



Companies Continue to Share Health Data Despite New Privacy Laws

CONSUMER REPORTS - MAGGIE OATES, MATT SCHWARTZ, JUSTIN BROOKMAN

BOLTIVE - CHRISTINE DESROSIERS, PAUL MAJOR

JANUARY 16, 2024



Table of Contents

[Summary](#)

[Introduction](#)

- [1. Loopholes abound in health data privacy](#)
- [2. Privacy is a public health issue](#)
- [3. States are making progress on loopholes](#)
- [4. Regulators are cracking down](#)
- [5. Under the hood of data sharing](#)
- [6. A long road ahead](#)

[Methods: How we spotted sharing of sensitive data](#)

- [1. Consumer personas developed](#)
 - [2. Personas visited target health sites and indicated interest](#)
 - [3. Personas browsed the web](#)
 - [4. Determined whether target sites respected privacy choices](#)
- [Categorizing tags and cookies](#)
- [Limitations to our method](#)

[Findings: Sharing is prevalent, laws are confusing](#)

- [Sharing seems to be the default](#)
- [Some opt-out and opt-in controls missing](#)
- [Some opt-out controls weren't fully useful](#)
- [It's unclear when laws even apply](#)
- [CASE 1, Dupixent: a medication info site](#)
- [CASE 2, TakeCareOf: personalized vitamins](#)
- [CASE 3, Evolve: treatment for teens](#)

[Discussion and Recommendations](#)

- [New laws do not seem to be effective at constraining data sharing](#)
- [Recommendations for policymakers](#)
- [Narrow the loopholes](#)
 - [Make data minimization the default, limit notice and choice](#)
 - [Beef up enforcement](#)
 - [Educate businesses](#)
- [Recommendations for businesses](#)

[Appendix A: Research Methods](#)

[Appendix B: Findings](#)

[Appendix C: Relevant Regulations](#)

Summary

Consumers seeking information about or treatment for their health needs deserve to have their data treated with respect. In the wake of mounting evidence that many health and wellness companies collect and share consumer data with a concerning long list of third parties, including social media companies, Consumer Reports and Boltive partnered to examine the data practices of ten health-related sites, focused on the use of that data for advertising. We created a variety of U.S.-based consumer persona bots who visited sites in spring 2023 looking for help with addiction treatment, sexual issues, disability aids, and other health needs. We collected and examined site cookies, advertising content, metadata, and privacy policies for evidence of collection and sharing to answer the central research questions: **Are health websites sharing personal or sensitive data? Do consumers have the ability to control this sharing?**

Nine of the 10 sites we examined raised at least one privacy concern. All collected health-related data, and some collected data that might be considered sensitive under various state laws. We found that because of varying applicability thresholds, vague definitions, and broadly defined carve-out exceptions, it is often unclear which laws apply to which businesses and data. Some of the sites that offered on-site cookie and sharing controls seemed to have technical issues that prevented our testers from limiting interest-based advertising cookies. Two sites that claimed they do not sell or share covered data appeared to allow third-party marketing cookies, which might legally constitute a sale. On the whole, it seemed that despite new health privacy protections in state laws, many health-related sites we examined shared data with third parties, often without easy-to-use controls. We end with recommendations for regulators and businesses on closing loopholes and prioritizing data minimization.

Introduction

1. Loopholes abound in health data privacy

Most consumers know the Health Insurance Portability and Accountability Act, or HIPAA, as the law that protects our health data. However, they generally do not know that HIPAA covers only a narrow range of health data, mostly consisting of data relevant to clinical settings and insurance. The cycle data in a menstrual cycle tracking app? The heart rate log collected by your fitness watch? They are often not “protected health information” in the United States. In a 2023 study headed by University of Pennsylvania researchers, 82 percent of consumers did not realize that HIPAA does not apply to many types of health-related data in mobile apps.¹

¹Turow et al., “Americans Can’t Consent To Companies’ Use Of Their Data,” Annenberg School for Communication, 2023, https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

One reason for that loophole is that HIPAA focuses on the type of business or institution generating or collecting the data—including healthcare providers, insurance companies, universities—rather than merely on the substance of the data itself. The health-relevant data collected by those specific institutions is often formally known as “health data” or “protected health information.” Meanwhile, many other types of business that collect wellness data are exempt from HIPAA even though a typical consumer might reasonably consider the data that they collect to be health data.² In this report, we use McGraw and Mandl’s term “health-relevant data” to refer to a more expansive definition that better aligns with consumer expectations of what health data includes (see [Figure 1](#)).

Figure 1: What is health-relevant data?

Figure by McGraw and Mandl 2021.³

Box 2 Major categories of health-relevant data with examples

1. **Category 1. Health Care System Generated.** Electronic medical record data, prescriptions, laboratory data—including molecular “omics” data, pathology images, radiography, payor claims data.
2. **Category 2. Consumer Health and Wellness Industry Generated.** Wearable fitness tracking devices, medical wearables such as insulin pumps and pacemakers, medical or health monitoring apps, patient-reported outcome surveys, direct-to-consumer tests (including DNA analysis) and treatments.
3. **Category 3. Digital Exhaust Generated as a Byproduct of Consumers’ Daily Activities.** Social media posts, Internet search histories, location and proximity data.
4. **Category 4. Non Health Demographic, Social, and Economic Sources.** Race, gender, income, credit history, employment status, education, level, residential zip code, housing status, census records, bankruptcy and other financial records, grocery store purchases, fitness club memberships, voter registration.

