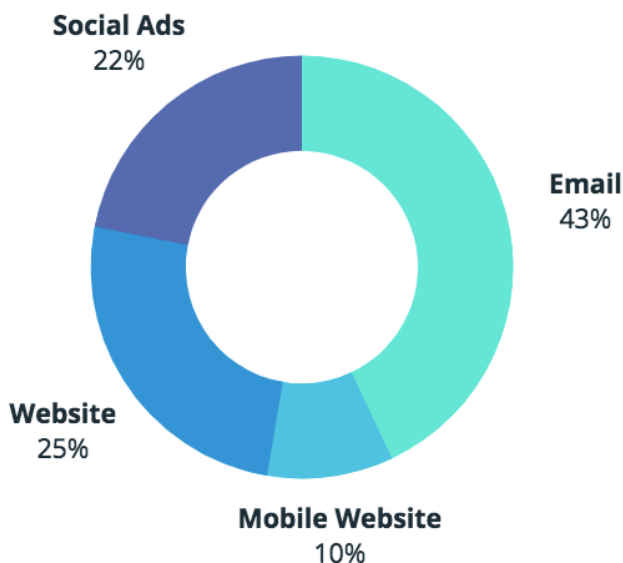
64%

Say they have experienced "creepy" personalization.

58%

Say they have broken ties with a brand over poor personalization.

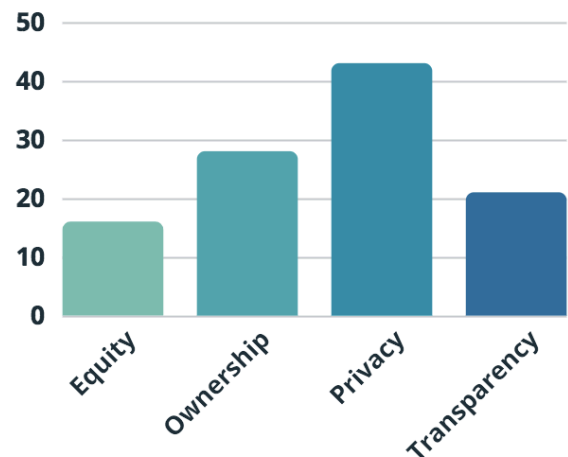
Where do consumers expect to see personalized experiences?



43%

expect to see personalized experiences in an email while only 10% expect personalization on a mobile website.

When it comes to personal data, what is most important?



40%

of participants say **Data Privacy** is most important to them.

NEW CONSUMER EXPECTATIONS

After enduring years of “creepy” and inaccurate personalization, consumers’ expectations have changed. Although they still want personalized experiences, data privacy concerns have reshaped what consumers are willing to accept.



CONSUMERS WANT PERSONALIZATION, BUT NOT TOO MUCH

As we’ve seen, using data to predict or make assumptions about customers can produce inaccurate or invasive marketing. As a result, customers are now quicker to cut ties with brands over poor personalization.

In fact, 41% of US consumers said they ditched a company because of “poor personalization and lack of trust.” These brand-consumer breakups cost companies \$756 billion in the US alone.

The cause? Many brands are currently prioritizing the wrong tactics and not paying attention to what consumers actually want - the ability to buy and consume on their own terms.

NEW CONSUMER EXPECTATIONS

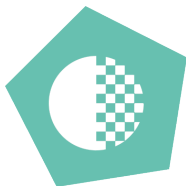


CONSUMERS WANT CONTROL OVER THEIR MARKETING DATA

When it comes to the collection of data, consumers want the control and transparency over what personal information is collected.

A recent study by The Economist found that 92% say it's important to control their own data, including about two of every three saying it's "very important". The majority also demand transparency about automatic data collection, which means being informed when personal data is being collected.

Going a step further, consumers also want to be in control of when their data is bought and sold - with 86 percent of consumers insisting that they should know when their data is passed on to third parties.



CONSUMERS EXPECT TRANSPARENCY + RESPECT

Nearly 27% of consumers have reported a brand experience that was too personal or invasive.

