How Consumer Privacy is Reshaping the Retail & Ecommerce Landscape

DATAGRAIL®

July 2020

www.datagrail.io

Introduction

Consumers are demanding increased privacy and transparency about how their personal data is handled

Brands that respond and prioritize privacy will win consumer loyalty in the decade ahead. According to Pew Research, the majority of Americans (64 percent) say they have personally experienced a major data breach.

A DataGrail study found that 54 percent of people feel either fed up, frustrated, or creeped out by companies that use their data to serve targeted ads. It's no wonder Americans listed "privacy of data" as the top priority companies should address this year, and four out of five believe there should be a law to protect their personal data.

The Age of Privacy has been a long time coming, so why are we highlighting this trend now? Because we're at a turning point in the journey.

In May 2018, the General Data Protection Regulation (GDPR) was introduced in the EU, forcing retailers to take stock of and potentially eliminate personal data they hold on consumers. It gave customers the right to request a copy of their data and have it erased. A month after GDPR went into effect, a Gartner survey showed that nearly a third of European consumers had exercised their new privacy rights, a much higher portion than expected.

While GDPR was the first, it's certainly far from the last. California's privacy law, known as the CCPA, went into effect on January 1, and enforcement began on July 1. This wouldn't be such a big deal for retailers if customers didn't have such high expectations of the customer experience (CX). **So how's a retailer to stay continuously compliant with existing and emerging privacy regulations all while exceeding customers' expectations?**

We're here to answer that question and more in this report, specifically created for retailers that want to get ahead of the competition.

Ready? Let's dive in.

Contents

The Retailer's Privacy Paradox 01

Third-Party Data vs First-Party Data vs Zero-Party Data 02

5 Ways to Give Customers Control of their Personal Data 04

Turn Privacy Into a Brand Differentiator 05

Case Study: Microsoft 05

DataGrail Study: Consumers' Privacy & Personal Data Expectations 07

Optimize the Customer Experience 08

Use Data to Wow Consumers in Unexpected Ways 09

Next Steps & Action Items 10

The Retailer’s Privacy Paradox

In 2020, retailers will embrace zero-party data as a way to mitigate the risk of privacy lawsuits, improve brand reputation, and gather more accurate consumer data to create significantly better customer experiences.

Zero-party data is information a person intentionally shares, but we’ll explain more about that in a second.

Consumers expect highly personalized experiences, but don’t want to give up their personal data all while governments around the world are enacting stringent privacy and security regulations around consumer data privacy.

Up until now, retailers used two types of data in order to deliver personalized experiences: first-party data and third-party data. Many have never considered zero-party data, but they should, especially in combination with first-party data.

Third-party data vs. first-party data vs. zero-party data

Third-Party Data

What is it?

- Data collected and compiled by outside vendors, which retailers purchase or rent from a brand
- Could be personally identifiable information (PII) or anonymized data
- EG: Demographics, online activity that guess at a consumer's interests and preferences

How do you get it?

- Purchase from third-party vendors

How do they get it?

- Gathered from a myriad of sources, with no clear origin

Cons:

- Comes with serious risk and liability
- Impossible to know how accurate it is, so can lead to bad customer experiences
- No competitive advantage because available to anyone who purchases

First-Party Data

What is it?

- Data collected directly from customer, typically during site browsing and sales transactions
- EG: Name, email, address, browsing habits, product preferences, etc.

How do you get it?

- Usually collected using tracking pixels, cookies and transaction data

Pros:

- Directly from source's behavior
- Shows trends over time

Cons:

- Behaviors/interactions may not accurately depict reality
- Consumers are weary of sharing their data now so harder to get
- Strict privacy laws and "cookieless" futures, make this data somewhat risky

Zero-Party Data

What is it?

- Information a consumer voluntarily and intentionally shares with a retailer

How do you get it?