2. Privacy is a public health issue

This discrepancy between the legal definition of “health data” and the broad consumer understanding of the term isn’t an innocuous misunderstanding; the stakes are high. In an environment where millions of consumers use health websites and apps to help take care of themselves and their loved ones, data privacy is a major public health issue. There is reason to believe that many consumers will not seek necessary treatment if they can’t be confident that their health data will be kept private. A 2015 systematic review found that the social stigma associated with some health conditions is among the top reasons consumers delay or avoid

² Theodos and Sittig, “Health Information Privacy Laws in the Digital Age: HIPAA Doesn’t Apply,” *Perspectives in Health Information Management*, no.18 (Winter 2021).

³ *ibid.*

getting help for mental health problems. Among stigma-related barriers, disclosure and confidentiality concerns seemed to be the most prominent type of stigma barrier, the review found.⁴ In addition, recent legislative and judicial developments concerning reproductive healthcare extend the potential effect of exposing healthcare data to legal jeopardy, further jeopardizing the safety and autonomy of individuals.

Data privacy is also a national security issue: In 2022, the U.S. National Counterintelligence and Security Center issued a specific warning about the security implications of sharing consumer health data in a manner that might enable “foreign exploitation.”

3. States are making progress on loopholes

Many U.S. states and agencies already recognize these issues. Since the passing of the 2018 California Consumer Privacy Act, state legislatures have slowly worked to increase protection of consumer data. Several states have comprehensive privacy laws on the books that include special protections for health data or categories of so-called “sensitive data,” which often include certain health-relevant information.

- Under the Virginia Consumer Data Protection Act (VCDPA), companies must receive consumer permission before processing sensitive data, which includes a “mental or physical health diagnosis.”⁵
- As of July 2023, residents of Connecticut⁶ and Colorado⁷ are also protected from the collection, use, sharing, and sale of sensitive data, including information concerning a “mental or physical health condition or diagnosis” and “sex life.”
- At the end of 2023, Utah will give consumers the right to opt out before a company processes data including “medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.”
- In 2024, Nevadans will have protections for data used “to identify the past, present or future health status” of a consumer, including inferences made that a consumer has any “health condition or status, disease or diagnosis.”⁸
- In the 2023 legislative session, Delaware, Indiana, Iowa, Montana, Oregon, Tennessee, and Texas passed comprehensive privacy laws that include special protections for sensitive data, including certain health-relevant information.⁹

⁴ Clement et al., “What is the impact of mental health-related stigma on help-seeking? A systematic review of quantitative and qualitative studies,” *Psychological Medicine*, no. 45.1 (2015), <https://pubmed.ncbi.nlm.nih.gov/24569086/>.

⁵ Consumer Data Protection Act, Chapter 53, Code of Virginia § 59.1-575, 2023, <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>. (See [Appendix C1](#) for excerpts.)

⁶ “The Connecticut Data Privacy Act,” Connecticut Office of the Attorney General, accessed April 5, 2023, <https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act>.

⁷ “Colorado Privacy Act (CPA) Rulemaking,” Colorado Attorney General, accessed April 5, 2023, <https://coag.gov/resources/colorado-privacy-act/>.

⁸ S.B. 370, 82nd Congress, Nevada, 2023, https://www.leg.state.nv.us/Session/82nd2023/Bills/SB/SB370_EN.pdf

⁹ Andrew Folks, “US State Privacy Legislation Tracker,” International Association of Privacy Professionals, 2023, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

- California has perhaps the most complex laws currently in place regarding health data. Californians may tell businesses to limit the processing and sharing of sensitive data, a broader category that includes information “concerning a consumer’s health” or “sex life.”¹⁰ The California Attorney General’s office has made clear that the California Confidentiality of Medical Information Act (CMIA) goes beyond HIPAA to explicitly include nonclinical mobile apps and wearables that collect medical information.¹¹ California regulations also require companies to provide consumers additional notice and choice for sensitive data that is used for special purposes, including re-targeted advertising, making inferences about consumers, or other purposes that seem unexpected to an average consumer.¹²
- Although Washington State does not have a comprehensive privacy law, a relevant section of its My Health My Data Act went into effect in July 2023.¹³ That law’s definition of health data is the broadest yet, going beyond health conditions and diagnoses to include future health, reproductive and sexual information, symptoms, and location or other data that identifies a consumer seeking healthcare services. In addition, data unrelated to health might be considered health data if it is used to infer health-related information. Washingtonians will have the right to opt in to collection and sharing of health data, the right to withdraw their consent, and a private right of action.

4. Regulators are cracking down

We applaud state and federal agencies that have been putting resources toward the enforcement of existing protections of health-relevant data. Some regulators are also actively looking to expand protections to close gaps in existing health privacy rules.

- In 2017, the Massachusetts Attorney General reached a settlement with Copley Advertising, a marketing company that used and shared location data to track patients in several states who entered reproductive health facilities. The AG claimed that geofenced marketing around medical facilities is an “unfair or deceptive” practice under Massachusetts consumer protection law.¹⁴

¹⁰ “California Consumer Privacy Act (CCPA),” California Office of the Attorney General, accessed April 5, 2023, <https://oag.ca.gov/privacy/ccpa>. (See Appendix C2 for CCPA excerpts.)

¹¹ “Attorney General Bonta Emphasizes Health Apps’ Legal Obligation to Protect Reproductive Health Information,” California Office of the Attorney General, May 2022,

<https://oag.ca.gov/news/press-releases/attorney-general-bonta-emphasizes-health-apps-legal-obligation-protect>.

¹² Stauss and Summers, “How do the CPRA, CPA & VCDPA treat sensitive personal information?” *ByteBack Law*, Feb 2022,

<https://www.bytebacklaw.com/2022/02/how-do-the-cpra-cpa-and-vcdpa-treat-sensitive-personal-information/>.