The cause? Almost two-thirds say it was because the brand had information about them that they didn't share knowingly or directly.

While 83% of consumers are open to sharing their personal data with businesses in exchange for better experiences, 96% of consumers want brands to be more transparent about the collection and use of their personal data.

In order to build trust and credibility, brands will need to take measures to ensure data privacy is respected.

GET AHEAD
+ **STAY AHEAD**





GET AHEAD + STAY AHEAD

THE WAY FORWARD HINGES ON TRUST AND RELATIONSHIPS

Moving forward, consumers expect relationships with brands to be similar to their real-life counterparts. When one party goes outside of the relationship for information, trust is broken.

To get and stay ahead of changing consumer expectations, marketers need to re-examine their data strategies and work to build trusting relationships with consumers.

The way forward hinges on accurate data, responsible data collection, and building trust through two-way digital dialogue.

GET AHEAD + STAY AHEAD

Since GDPR came into effect, it is estimated that 75% of all UK marketing data was rendered obsolete. To continue personalizing, marketers must re-examine their datasets and in many cases, start from scratch.

You can rebuild your data assets for accuracy and longevity by throwing out bad data, determining what you actually need, and by sourcing responsibly.

1. Throw out the inaccurate, irrelevant, outdated, and/or illegal data

The first step in rebuilding your data assets is to look closely at what you have and decide whether it's worth keeping.

Where did the data come from? How old is it? Do I really need this data? Was the data collected with consumer consent?

All of these questions can help when assessing whether or not to clean out your data.

For instance, if the majority of your data was bought from a third-party data vendor five years ago, you run the risk of outdated information.

If you didn't directly collect the data, consumers may be turned off when you personalize a message based on another company's information.

Also keep in mind, if you can't trace the roots of or didn't collect the data yourself, you run the risk of inaccuracy. A recent study published in Digiday revealed that a major third-party data vendor had 84% of users marked as both male and female. Another Digiday study found that 82% of marketers believe that third-party data is unreliable, largely due to its inaccuracies.

75%

Since GDPR came into effect, it is estimated that 75% of all UK marketing data was rendered obsolete.

82%

Digiday found that 82% of marketers believe third-party data is unreliable, largely due to its inaccuracies.

GET AHEAD + STAY AHEAD

2. Determine what data you actually need

Once you've successfully cleaned your data, ask yourself what data is needed to deliver personalized experiences.

What type of experiences do you want to deliver? What are the top 3-5 things you want to know about your customers? What do you have? What is missing?

For instance:

- **An eCommerce brand** may want to deliver custom shopping recommendations. They have transactional data and search history, but need to understand individual style preferences.
- **A travel company** may want to create custom itineraries based on individuals' travel preferences. They might have a record of previous trips, but are missing when consumers are planning to take their next vacation or who they plan to travel with.
- **A media company** may want to tailor topics to readers' content preferences. They understand what stories are performing well, but not necessarily what types of content consumers want to read.

In each case, brands must first decide the type of personalized experience they want to create, assess the data points they have, and decide what information is needed.

3. Source Responsibly

When looking to fill in the gaps, rebuild your dataset with fresh, accurate and responsibly sourced data.

Two options that fit the bill include **second-party** and **first-party data**. Although not perfect, these two types of marketing data eliminate the issues with third-party data and are sourced from direct relationships with consumers.

SECOND-PARTY DATA

Second-party data is another brand's, publisher's, or marketer's first-party data that you have access to. Two-times as many marketers say second-party data gives them good insights into their customers, as opposed to third-party data.

Second-party data can help you extend your audience, but it does have some limitations. Getting access to another entity's proprietary data set comes with red tape. It takes an significant amount of time to find, negotiate, and administer these deals.

Brands sharing their first-party data with another brand need to consider the implications concerning consumer privacy (especially in light of GDPR). Consumers must also be able to opt out of their data being leased to another company.

FIRST-PARTY DATA

First-party data is information that a company owns about consumers, created and collected through a direct relationship with that consumer.

Ninety-two percent of marketers believe using first-party data is critical to their growth and 81% percent see strong ROI from using first-party data in campaigns.

