Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

August 2026

How companies use your data and how to protect it

In a world where most every online action leaves a digital footprint, data brokers have become major players in collecting and selling personal information. These companies gather data from countless sources, analyze it, and package it for sale to advertisers, financial institutions, marketers, and even other data brokers.

Who are data brokers?

Data brokers are companies that specialize in collecting and aggregating consumer data. They gather information from a variety of sources – public records, loyalty programs, online browsing histories, mobile apps, subscription services, retail transactions, social-media activity, and other sources. Much of this data collection is technically legal, but it often happens without consumers' explicit awareness.

Once collected, data is sorted into detailed consumer profiles, which can range from basic demographic details to highly specific insights about behaviors, habits, and personal preferences. Data brokers use algorithms and analytics to infer patterns, allowing them to categorize individuals into groups such as "homeowners," "new parents," "outdoor enthusiasts," or "high-value spenders."

What data do they sell?

The information sold by data brokers varies widely. Commonly shared data categories include:

- Names, addresses, phone numbers, and demographic information.
- Shopping history and brand preferences.
- Income ranges, household size, and lifestyle interests.
- Online behavior, including browsing patterns and frequently visited websites.
- Location data collected from mobile apps.
- Predictive insights, such as purchase likelihood or financial risk indicators.

Some brokers also handle more-sensitive categories, such as health-related buying habits or behavioral predictions. Although data is usually sold in bulk rather than tied to a single identified person, the level of detail can still expose consumers to risks ranging from targeted scams to discriminatory marketing practices.

Why it matters

The profiles that consumers fall into influence the ads they see, the prices they're offered, and even how companies assess them for credit, insurance, and/or employment. In the wrong hands, detailed data can also increase exposure to fraud and identity theft.

How to protect your personal information

Even though data collection is widespread, consumers can take practical steps to limit how much of their information ends up in databases:

- Minimize data sharing. Limit participation in loyalty programs, free apps, and online quizzes. Review privacy settings on social media to restrict what you share publicly.
- Opt out of data broker lists. Major brokers offer opt-out forms, although the process can be tedious. Privacy services can automate removals across multiple databases for convenience. Retail websites may have a link at the bottom of the page with options for opting out of data collection.
- Limit mobile app permissions. Disable unnecessary access to your location, contacts, photos, and activity data.

- Read privacy policies to understand which of your information is being shared and with whom. In general, if a privacy policy doesn't restrict sharing, it's likely that an app or website is sharing your information.

How to safeguard your personal identifiable information

Data brokers are deeply embedded in the modern digital marketplace, but consumers are not powerless. By being selective about the information they share and being proactive about opting out, individuals can significantly reduce their exposure and protect their personal information.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Are there privacy risks with AI use?

Consumers have many questions about popular artificial intelligence (AI) tools. Is AI safe to use? Will AI violate my privacy? Such concerns are legitimate for those relying on AI tools to help with everyday tasks.

Many people are starting to use ChatGPT, Gemini, and/or Claude to do research, track tasks, and tackle other work and household issues. These powerful tools rely on AI to create specifically tailored responses to each inquiry.

The very act of typing information into a public chatbot means losing some control over any information being disclosed by a consumer. Many AI tools use what the information typed into it and the files shared with it to help better train the model to become even "smarter." The model, then, is always finding ways to improve how it interacts with consumers as well as the results provided in real time to help users with tasks. Unless you explicitly "opt out" based on settings found within the specific AI tool, personal conversations may be stored and analyzed. If you're using the free version, you may not be able to opt out of your information being used to train the model. Also, keep in mind that, just as a medical office or at a retail chain storing your information can be compromised by a data breach, so can AI tools.

AI platforms may also infer personal details about you based on your questions and responses, which might trigger advertising of targeted products and services. And if you have other accounts associated with the parent company of the AI chatbot, there could be information shared cross-platform. For example, if you're using Google Gemini, it may also cross-reference your account information and activities in other Google products and services, such as your Gmail account.