- Consumers elect to give this data directly to retailers, to provide more insights into their preferences

Pros:

- Less risky
- More accurate
- More insights into users' motivations, intentions and interests so more robust view of consumer
- Builds direct relationships with consumers and increases brand loyalty

Cons:

- Takes time to develop consumer trust

Opportunity:

Put consumers in control of their data

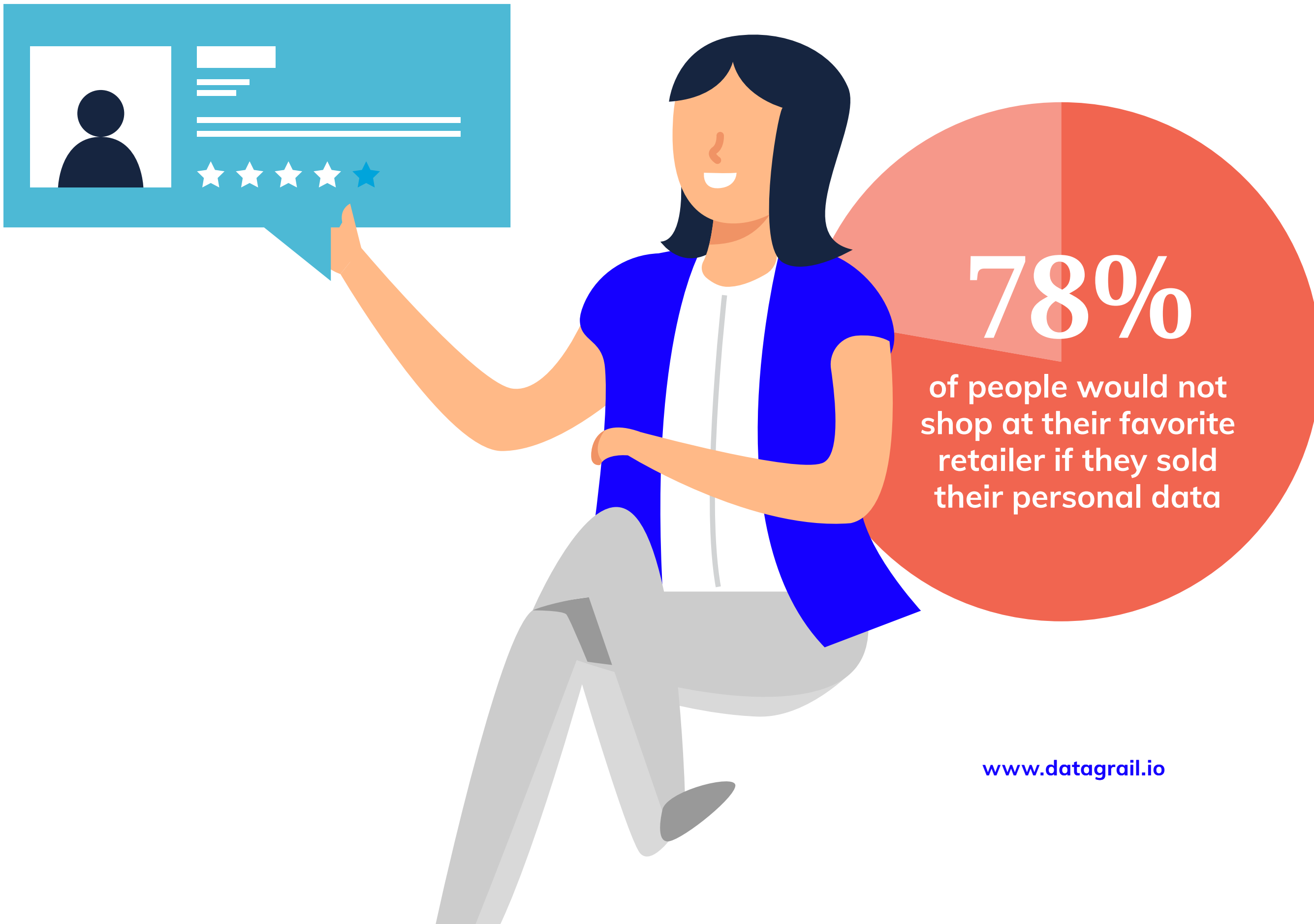
While 83 percent of consumers expect to have control over how businesses use their data, the majority feel like they have little to no control over how retailers use it.

What they can control, however, is where they spend their money.

> "...the majority feel like they have little to no control over how retailers use [their data]."

DataGrail's consumer privacy survey found that **78 percent of people** would not shop at their favorite retailer if they found that they sold their personal data, and that three out of four respondents would pay more for online services to ensure they didn't sell their data.

Retailers that give users the control they so badly desire will not only increase trust but also make customers feel accountable to actively managing it, like they would a bank account.



78%

of people would not shop at their favorite retailer if they sold their personal data

5 Ways to Give Customers Control of Their Personal Data

1 Be transparent

Ask for the data you need up-front and explicitly state why you need it. Be transparent and genuine.