However, first-party data is the hardest category of marketing data to get at scale.

The methods of collecting it have inherent limitations: Focus groups are limited to 10-12 people, surveys have an average response rate of 10-15%, transactions only give you things like purchase amount, credit card type, and address, and most forms convert at rates below 25%.

Regardless if the data is second-party or first-party, what matters is the method by which it's captured. When personalization is built on these datasets, the consumer is aware of their buy-in. This leads to transparency and ultimately builds trust.

TWO-WAY DIALOGUE

In order to meet evolving expectations, businesses must create ongoing, two-way digital dialogues that resemble conversations customers would have in person.

One way to do this is through **declared data** capture.

CAPTURING DECLARED DATA

Taking first-party data a step further, declared data can help alleviate data privacy concerns by bringing data capture and activation out into the open.

Declared data is a type of first-party data that has been willingly and explicitly shared by an individual consumer, often about their motivations, intentions, interests, and preferences.

The key difference is that it comes directly and actively from customers.

Declared data doesn't replace your other data; it enhances it. Declared data is yours and it tells you what makes your customers unique as individuals. Used together, multiple data types will give you the most complete picture of your customers.

DECLARED DATA + PERSONALIZATION

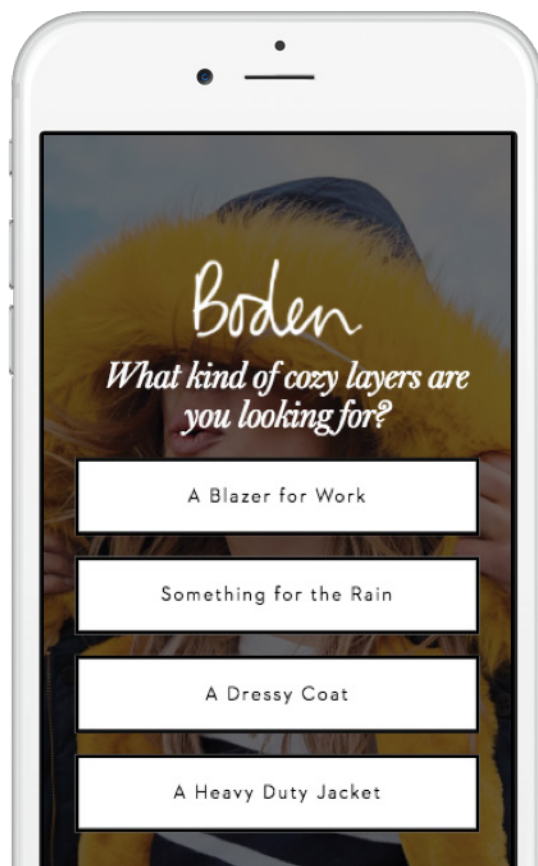
When personalization is done correctly with consumer buy-in, the results are dramatic. In fact, we've found that through activating declared data for personalization, business can see results such as **50% increase in conversion rates** and **9X in email click-through rates**.

..... **9X**

By capturing declared data on traveler preferences, Regent Seven Seas Cruises executed a personalized email campaign that saw **2X email open rates and 9X email click-through rates**.

..... **50%**

By capturing declared data on buyer intent, Boden created Facebook custom audiences to drive **50% more mobile conversions** through remarketing.

