How Businesses Are Collecting Data (And What They're Doing With It)

Many businesses collect data for multifold purposes. Here's how to know what they're doing with your personal data and whether it is secure.

Written by: **Max Freedman,** Senior Analyst Editor Reviewed: **Sandra Mardenfeld,** Senior Editor
Updated Oct 20, 2023

How can you protect your data?

As technologies that capture and analyze data proliferate, so do businesses' abilities to contextualize data and draw new insights from it. Through consumer behavior and predictive analytics, companies regularly capture, store and analyze large amounts of quantitative and qualitative data on their consumer base every day. Some companies have built an entire business model around consumer data, whether they sell personal information to a third party or create targeted ads to promote their products and services.

Here's a look at some of the ways companies capture consumer data, what they do with that information, and how you can use the same techniques for your own business purposes.

Types of consumer data businesses collect

The consumer data that businesses collect break down into four categories:

1. **Personal data.** This category includes personally identifiable information such as Social Security numbers and gender, as well as nonpersonally identifiable information, including your IP address, web browser cookies and device IDs (which both your laptop and mobile device have).

2. **Engagement data.** This type of data details how consumers interact with a business's website, mobile apps, text messages, social media pages, emails, paid ads and customer service routes.
3. **Behavioral data.** This category includes transactional details such as purchase histories, product usage information (e.g., repeated actions) and qualitative data (e.g., mouse movement information).
4. **Attitudinal data.** This data type encompasses metrics on consumer satisfaction, purchase criteria, product desirability and more.

How do businesses collect your data?

Companies capture data in many ways from many sources. Some collection methods are highly technical, while others are more deductive (although these processes often employ sophisticated software).

The bottom line, though, is that companies are using a cornucopia of collection methods and sources to capture and process customer data on metrics, with interest in types of data ranging from demographic data to behavioral data, said Liam Hanham, data science manager at Workday.

"Customer data can be collected in three ways: by directly asking customers, by indirectly tracking customers, and by appending other sources of customer data to your own," said Hanham. "A robust business strategy needs all three."

Businesses are adept at pulling in all types of data from nearly every nook and cranny. The most obvious places are from consumer activity on their websites and social media pages or through customer phone calls and live chats, but there are more interesting methods at work as well. **[Make sure your company has the best business phone system.]**

One example is location-based advertising, which uses tracking technologies such as an internet-connected device's IP address (and the other devices it interacts with – your laptop may interact with your mobile device, and vice versa) to build a personalized data profile. This information is then used to target users' devices with hyperpersonalized, relevant advertising.

Companies also dig deep into their customer service records to see how customers have interacted with sales and support departments in the past. Here, they are incorporating direct feedback about what worked and what didn't, what a customer liked and disliked, on a grand scale.

Besides collecting information for business purposes, companies that sell personal information and other data to third-party sources have become commonplace. Once captured, this information regularly changes hands in a data marketplace of its own.

Key Takeaway

Customer data can be collected in three ways: by directly asking customers, by indirectly tracking customers, and by appending other sources of customer data to your own.

Turning data into knowledge

Capturing large amounts of data creates the problem of how to sort through and analyze all that information. No human can reasonably sit down and read through line after line of customer data all day long, and even if they could, they probably wouldn't make much of a dent. Computers, however, sift through this data more quickly and efficiently than humans, and they can operate 24/7/365 without taking a break.

As machine learning algorithms and other forms of AI proliferate and improve, data analytics becomes an even more powerful field for breaking down the sea of data into manageable tidbits of actionable insights. Some AI programs will flag anomalies or offer recommendations to decision-makers within an organization based on the contextualized data. Without programs like these, all the data captured in the world would be utterly useless.

Tip

The best CRM software can be used to store customer data in an easily accessible way that makes it useful to your sales and marketing teams.

How do businesses use your data?

There are several ways companies use the consumer data they collect and the insights they draw from that data.

1. To improve the customer experience

For many companies, consumer data offers a way to better understand customer needs and boost customer engagement. When companies analyze customer behavior, as well as vast troves of reviews and feedback, they can nimbly modify their digital presence, goods or services to better suit the current marketplace.

Not only do companies use consumer data to improve consumer experiences as a whole, but they also use data to make decisions on an individualized level, said Brandon Chopp, digital manager for iHeartRaves.

“Our most important source of marketing intelligence comes from understanding customer data and using it to improve our website functionality,” Chopp said. “Our team has improved the customer experience by creating customized promotions and special offers based on customer data. Since each customer is going to have their own individual preferences, personalization is key.”

2. To refine a company’s marketing strategy

Contextualized data can help companies understand how consumers are engaging with and responding to their marketing campaigns, and adjust accordingly. This highly predictive use case gives businesses an idea of what consumers want based on what they have

already done. Like other aspects of consumer data analysis, marketing is becoming more about personalization, said Brett Downes, director at Haro Helpers.

“Mapping users’ journeys and personalizing their journey, not just through your website but further onto platforms like YouTube, LinkedIn, Facebook or on to any other website, is now essential,” Downes said. “Segmenting data effectively allows you to market to only the people you know are most likely to engage. These have opened up new opportunities in industries previously very hard to market to.”

3. To transform the data into cash flow

Companies that capture data stand to profit from it. Data brokers, or data service providers that buy and sell information on customers, have risen as a new industry alongside big data. For businesses that capture large amounts of data, collecting information and then selling it represent opportunities for new revenue streams.

This information is immensely valuable for advertisers, and they’ll pay for it, so the demand for more and more data is increasing. That means the more disparate data sources data brokers can pull from to package more thorough data profiles, the more money they can make by selling this information to one another and to advertisers.