You may be surprised that consumers are willing to give companies they trust the data they want, when it's asked in the right way at the right time. Stitch Fix is a prime example of a retailer that has personalization down to a [very human] science.

2 Ask for feedback

Also ask for feedback after you deliver the results.

This could be as easy as installing a scroll-up feedback poll with a tool like Hotjar to make sure customers are actually getting the right kind of product recommendations or content for them.

3 Write a clear privacy policy

Write a clear privacy policy that is easy to find and read.

The New York Times reviewed more than 150 privacy policies and rated BBC as the best overall, with Craigslist and Vimeo earning top spots as well for its level of readability.

Bookmark this resource
Usable Privacy Policy Project

4 Simplify DSAR & DNS requests

Make data subject access requests (DSARs) and Do Not Sell (DNS) requests easy for consumers.

Provide a simple and straightforward method for consumers to submit DNS and DSARs, which are required under privacy regulations such as GDPR and CCPA. When brands don't do this, consumers head to Twitter. See thread.

If the above Twitter thread sounds like your company's current DSAR process, consider giving DataGrail a test drive, which automates all of Restoration Hardware's DSARs.

5 Respect consumer preferences

Adhere to consumers' preferences.

This is a big one. A DataGrail study found that 63 percent of people have unsubscribed from an email list, yet continue to receive email from that company. How aggravating is that?

To ensure this doesn't happen to one of your customers, retailers need a system that integrates all of your third-party cloud vendors across the entire organization, so when a consumer updates their preferences, it's reflected across all of your systems.

Turn privacy into a brand differentiator

Ninety-four percent of consumers say they're more loyal to brands that offer complete openness, and 89 percent of people say they're willing to give transparent companies a second chance after a bad experience.

Just as consumers reward businesses that try to do the right thing, they're also willing to stray from those that don't. In recent years, the way in which companies have prioritized data privacy has become a significant factor in influencing consumer sentiment.

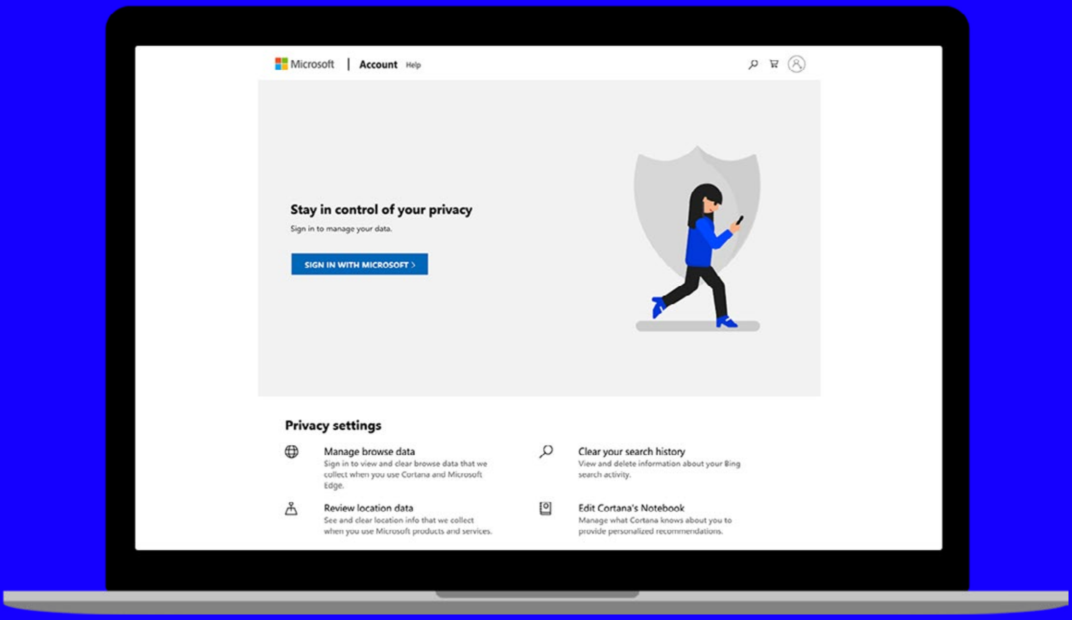
According to the Axios Harris Poll, which ranks the most visible companies' consumer reputations, Facebook, Amazon, Apple, Netflix and Google (FAANG) took a massive reputation hit, with Facebook's reputation plummeting the most following the Cambridge Analytica scandal. The issue at hand? According to the poll, "At the core of America's concern with Silicon Valley is data privacy."