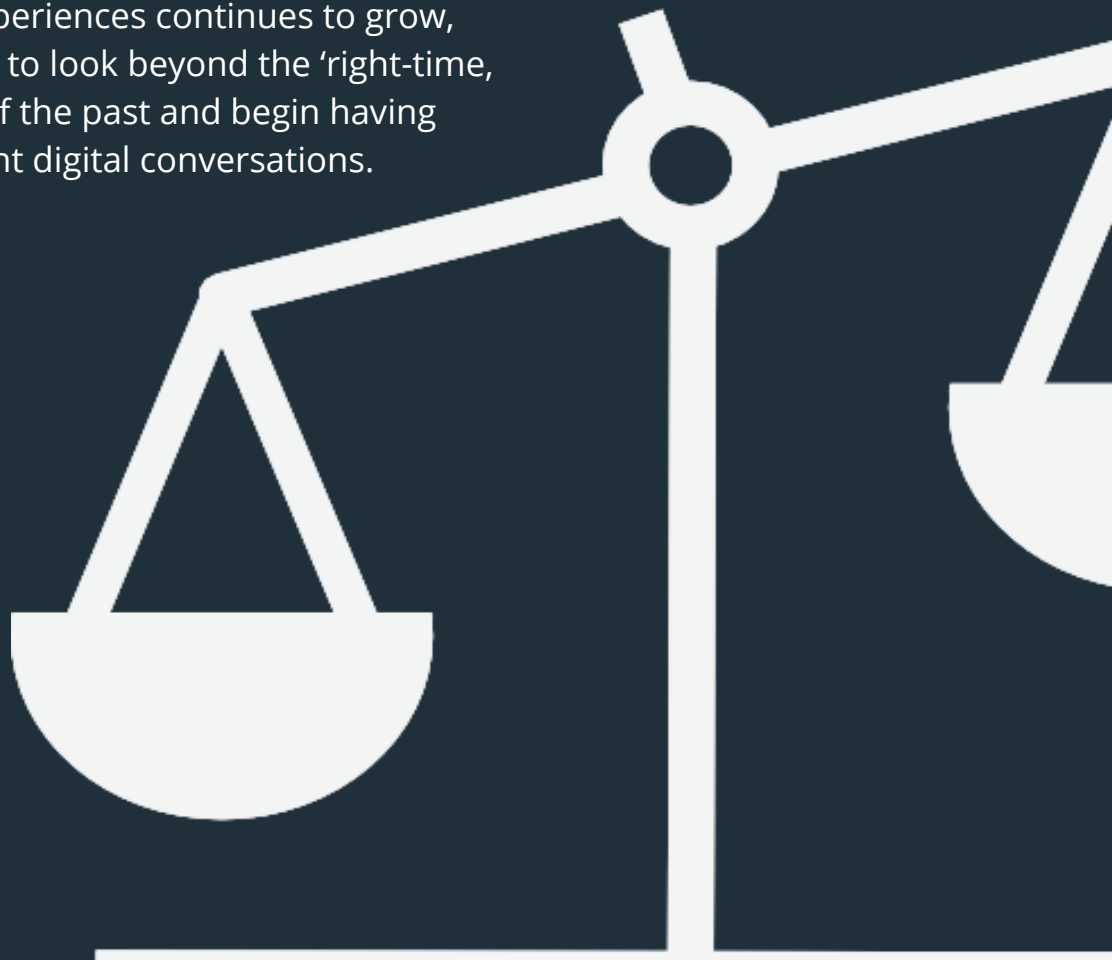


OVERCOMING THE PARADOX

In order to overcome the personalization vs. privacy paradox, marketers will need to regain consumer trust by evaluating their existing datasets and implementing methods for honest data capture.

In this Post-Cambridge Analytica environment, marketers must adapt. Consumers prefer consent-based marketing over third-party data tracking by a **2:1 margin** and will begin to gravitate toward brands that offer more transparency and control over their data.

These sentiments are here to stay and as demand for personalized experiences continues to grow, marketers will need to look beyond the 'right-time, right-place' tactics of the past and begin having two-way, transparent digital conversations.



ADDITIONAL CONSIDERATIONS

How ready is your brand to overcome the privacy versus personalization paradox? Begin by considering the following:

- How much of your marketing data was purchased through third-party vendors?
- How often do you activate personalization tactics based on third-party data?
- When was the last time you refreshed your marketing data?
- Was your data sourced responsibly with explicit consumer consent?
- Do you offer consumers a way to control what marketing data can be used and kept?
- Does your current personalization strategy encourage two-way dialogue?