¹³ My Health My Data Act, HB 1155, Washington State House, 2023,

<https://app.leg.wa.gov/billsummary?BillNumber=1155&Year=2023>.

¹⁴ “Massachusetts AG Settles Geofencing Case with Copley Advertising,” *Practical Law Commercial Transactions*, Thomson Reuters, May 2017,

<https://content.next.westlaw.com/practical-law/dhttps://content.next.westlaw.com/practical-law/document/I4c6e0102301611e798dc8b09b4f043e0/Massachusetts-AG-Settles-Geofencing-Case-with-Copley-Advertising>.

- In California, the Attorney General settled a 2020 case with the fertility and menstrual cycle tracking app Glow for creating a feature that allowed users to share their health data without sufficient security protections.¹⁵
- These above two enforcement cases are particularly salient in the wake of the 2022 Supreme Court decision in *Dobbs v. Jackson Women's Health Organization*, which rolled back some federal protections for abortion. Advocates have growing concerns about the use of surveillance to target people seeking reproductive health care.¹⁶
- In an effort to plug holes in HIPAA protections, the Federal Trade Commission (FTC) argued in 2021 that the provisions of the Health Breach Notification Rule (HBNR)¹⁷ apply not only to cyber security breaches and hacks, but also to unauthorized sharing of sensitive data by health-relevant apps.¹⁸ In early 2023, the FTC brought an enforcement action against GoodRx, a prescription drug discount company that allegedly used third-party trackers on its site and supplemented tracking data with user location and the names of specific drugs.¹⁹ The fertility tracking app Premom settled with the FTC in May 2023 after allegedly disclosing sensitive, identifiable health data via third-party programming tools (also called SDKs) such as those from AppsFlyer and Google.²⁰ The FTC continues to refine the HBNR in an attempt to better protect consumers from the sharing of health-related data. In May 2023, the agency announced a new proposed draft of the rule, clarifying that it can cover websites, apps, or devices that provide “health care services or supplies.”²¹
- In March 2023, the FTC issued a consent order against BetterHelp, alleging that the online counseling service was using unfair and deceptive practices in sharing user data with social media companies despite promising users otherwise. The agency clarified in the order that the mere fact that a user has sought therapy should be considered “highly sensitive, and may cause harm if disclosed to third parties alongside identifying data.”²²

¹⁵ “Attorney General Becerra Announces Landmark Settlement Against Glow, Inc.: Fertility App Risked Exposing Millions of Women’s Personal and Medical Information,” California Office of the Attorney General, September 2020, <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-inc-%E2%80%93>

¹⁶ Anya Prince, “Reproductive Health Surveillance,” *Boston College Law Review* (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4176557.

¹⁷ FTC, “Health Breach Notification Rule; Final Rule,” Federal Register, 16 C.F.R. Part 318, <https://www.ftc.gov/legal-library/browse/federal-register-notices/health-breach-notification-rule-final-rule>.

¹⁸ “FTC Warns Health Apps and Connected Device Companies to Comply with Health Breach Notification Rule,” Federal Trade Commission, September 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule>

¹⁹ “FTC Enforcement Action to Bar GoodRx from Sharing Consumers’ Sensitive Health Info for Advertising,” Federal Trade Commission, February 2023. <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>

²⁰ “Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order,” Federal Trade Commission, May 2023. <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

²¹ FTC, “Health Breach Notification Rule,” Code of Federal Regulations, 16 CFR Part 318, <https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule>.

²² FTC, “BetterHelp Agreement Containing Consent Order,” No. 2023169, p. 16, March 2023. <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter>.

In contrast to many definitions of “sensitive” in privacy legislation mentioned above, this argumentation did not need to include specific medical conditions or symptoms.

- In July 2023, the FTC and the Health and Human Services’ Office for Civil Rights released a joint letter regarding the use of online tracking technologies. The letter specifically advises health-relevant businesses to use caution when integrating tracking tech such as Meta/Facebook pixels and Google Analytics, regardless of whether a business is covered by HIPAA.²³

5. Under the hood of data sharing

Most of the aforementioned enforcement cases focus on sensitive data shared for the purpose of advertising. Contemporary web and app marketing infrastructure is a surveillance network of pixels, cookies, click tracking, tags, social share buttons, and other metadata that’s largely invisible to website and app users.

When a consumer visits a website, the code that makes the site work is downloaded by the consumer's browser. This body of code often includes scripts and tags that activate third parties to deliver business services such as chatbots, anti-fraud protections, and advertising. Once a third-party vendor's technology is active on a consumer’s browser, it sends information back to its own servers, which the vendor then uses to provide services for the site.

Depending on the vendor, information can be sent back and forth between the site and the vendor's servers or it can be written to “cookies,” small text files that are saved locally on the consumer's browser. As a consumer continues browsing the web, the same third-party vendors may provide services to the other sites the consumer visits. These services will check for their existing cookies, allowing these businesses to track a consumer across multiple sites.²⁴

Many vendors also allow subcontractors—fourth parties, in effect—to load on the page and collect information. While some third- and fourth-party data sharing is used for legitimate business purposes, it also poses privacy issues by allowing for the sharing of personal data without the consumer’s knowledge. In some cases, for example, sites, vendors, and their subcontractors sell data behind the scenes to companies that were not active on the page at all, such as data brokers.

This behind-the-scenes ecosystem is so complex that not all businesses that allow third- and fourth-party data sharing are doing so knowingly. Regardless of intent, however, businesses have an obligation to monitor what data is being collected and shared on their site, and to communicate accurately with their visitors.

²³FTC and U.S. Department of Health and Human Services Office for Civil Rights, “Re: Use of Online Tracking Technologies,” July 2023,

https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

²⁴Christine Desrosiers, “Whitepaper: Digital Advertising Unboxed,” Boltive, Oct 2022,.