4. To secure more data

Some businesses even use consumer data as a means of securing more sensitive information. For example, banking institutions sometimes use voice recognition data to authorize a user to access their financial information or protect them from fraudulent attempts to steal their information.

These systems work by pairing data from a customer’s interaction with a call center, machine learning algorithms, and tracking technologies that can identify and flag potentially fraudulent attempts to access a customer’s account. This takes some of the guesswork and human error out of catching a con.

As data capture and analytics technologies become more sophisticated, companies will find new and more effective ways to collect and contextualize data on everything, including consumers. For businesses, doing so is essential if they want to remain competitive well into the future; failing to do so is like running a race with your legs tied together. Insight is king, and insight in the modern business environment is gleaned from contextualized data.

Data privacy regulations

So much consumer data has been captured and analyzed that governments are crafting strict data and consumer privacy regulations designed to give individuals a modicum of control over how their data is used. Below are four prominent consumer privacy regulations.

European Union General Data Protection Requirements

The European Union's General Data Protection Requirements (GDPR) lays out the rules of data capture, storage, usage and sharing for companies. GDPR regulation and compliance doesn't just matter for European countries – it's a law applicable to any business that targets or collects the personal data of EU citizens.

Did You Know?

Companies that ignore GDPR compliance and fail to abide by their legal obligation to uphold consumer privacy may face fines of up to 20 million euros or up to 4% of annual revenue, whichever is higher.

California Consumer Privacy Act

Data privacy has made it to the U.S. in the form of the California Consumer Privacy Act (CCPA). The CCPA is similar to GDPR regulation but differs in that it requires

consumers to opt out of data collection rather than putting the onus on service providers. It also names the state as the entity to develop applicable data law rather than a company's internal decision-makers.

Virginia Consumer Data Protection Act

On January 1, 2023, the Virginia Consumer Data Protection Act (VCDPA) will go into effect. As with the CCPA, the VCDPA will put the onus on consumers to opt out of companies processing or selling their data. The VCDPA will also require companies to store only data relevant to their goals and then delete that data once the goal has been achieved. Any companies to which the VCDPA applies must inform consumers of their rights under the law and how to exercise them.

Colorado Privacy Act

On July 1, 2023, the Colorado Privacy Act (CPA) will go into effect. As with the CCPA and the VCDPA, the CPA requires consumer opt-out. The CPA covers targeted advertising and certain types of data-based profiling as well. Data-holding entities will be required to address consumer requests within 45 days and display privacy notices on their websites.

Tip

If you're looking for an easy way to understand privacy policies without reading them top to bottom, check out this helpful privacy policy analyzer tool from Security.org.

What do consumers think of business data collection?

According to a 2022 Ipsos poll, 70% of Americans think that, over time, limiting who can and can't access their data has become tougher. This poll also found that only 34% of Americans think that companies adequately safeguard consumer data.

Ipsos also asked the poll's 1,005 respondents about how they protect their data. Only 16% of respondents took all six data security measures about which Ipsos asked. Another 49% of respondents took three or fewer of these measures. There was a correlation between a respondent's number of security measures taken and their cynicism about adequately controlling access to their data.

Further, 78% of respondents said they wanted to require companies to obtain their consent before accessing and using their data. Similarly, 71% wanted to stay anonymous online, and 70% wanted the ability to scrub their data from the internet. Taken as a whole, the results suggest that the average consumer is both worried about their online data and unsure of how to protect it.

How can you protect your data?

Experts recommend taking the following steps to keep your data as private as possible.

- **Block ads and trackers.** The ads you encounter while browsing the internet can collect your data. Many websites also include trackers that can obtain your data, and businesses can access this data. Browser extensions that block ads and trackers can create a privacy barrier around this information.
- **Use a VPN.** When you browse the internet with a VPN, you tunnel information from your device to a server. This tunneling hides your browsing activity, putting up a wall between businesses and your data. The VPN will encrypt all your data as well.
- **Reconsider free apps and platforms.** Social media platforms are free because they sell your data to make a profit. The same may be true for any free app. That's a reason to avoid free apps or limit your free app usage to solely those from reputable companies. For example, the free Slack mobile app is probably fine since you can pay for Slack. But some random free gaming app with no paid option might be selling your data.
- **Sign up for unimportant memberships with fake information.** Nobody would tell you to use a fake name, phone number or address for, say, your health insurance plan. But that's a trusted and necessary service with a revenue stream independent of your personal data. On the other hand, non-essential services – say, a streaming

subscription – might sell your name, phone number and address data. Using fake information can protect your data in this case.

- **Avoid linking your apps**. Connecting your personal apps can make them more convenient to use, but these apps will also share your data with one another. See if you can go without connecting apps so that you don't build more bridges from your data to businesses.

The future of business data use

Data privacy regulations are changing the way businesses capture, store, share and analyze consumer data. Businesses that are so far untouched by data privacy regulations can expect a greater legal obligation to protect consumers' data as more consumers demand privacy rights. Data collection by private companies, though, is unlikely to go away; it will merely change in form as businesses adapt to new laws and regulations.

Adam Uzialko also contributed to the reporting and writing in this article. Some source interviews were conducted for a previous version of this article.

Written by: **Max Freedman,**
Senior Analyst

Max Freedman has spent nearly a decade providing entrepreneurs and business operators with actionable advice they can use to launch and grow their businesses. Max has direct experience helping run a small business, performs hands-on reviews and has real-world experience with business technology. At Business News Daily, Max covers accounting software, POS systems and digital payroll solutions, as well as leading medical software and text message marketing services. Max has written hundreds of articles for Business News Daily on a range of valuable topics, including small business funding, time and attendance, marketing and human resources.

EMAILLINKEDIN