ENDNOTES

PAGE 3:

- (2015, January 28). [Data Privacy is a Major Concern for Consumers](#) | TrustArc
- (2013, April 22). [94% of businesses say personalisation is critical to their success](#) | Econsultancy

PAGE 4:

- (2012, February 16). [How Companies Learn Your Secrets](#) | New York Times
- (2018). [Making it Personal](#) | Accenture

PAGE 5:

- (2018). [GDPR Information Portal](#) | EU GDPR
- (2018, April 4). [FACEBOOK EXPOSED 87 MILLION USERS TO CAMBRIDGE ANALYTICA](#) | Wired
- (2017). [The Equifax Data Breach](#) | Federal Trade Commission
- (2017, October 4). [Every Single Yahoo Account was Hacked](#) | CNN
- (2016, January 28). [Survey: More Americans worried about data privacy than income](#) | CBS

PAGE 7:

- (2018, February 8). [Consumer Demand for Personalized Content Reaches All-Time High](#) | CMO
- (2015, November). [Personalizing at Scale](#) | McKinsey & Company
- (2016, May 24). [Big Data, Analytics Sales Will Reach \\$187 Billion By 2019](#) | Information Week
- (2017, December 5). [Study: Companies spend more than \\$20B on third-party audience data, solutions](#) | Marketing Dive
- (N/A). [The Four V's of Big Data](#) | IBM

PAGE 8:

- (2014, January 28). [Defining Third-Party Data](#) | AdAge

PAGE 9:

- (2018, February 22). [Consumers Find Personalization Creepy, Study Says](#) | MediaPost

PAGE 10:

- (2018, April 10). [After Facebook hearing, senators roll out new bill restraining online data use](#) | The Verge
- (2018, January 28). [How Much Privacy People Will Give Up for Personalized Experiences](#) | AdWeek

PAGE 12:

- (2016, April 26). [Leadership In The Age Of The Customer](#) | Forrester
- (2018, May 9). [Data Wars: Information's Role in the New Era of Advertising](#) | Adlucent
- (2018). [What the Internet of Things Means for consumer privacy](#) | The Economist

PAGE 15:

- (2017, December 5). [The Price of Personalization Failure](#) | eMarketer

PAGE 16:

- (2017, March 7). [Global Study Indicates Nearly Nine Out of Ten Consumers Concerned About Data Security and Privacy; However, 80 Percent Demand Personalized Service](#) | Business Wire

PAGE 19:

- (2018, January 25). [GDPR kicks in this month: Here's how to save your marketing data](#) | Campaign
- (2017, January 5). [Why is third-party data still often wrong?](#) | Digiday
- (2018, January 15). [Publishers Warm to GDPR Benefits](#) | Digiday

PAGE 20:

- (2015, June). [The Promise of First-Party Data](#) | Signal
- (2016, September 16). [Taking a Second Look at Second-Party Data](#) | Speedeon Data
- (2015, May 21) [An In-Depth Look At Second-Party Data For Digital Marketers](#) | Marketing Land
- (2017). [An Audience of Individuals](#) | Think With Google
- (2015, June 23). [The Marketing Impact of First-Party versus Third-Party Data](#) | MarTech
- (2015, July 27). [What's a Good Survey Response Rate?](#) | SurveyGismo
- (2010, October 11). [Which Types of Form Fields Lower Landing Page Conversions?](#) | HubSpot

PAGE 22:

- (2018, January 23). [Declared Data, Defined](#) | Jebbit

PAGE 23:

- (2018, May 14). [New Survey Reveals Consumer Conflict between Privacy and Personalization](#) | Globe News Wire

GET A DEMO

To learn more about how to achieve great personalization at scale while respecting consumer data privacy visit: jebbit.com/demo

DECLARED DATA PLAYBOOK

Learn how you can use declared data to power personalized, contextually relevant marketing at: info.jebbit.com/the-declared-data-playbook

ABOUT JEBBIT

Founded by two entrepreneurs sick of online advertising's status quo, Jebbit's mission is to empowering the world's largest organizations to better communicate with and understand their audiences. As the world's first declared data platform, Jebbit gives enterprise brands the power to treat each customer as the individual they truly are through personalized marketing.

jebbit