<https://www.boltive.com/articles/whitepaper-digital-advertising-unboxed>.

6. A long road ahead

Many regulators are working to encourage data protection using only limited enforcement tools. While a promising start, the protections for health-relevant data provided by states apply to only a fraction of the U.S. population and to only a fraction of health-relevant data. And even in the states that do protect health-relevant data, protections and rules vary greatly depending on how expansively “sensitive” and “health data” are defined.

Meanwhile, despite the precedents in federal and state enforcement actions, health apps and websites continue to share sensitive information about their users. Online mental health provider Cerebral, for example, admitted in March 2023 to using third-party trackers and inadvertently sharing data on millions of users.²⁵ In 2022, the FTC filed a lawsuit against location data broker Kochava for allegedly selling location data to companies to use for advertising. The data may be used to reveal patient visits to health clinics, worship sites, and addiction recovery facilities.²⁶ The case was ongoing as of this writing, with an amended complaint publicly released in November 2023²⁷ after an initial court dismissal,²⁸ which we interpret as an illustration of the difficulties enforcement agencies face on privacy actions.

FTC Chair Lina Khan asserted that while the existing Health Breach Notification Rule “imposes some measure of accountability on tech firms that abuse our personal information, a more fundamental problem is the commodification of sensitive health information, where companies can use this data to feed behavioral ads or power user analytics.”²⁹

In agreement with Chairwoman Khan, our work offers empirical evidence to demonstrate the continued need for enforcement cases and legislative changes to protect the sensitive data of everyday people.

²⁵ Gliadkovskaya, “Cerebral shared private health data on 3.1M users for years with advertisers, social media platforms,” *Fierce Healthcare*, March 2023,

<https://www.fiercehealthcare.com/digital-health/cerebral-hipaa-violation-shared-data-millions-users-tech-giants>

²⁶ FTC, “FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations,” August 2022,

<https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other>.

²⁷ FTC, “FTC vs Kochava, Inc.,” November 2023,

<https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc.>; Singer, “Judge Dismisses F.T.C.

Lawsuit Against a Location Data Broker,” *New York Times*, May 5, 2023,

<https://www.nytimes.com/2023/05/05/business/ftc-kochava-location-data.html>

²⁸ U.S. District Court for the District of Ohio, “Memorandum Decision and Order,” FTC v. Kochava Inc., May, 4, 2023, Case No. 2:22-cv-00377-BLW,

<https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/court-dismissal-ftc-suit-against-kochava-5-4-23.pdf>. For an overview of motions, see “FTC v. Kochava, Inc. (2:22-cv-00377),”

CourtListener, <https://www.courtlistener.com/docket/64930092/federal-trade-commission-v-kochava-inc>.

²⁹ FTC, “FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule,” Sept 2021,

<https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health-breach-notification-rule>

Methods: How we spotted sharing of sensitive data

Below, we describe the four-step process we used to collect cookie and advertising information from 10 health-related sites. That process included the use of Privacy Guard, a tool developed by the privacy compliance firm Boltive to help companies audit their websites' collection of visitor data and share data, and honor privacy controls such as opt-out tools.

1. Consumer personas developed

We used Boltive's Privacy Guard tool to create automated web-browsing bots that mimic the online behavior of specific consumer "personas" searching for health-related products, services, and information. For example, one persona was a California Mac user looking for online help with a sexual health issue and doing some general browsing. Another was a privacy-conscious Virginian looking to purchase an accessibility device and have it delivered to their home. We also created a control persona, a California user who browsed generic weather and celebrity news information and no health-relevant sites.

If available, some personas made a privacy choice using a "consent signal." One persona (the "Virginia persona") explicitly consented to data collection, while another (the "Do Not Sell/Share persona") used tools to opt out of data sharing.

Personas all had an IP address located either in California or Virginia. These states were of particular interest because both recently enacted regulations that govern the use and collection of sensitive data. As noted above, Virginia requires that companies receive opt-in consent before processing sensitive data, and California guarantees consumers the right to opt out of the sharing of sensitive data for marketing purposes.

2. Personas visited target health sites and indicated interest

We selected a list of 10 "target sites" that might collect health-relevant data. We aimed to include sites that address a range of health topics (e.g., sexual health, mental health, disability aids) and offer users a range of privacy tools (e.g., consent pop-ups, Do Not Sell links, no apparent tools) and functions (e.g., retail, direct services, informational, referral sites). The sites we chose include ones operated by a large national retailer, a small disability-focused retailer, two international pharmaceutical companies, and a regional mental health services chain.

Health sites often have legitimate reasons to collect some amount of data in response to certain user actions, which we refer to below as "buy signals," such as putting an item in a shopping cart, filling out an interest form, or taking an online quiz. But they sometimes collect or

repurpose user data with the intention of using it to trigger interest-based advertisements (IBA) or as part of a larger marketing funnel.

Whenever possible, our personas performed a buy signal each time they visited a target site. For example, one persona searched Google for “teen depression” in California, clicked a Google Ad link for “Newport Academy,” and then browsed 10 pages related to depression and residential treatment programs. Another persona visited online bookstore Barnes & Noble, browsed books related to an invisible disability,³⁰ and added three to their shopping cart.

Special attention was given to buy signals that collect data that might imply or confirm a specific medical condition—a quiz that asks if the user has anemia, for instance—because, although the definitions of “sensitive data” vary by statute, almost all include specific medical conditions.

[Table 0](#) summarizes the names and attributes of the personas. See [Appendix A1](#) for a list of specific target sites, buy signals, and consent mechanisms.