Here are some tips to help protect yourself when using AI platforms:

- Avoid disclosing personal identifying information into AI tools. For example, be careful not to include names, addresses, account numbers, and Social Security numbers. Consider whether you would share this information with a stranger: If you wouldn't, don't share it with an AI chatbot.

- Review the AI tool's privacy policy and account settings. Look for options such as one that turns off model training. This should help prevent your conversations from being saved and from being used to help refine the AI tool's performance. Some chatbots provide enhanced privacy options such as "incognito" modes or "temporary" chats that won't be retained in the AI platform's system.
- Be especially careful with free versions of AI tools. Enterprise or paid versions of AI chatbots may include stricter data-processing agreements to help prevent your data from being ingested into the public model.
- Know that most of the major AI platforms allow you to use a basic version without signing in or linking your chat to the personal information you may have stored in your account. However, that doesn't mean it won't use the information you provide to train the model.
- Most AI platforms allow you to delete old chats. If you have any second thoughts about information you have already shared, delete the old chat. Be aware that AI platforms may vary in how quickly or completely your chats are deleted from their databases.
- Understand that apps you already interact with may currently be integrating AI. If you get a notification or hear that AI is now part of an app and you don't want the AI tool to have access to or be trained on your information, check the app settings to see whether opting out is an option.

If you suspect a scam or an unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Learn about medical identity theft

Identity thieves steal personal information – say, your Social Security number – to use for many purposes. Some want to open a credit card or take out a loan in your name.

Others use your Social Security number or other information, such as a health insurance account number or a Medicare account number, to have you billed for doctor's visits, prescriptions, medical devices, or even a surgery. This is called medical identity theft.

Medical identity thieves can hold you financially responsible for expensive medical procedures and equipment as well as prematurely exhaust your benefits while a scammer uses your insurance or Medicare plan for medical treatments. This criminal behavior can also lead to misinformation becoming part of your medical file, which can lead to improper treatment and other dangerous errors affecting your future care.

To ward off medical identity theft, keep all of your medical insurance records in a safe place. Such records include health insurance enrollment forms, cards and explanation of benefits statements; Medicare summary notices; billing statements from medical providers; and prescriptions and prescription bottles.

Remember that identity thieves will dumpster-dive and go through an unlocked mailbox to try to uncover personal information. As with other sensitive information, statements containing medical details should be removed from your mailbox as soon as possible. Consider receiving medical bills and statements online to help limit the amount of information you get by mail. Shred medical information you no longer need, and use a permanent marker to block out information that cannot be shredded.

Here are some red flags from the Federal Trade Commission (FTC) to help spot medical identity theft:

- You receive a doctor's bill or an explanation of benefits for services you didn't receive or prescription medication you don't take. Be sure to read your insurance company's explanation of benefits and Medicare's summary notices to verify every charge.
- A debt collector contacts you about a medical debt you don't owe.
- Your credit report shows medical debt collection notices that you don't recognize.
- You receive a notice from a health insurance company that you've reached your benefits limit.

Consumers looking for a self-help plan to recover from identity theft can visit www.IdentityTheft.gov.

Surprise billing

Recent federal and state laws protect consumers with private health insurance from receiving and paying medical bills at amounts higher than the in-network insurance amount for emergency or other unanticipated out-of-network care. Potential scenarios include receiving emergency care at an out-of-network facility and receiving some services, such as imaging, from an out-of-network provider during scheduled care with an in-network provider. In circumstances such as this, providers are generally not allowed to "balance bill" the patient and must work out any payment differences with the insurance company. Patients may still receive a bill because, under the laws, they remain responsible for any amounts (as copays and deductibles, for example) that meet the in-network limits.

Based on these laws, patients with health insurance should not receive surprise bills for unanticipated out-of-network care for services performed in or after 2022.