Case Study: Microsoft

Microsoft, on the other hand, dramatically improved its reputation. The company's reputation has been on a steady incline since 2016, ranking at No. 20 from 2016-2017, No. 11 in 2018 and breaking the top 10 at No. 9 in 2019, in which it ranked No. 4 overall for Business Trajectory with notable ranks for Trust (No. 19) and Character (No. 18).

Could it be related to the fact that they created a robust customer privacy dashboard, and applied CCPA rules broadly, across all Americans?

It's very likely!



Stay in control of your privacy

Sign in to manage your data.

Privacy settings

Manage browse data
Sign in to view and clear browse data that we collect when you use Cortana and Microsoft Edge.

Clear your search history
View and delete information about your Bing search activity.

Review location data
See and clear location info that we collect when you use Microsoft products and services.

Edit Cortana's Notebook
Manage what Cortana knows about you to provide personalized recommendations.

All of the above boils down to consumers' increasing concerns around data privacy.

In the same poll, 69 percent of Americans said companies should be addressing data privacy, but only 17 percent feel they are making an impact.

Not surprisingly, this is the biggest issue driving Facebook's decline: with only 15 percent of Americans agreeing that Facebook "Securely protects its customers personal information and data;" Google: 37 percent, Apple: 35 percent.

DataGrail Study: Consumers’ Privacy & Personal Data Expectations

4 in 5 Americans think there should be a law in place to protect personal data

3 in 4 would boycott their favorite retailer if it failed to keep personal data safe

7 in 10 want to deny businesses the ability to sell their data to third parties

83% expect to have control over how businesses use their data

71% of people would like to know which businesses are collecting data on them and how they use it

54% are frustrated by companies that use their data to serve targeted personalized ads

Brands who were prepared to meet and exceed the GDPR standards, saw a marked increase in consumer trust, loyalty and engagement levels. - CMO

68% expect to be able to opt-out of a company selling their data to a third party

Optimize the Customer Experience

Another way to make privacy a brand differentiator is to make it easy for people to change their privacy settings on your website. More importantly, customers need to be able to find the privacy policy on your website. As it turns out, many – even power users – cannot, according to a recent survey, which had participants search for privacy choices and policies in the account settings of popular websites, such as nytimes.com and foodandwine.com.

The takeaway from the survey is that there needs to be an industry standard for these settings and policies, just as unsubscribe links have become standardized to appear at the bottom of emails. Linking to them in the footer is a good place to start. Additionally, it helps if you link to this page(s) from multiple parts of the website.

> *"The pressure is building up for companies to make these choices easier for people to use. It's up to us as academics to communicate our findings with external stakeholders like regulators or companies themselves."* (Tech Xplore)

Bookmark this resource
Privacy UX: Privacy-Aware Design Framework

Opportunity:

Use data to wow consumers in unexpected ways

Reading Recommendations
What shoppers really want from personalized marketing

Retailers walking a tightrope between data privacy and personalization

Imagine having your customer manage and regularly update their own comprehensive CRM profile?

- The data would be more accurate since they're volunteering the information.
- Two-thirds of European brands indicated that they actually increased their programmatic ad spending in the eight months after the GDPR came into force on May 25th, 2018. Three-quarters (76%) of UK brands also reported data quality improvement. — IAB
- Zero-party data enables greater personalization, which potentially can increase average order value (AOV) because shoppers are more likely to spend more when the experience is properly tailored to them.
- 49% of consumers have purchased a product that they did not initially intend to buy after receiving a personalized product recommendation from a brand.
- It creates a greater feeling of trust and connection to a brand.
- Zero-party data enables retailers and brands to build direct relationships with consumers, and, in turn, better personalize their marketing efforts, services, offers and product recommendations without the guesswork.

Next Steps:

Make privacy your competitive advantage

By now, you understand the potentially massive implications of not complying with new privacy regulations, but you may be wondering:

Where do we go from here?

Don't fret - DataGrail has you covered.

Action Items

1

Read our in-depth, step-by-step CCPA Compliance Guide to learn exactly what retailers must do to become compliant

2

Request a complementary demo of DataGrail, the highest rated privacy compliance software on G2 (rated 5 stars!)

3

Benchmark where you are compared to your peers, in our first-ever State of CCPA report. See how many data subject requests you should anticipate as enforcement for CCPA ramps up www.datagrail.io

DATAGRAIL®