3. Personas browsed the web

After visiting a target site, all personas visited a series of general-interest sites (e.g., weather, celebrity news). The purpose was to determine whether the user would receive a targeted ad based on data shared on the health-relevant website.

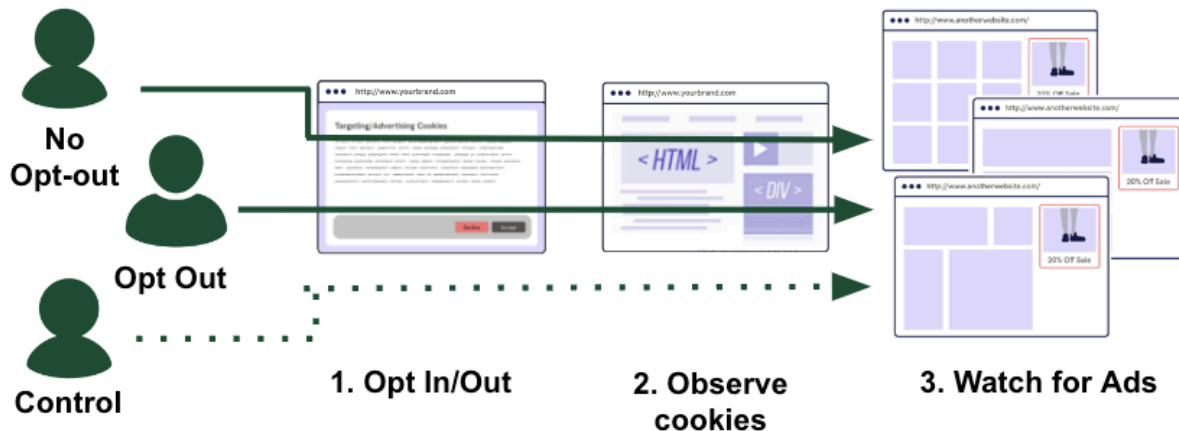
In general, here is the web browsing path taken by each persona:

- A. Persona is assigned a condition (e.g., a location, a privacy choice, see [Table 0](#))
- B. Persona browses the web in a general manner
- C. Persona visits a target health-relevant site
- D. Persona makes a privacy choice (consent signal: e.g., opts in to data collection, opts out of data sharing, or makes no choice) and checks whether that choice is respected
- E. Persona shows interest in products/services with a buy signal (e.g. shopping cart, quiz)
- F. Persona visits 10 general-interest websites and checks for advertisements from the target site in step C
- G. Persona repeats step F every two hours for two weeks

Note that not all these steps are relevant to all personas. For example, the control persona skips steps C-E. Some personas skip step D if their target site does not seem to provide any privacy choices.

³⁰ “Not all disabilities are apparent from the outside. These physical, mental, or neurological conditions—known as invisible, or non-apparent, disabilities—can limit or challenge a person’s movements, senses, or activities...” from Brenda Álvarez, “What to Know About Invisible Disabilities,” *National Education Association*, August 2021, <https://www.nea.org/nea-today/all-news-articles/what-know-about-invisible-disabilities>.

Figure 2: Personas browse the web, take a privacy action, and observe changes



4. Determined whether target sites respected user privacy choices

When a company makes a promise in a privacy notice or offers users a privacy choice, it should make good on those commitments. For each target site, we collected three observations (details in [Appendix A2](#)) to determine whether a site’s stated data practices align with its actual behaviors: the presence of data sharing, re-targeted advertisements, and consent mechanisms.

Changes in data sharing. When a persona opts out of sharing, opts out of targeted ads, opts out of third-party cookies, or withholds consent regarding cookies, we generally expect that action to trigger changes in cookies and tags. Depending on the specifics of the mechanism, third-party cookies should drop or metadata tags might change. If no changes occur, it could be a sign that the site’s opt-out mechanism is malfunctioning or is improperly configured; alternatively, it could mean that data wasn’t being shared for a purpose covered under an opt-out or that the site may have behind-the-scenes instructions to third parties instructing them to limit how the shared data is used. In other words, no changes in cookies doesn’t necessarily mean an error was made, because some cookies might be related to site functionality or legally acceptable use-cases (e.g., analytics). More details are available in [“Categorizing tags and cookies.”](#)

Presence of re-targeted advertisements. In step F above, we visited general-interest, non-health-relevant sites and kept a record of all the advertisements served. The presence of creative, partner, and other relevant ad data was examined for connection to the target site. The presence of a specific targeted advertisement usually indicates that data is being shared between ad tech companies.

If the persona opted in to processing and sharing of sensitive data, we would not be surprised to find that the company delivered interest-based ads. If a persona opted out, on the other hand, we would generally expect the persona to receive *no* interest-based advertising from that site.

Of course, a persona may have been served a health-relevant ad by chance, rather than as a result of online tracking. We used the control persona to control for that possibility.

Consent or transparency required at collection. In addition to the automated data collection from personas, we manually examined the privacy choices, privacy notices, and consent mechanisms of the target sites. We investigated the buy signal and collection practices of each target site to determine whether the data collected might be considered health data or sensitive data under California and Virginia law. For more on the specifics of these laws, see [Appendix C](#).

Table 0: Summary of persona conditions				
	No Opt-Out Persona	Virginia Persona	Do Not Sell/Share Persona	Control
IP Location	California	Virginia	California	California
Device Type	Desktop Mac	Desktop Mac	Desktop Mac	Desktop Mac
Browser	Chrome	Chrome	Chrome	Chrome
Consent Signal	Go to target site. Interact with consent tech to opt in if offered, or take no action	Go to target site. Accept Opt In to process sensitive data if offered. Interact with consent tech if offered, or take no action ³¹	Go to target site. Interact with consent tech to opt out of sales, if offered	Do not go to target site. Perform no consent actions
Buy Signal	Perform health-relevant actions to get into marketing funnel	Perform health-relevant actions to get into marketing funnel	Perform health-relevant actions to get into marketing funnel	Do not go to target site

³¹ We intended to investigate the impacts in Virginia of opting in to sensitive data processing vs declining to opt in. However, so few sites offered a meaningful opt-in that we decided not to attempt that analysis.