Consumers receiving a surprise bill that they believe violates these laws can first try to resolve the issue directly with their insurance and care provider. Unresolved disputes can be reported to the Ohio Department of Insurance at consumer.complaint@insurance.ohio.gov or by calling 800-686-1526. For more information about surprise billing, click here to access the Department of Insurance's surprise billing toolkit.

Retail scams: What every consumer should know

As online shopping grows in popularity, retail scams continue to rise, making it more crucial than ever for consumers to understand how scammers operate. Fraudulent retailers use sophisticated psychological tricks, fake websites, and misleading marketing practices to appear legitimate. By recognizing the warning signs, shoppers can protect their money, their personal information, and their peace of mind.

- **Too-good-to-be-true discounts:** Scam websites often lure victims with extremely low prices or unrealistic promotions. These offers are usually paired with high-pressure tactics, such as countdown timers, aggressive pop-ups, or claims that "only a few items remain." Although legitimate retailers may run limited-time sales, they rarely flood every page of their website with urgent messaging. If the price feels impossible to believe, trust your instincts and proceed with caution.
- **Sloppy website content:** Poor grammar, awkward wording, or repetitive product descriptions are red flags. Many scam sites rely on low-quality or AI-generated text, making their pages feel generic or inconsistent. Fake reviews are common, too, often appearing copied, overly positive, or identical across different products. A professional, established retailer maintains clear, organized, and well-written content across its site.
- **Suspicious payment methods:** Fraudulent sellers frequently request untraceable forms of payment, such as gift cards, wire transfers, cryptocurrency, or payment links sent through text or social media. These methods are designed to prevent chargebacks or refunds when the scam works. Authentic retailers typically support secure, traceable payment options such as credit cards or recognized digital platforms.
- **URL and domain warning signs:** One of the best ways to spot a scam is to analyze the website address. Fake retailers often mimic legitimate companies by changing a letter, adding an extra word, or using a strange domain suffix. Look for HTTPS encryption and check whether the domain matches the brand name exactly. Many scams operate on newly created websites that disappear after a short period.
- **Fake trust badges and missing contact info:** Scam websites frequently display counterfeit "secure checkout" icons or copied privacy policy language. They may lack real customer service channels, physical business addresses, or functional phone numbers. A genuine retailer provides clear, verifiable ways for customers to get support.
- **Counterfeit products and misrepresentation:** Not all retail scams involve undelivered orders. Some send low-quality or counterfeit products instead of the items advertised. These sellers typically offer no valid return policy, with the return instructions leading nowhere. If a website's product photos appear inconsistent — or too polished, compared with its overall design — this may be a sign that it isn't legitimate.
- **Modern digital scams:** Emerging threats such as QR-code scams, phishing pages, and deepfake messages add another layer of risk. Even communications that seem to come from a friend, family member, or familiar brand should be verified through a reliable channel. Do not send money or click a link before obtaining that verification.

How to tell a scam site from a real one:

- Verify the URL and look for secure HTTPS browsing.
- Review the retailer's contact information and return policies.
- Search for independent reviews outside the site.
- Use only secure, traceable payment methods.
- Look for consistency in branding, product descriptions, and customer service practices.

If you suspect a scam or an unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

OHIO SALES TAX HOLIDAY - GOOD NEWS TO KNOW

This year, the Ohio sales-tax holiday will span a weekend (three days) – from **Friday Aug. 7 through Sunday Aug. 9.** The event permits tax-free online and in-person purchases on all eligible back-to-school items.

When shopping, make sure that you are aware of the items eligible for the exemption this year:

- Clothing priced at $75 or less per item.
- School supplies priced at $20 or less per item.
- School instructional materials priced at $20 or less per item.

Also, practice sound shopping habits, such as keeping receipts and knowing the return policies of the stores where you shop.

The Ohio Department of Taxation provides detailed information about this year's sales-tax holiday. Before shopping, consider the types of purchases you plan to make and review the department's website.