Categorizing tags and cookies

Part of our analysis involved assessing the underlying purpose of any cookies and tags we found on sites. Here are some of the considerations we used to categorize the purpose of cookies.

Based on regulatory guidance and enforcement actions, including the California Attorney General's 2022 complaint against Sephora,³² we generally presumed that the appearance of interest-based advertising activities on a website inherently carry a risk of consumer data being collected, used, and/or shared inappropriately. Boltive relies on domain expertise, public documentation, and research on historical practices to determine whether vendors on a site are engaging in collection and sharing related to interest-based advertising. When those vendors' cookies and tags are not removed or suppressed after opt-out—or when opt-out mechanisms are not provided—we categorize those cookies and tags as risky.

For example, Meta offers cross-site consumer tracking services, including first- and third-party cookies, that many companies use to target advertising on the Facebook social media platform. These cookie and pixel tools can also be used for analytics services and performance analysis.³³ Businesses that use these Meta services have the ability to adjust whether cookies are present, which cookies are placed, and how much information is added in a given cookie and shared with Facebook.³⁴ Previous research alleges that those Meta pixel tools have been used to share sensitive information from hospital websites.³⁵ We don't know what settings businesses are selecting under the hood, so we take a conservative approach and categorize most Facebook cookies as risky because of the popular cross-site advertising dimension of the service. As we discuss in our [Limitations](#), site inspection doesn't let us know for sure what happens behind the scenes; we don't know the actual activities the target site is engaging a vendor to perform or whether they have appropriate data protection agreements in place with the vendor. For example, a company could engage a digital ad vendor who offers a range of services that include interest-based advertising, and choose to only use the vendor's non-interest-based advertising services. It is not possible for us to detect that in the site code.

³² "Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act," California Office of the Attorney General, August 2022, <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>

³³ "Facebook Cookies Policy," Facebook, accessed September 28, 2023, <https://www.facebook.com/privacy/policies/cookies>

³⁴ "About Cookie Settings for the Meta Pixel," Business Help Center, Meta, accessed December 13, 2023, <https://www.facebook.com/business/help/471978536642445?id=1205376682832142>.

³⁵ Feathers et al., "Facebook Is Receiving Sensitive Medical Information from Hospital Websites," *The Markup*, June 16, 2022, <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

Limitations to our method

Sites are black boxes. One significant limitation of our analysis is limited visibility into the data collection and processing practices of specific companies. We were able to collect enough data to make good-faith judgments on the extent to which websites were collecting sensitive data. But we generally did not have enough to determine whether or how that data was being stored and used.

For example, while large vendors have publicly documented the purposes of some of their cookies, it is not always possible to determine if a given third-party cookie is being used for legitimate analytics or advertising. As a result, we may be overestimating the rate of unexpected third-party sharing when cookies are actually being used for expected business purposes. On the other hand, we may be underestimating the rates of third-party sharing, because we have little information about undetectable server-to-server sharing or offline sharing/sale to data brokers.

We don't always know which state laws apply. Most state-level consumer privacy legislation kicks in when a company collects data from a certain number of consumers who reside in a given state. For example, the Virginia Consumer Data Protection Act covers only businesses that have processed personal data of at least 100,000 Virginians or that hold personal data on at least 25,000 Virginians and make substantial annual profit from personal data sales. In California, businesses are covered if they generate large revenues, buy, sell, or share information on 100,000 Californians annually, or generate at least half their revenue from selling personal information.³⁶ As a result, it is possible that some of the businesses we discuss in this report are not covered by all state privacy laws. Additionally, during the data analysis of this report, enforcement of California privacy regulations was paused by a June 2023 court decision.³⁷ If sites we analyzed were not fully complying with California regulations, they might not be held responsible.

Limits on personal information. Out of respect for companies and their employees, we refrained from interacting with sites in a way that would put a burden on company resources. For example, we did not fill out intake forms for treatment facilities, as that likely would trigger a phone call or human intervention. This practice limited our ability to exhaustively explore what data might be collected while using a site.

We simulated our location. Most privacy laws allow companies to geofence information and content (for example, to show California rights information only to Californians). Sites often practice this based on the perceived location of the user's IP address. IP location tracking is usually a probabilistic inference; our use of proxy IPs can occasionally have failures, so it's possible we missed geofenced information.

³⁶ See [Appendix C](#) for specifics on California and Virginia thresholds.

³⁷ Robert Yang, "California Superior Court Put the Brakes on Enforcement of California Privacy Rights Act," *National Law Review*, July 7, 2023, <https://www.natlawreview.com/article/california-superior-court-put-brakes-enforcement-california-privacy-rights-act>

Not a representative survey. Our target sites were not randomly selected. With this preliminary report, we aimed to illustrate the problem rather than make claims about the state of the entire wellness industry.

In an effort to mitigate some of these limitations related to technical and legal transparency, we reached out to all 10 companies to ask for comments (see [Appendix A3](#)).

Findings: Sharing is prevalent, laws are confusing

The 10 sites we examined all collected sensitive health information and had the possibility of sharing data with a number of third parties. In some cases, they did so even when we tried to exercise rights to limit sharing. Given the nature of the sites we selected, all needed to collect health-relevant information from consumers. However, they were generally not transparent about how that data was being used and offered consumers little control over its use. When controls were offered, they sometimes didn't function effectively. While we don't have full visibility into what happens under the hood of these websites, the pairing of extensive data sharing with ambiguity about the purposes for which sensitive health data is being used gives cause for concern for consumers looking for online health information.

We began this research with the intent to analyze site compliance with new sensitive-data laws. However, we found that ambiguity in the laws and lack of transparency in sites limited the strength of our findings about compliance. Instead, we present some of the challenges privacy law raises and illustrate our findings through three case studies.

Sharing seems to be the default

Despite new legislation meant to give consumers greater control over the collection and sharing of sensitive data, many sites we examined appeared to default to sharing health-relevant data with third parties. Ad-related tags or cookies³⁸ were present on nine of the 10 sites, meaning that most visitors are at risk of having their health-related data used for marketing purposes. The No Opt-Out Persona column of [Table 1](#) shows the number of cookies present on each site that were likely related to interest-based advertising,³⁹ which represents the default experience of a typical California consumer.

Some opt-out and opt-in controls missing

In some cases, visitors were not given controls for managing sharing. Two sites (MaxiAids and Newport Academy) claimed in their privacy policies that they do not sell data, but both appear to allow third parties to place marketing-related cookies on their site, which might legally constitute a sale in California or other states. Neither site provided a Do Not Sell request process ([Appendix B2](#)).

Virginia law requires businesses that process sensitive data to collect consent before processing or sharing. While Virginia's definition of "sensitive" and "consent" are somewhat narrow, there were some sites (LoveWellness, Dupixent) that appeared to collect data that is likely to qualify as a specific health diagnosis. For example, a personalized quiz on LoveWellness inquired about specific vaginal health matters such as bacterial vaginosis, likely a

³⁸ See Methods section, "[Categorizing tags and cookies](#)," for more information.

³⁹ *Ibid.*

medical diagnosis that would be covered by Virginia law. Although answering a recommendation quiz could be interpreted as implicit consent for some processing, no explicit request for additional processing was made, and limited transparency information was offered during the quiz ([Appendix B1](#)).⁴⁰ Overall, only one site in our study ([Case 2](#)) offered a clear Virginia-specific consent collection.

Table 1: Differences in marketing cookies across personas that opted out vs. not

Differences in marketing cookies across personas that opted out vs. not Columns show the count for California personas of cookies that were categorized as relating to interest-based advertising.		
We would generally expect to see a reduction in cookies when going from No Opt-Out to the Opt-Out persona (also called "CA Do Not Sell/Share" persona). Some businesses did not offer an on-site method, or any method, for opting out of cookies. See Appendix A1 for details on opt-outs.		
	No Opt-Out Persona (count of IBA cookies)	Opt-Out Persona (count of IBA cookies)
Dupixent	59	No on-site opt-out provided
Newport Academy	29	No opt-out provided
Viking Man	46	No opt-out provided
LoveWellness	22	18
Everlywell	32	No on-site opt-out provided ⁴¹
Fertility Out Loud	22	No on-site opt-out provided
TakeCareOf	20	8 ⁴²
Evolve	7	7
MaxiAids	6	No opt-out provided
Barnes & Noble	0	0

⁴⁰ It is also possible that some of the sites were not covered by Virginia’s law if they did not collect data from enough Virginia consumers (see [Limitations](#) section).

⁴¹ A representative from Everlywell stated that the site added on-site cookie controls in September 2023, after our analysis.

⁴² In a November 2023 comment, TakeCareOf stated that while these cookies do persist, the site is configured to block data sharing with third parties after opt-out. If implemented correctly, the cookies we categorized as risky do not represent a risk of sharing data for interest-based advertising.

Some opt-out controls weren't fully useful

The Opt-Out persona column of [Table 1](#) illustrates the number of marketing-related cookies set for privacy-motivated consumers who took some steps to opt out of sharing their data. First, in some cases, sites did not clearly offer consumers the ability to opt out of data sharing, even for consumers in California. When it was available, opting out did sometimes reduce the number of marketing-related objects on the page, though not always. It is also possible that the opt-out was effectuated behind the scenes, if the site allowed cookies but blocked sharing or requested limitations through other means. But consumers who opt out, explicitly exercising their legal right to stop sharing, have reason to expect sharing to stop entirely (which would yield a column of zeros in [Table 1](#)). Several sites appear to share data with third parties for marketing, even after visitors instruct them not to.

It's unclear when laws even apply

Even after extensive analysis of state regulations, site privacy notices, and business practices, our team of expert researchers found it difficult to make confident statements about whether sites are in compliance with the various new privacy laws. Because of varying applicability thresholds, vague definitions, and broad carve-outs, it is often unclear which laws apply to which businesses and data. In short, it is virtually impossible for anyone to know when their browsing is protected by their own state laws. Below, we discuss several factors that make it challenging for both experts and consumers to interpret the law.

Businesses may not collect data from enough consumers to be covered by laws. As discussed earlier, most consumer privacy legislation kicks in when a company collects data from a certain number of consumers who reside in a given state. Usually only the business itself knows the internal metrics that determine which state laws apply at any given time. Businesses sometimes hint in their privacy policies about whether they are covered by a given jurisdiction, but researchers and consumers can often only guess about what protections apply.

Virginia's definition of "sensitive" is difficult to interpret. There is not yet regulatory clarity or case law on what counts as sensitive under these new state laws. For example, Virginia's definition of sensitive includes "personal data revealing" "mental or physical health diagnosis" ([Appendix C1](#)). It is unclear how direct or indirect data must be to reveal a diagnosis. If a customer with asthma browses for a book named "Managing Your Asthma," does it reveal a diagnosis? What if that customer doesn't yet have a formal diagnosis by a doctor? Health conditions or symptoms such as pregnancy or others that most of us consider sensitive may or may not be considered a diagnosis under Virginia's privacy law.

California's broad exceptions muddy protections for sensitive data. California privacy law contains a relatively expansive definition of "sensitive," but it carves out substantial exceptions when it comes to providing protections for that sensitive data.

Most of the 10 sites we examined were likely covered by CCPA, as evidenced by the fact that many mention California-specific rights in their privacy notices. Further, most of those sites likely collected sensitive personal information under California’s definition, which includes data “concerning a consumer’s health” or “sex life.” (See [Appendix B1](#)).

However, two provisions in CCPA muddy the protections for sensitive data. One excludes sensitive information that is collected or processed *without* the purpose of “inferring characteristics about a consumer.”⁴³ Researchers and consumers typically have little to no visibility into whether a specific piece of data is being used for making inferences (see [Figure 3](#) for examples). Even when used for marketing purposes, inferences and profiling are activities that usually happen behind the scenes.

A second provision in the CCPA⁴⁴ also carves out exceptions for sensitive data if the data is being used for any number of permitted operational purposes, including security, fraud prevention, internal product development, and short-term, transient, “nonpersonalized” contextual advertising.⁴⁵ In practice, these purposes are again often impossible to parse from the outside, leaving researchers and consumers wondering whether their sensitive information is being appropriately managed.

To help address this lack of transparency, the regulations require that businesses that take advantage of either loophole must state in their privacy policy that they use sensitive data only for permitted purposes, not for profiling.⁴⁶ While examining the privacy policies of the eight sites that did not provide a right to limit the use of sensitive data, we found only vague examples of this type of statement. For example, TakeCareOf’s policy states that they may collect sensitive data and that they “only process such information for purposes authorized by law.”

In summary, it is extremely difficult for external observers to deduce the purposes for which sensitive health-related data is collected or shared, despite new legislation specifically designed to protect this data.

⁴³ CCPA § 1798.121(d).

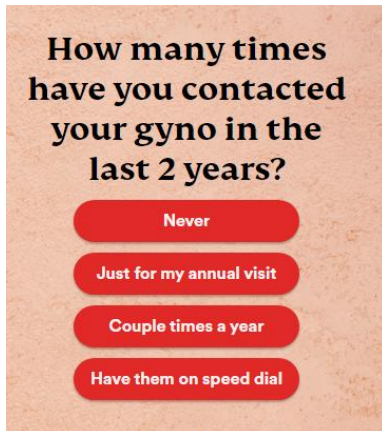
⁴⁴ CCPA § 1798.121(a). See Appendix C2, [Selected Provisions](#).

⁴⁵ CA Code Regs. Title 11 § 7027(m). (March 29, 2023) See Appendix C2, [Selected Regulations](#).

⁴⁶ CA Code Regs. Title 11 § 7027(g). (March 29, 2023) See Appendix C2, [Selected Regulations](#).

Figure 3: Examples of legally sensitive data collected

On the left is a May 2023 screenshot from LoveWellness, illustrating an example of a quiz question that collects data likely considered sensitive in California. On the right is a May 2023 screenshot from Dupixent illustrating an example of a quiz question that collects data likely considered sensitive in states including California and Virginia, as it identifies a specific medical condition and medical history. Neither site mentioned sensitive data rights; we don't know whether this is because data is being used for allowed exceptions, because of an oversight on the company's part, or for some other reason.



CASE 1

Dupixent: a medication info site

[Dupixent.com](https://www.dupixent.com) is a medication information site jointly operated by two pharmaceutical companies, Sanofi and Regeneron. Visitors likely come to the site to learn more about the medication, and can choose a specific condition to treat, including asthma and eczema.

Multiple privacy policies. The only privacy information on the site is a generic footer that links out to two parent company privacy notices:

Sanofi and Regeneron are industry partners, who are committed to handling personal data in ways that respect your privacy. Both companies may independently process your personal data to manage patient support programs and product marketing campaigns. Please refer to Regeneron's Privacy Notice

and Sanofi's Privacy Policy and Cookies Policy for more information regarding processing of your personal data.

Expecting consumers to read even a single privacy notice is somewhat unrealistic, and it's safe to assume almost no consumers follow links to, and read, two separate policies. Even for our team of experts, it was difficult to reconcile the two policies, which could contain contradictory information about data collection and use practices. To make matters worse, because the site is clearly run by pharmaceutical companies, visitors are likely to assume—incorrectly—that any personal data they reveal on the site is covered by HIPAA.

Sensitive data collected without transparency. Our personas visited the site and took a quiz to help generate a personalized guide for discussing asthma treatment with a doctor ([Figure 4](#)). The quiz contains very direct questions about medical conditions (see [Figure 3](#) above). The data collected is likely considered sensitive data in multiple states, including both California and Virginia.

When consumers provide sensitive information to the Dupixent site, they are not provided with contextual information about how that data is going to be used. While we do not know if the collected data is used for profiling or targeted ads, we did detect that the site was sharing data with dozens of companies, including AppNexus, DoubleClick, and Facebook.

The CCPA obligates companies processing sensitive data either to provide consumers the right to limit the use of their sensitive data or to disclose that sensitive data is being used only for permitted purposes. The VCDPA vaguely requires companies to obtain opt-in consent for processing of sensitive data. (We do not know if Dupixent has enough Virginia users to trigger the VCDPA, but the companies likely meet the CCPA threshold, which applies the law to companies with over \$25 million in revenue.) One of Dupixent's privacy policies (by parent company Regeron) states that for sensitive data, the company "will not disclose your personal data to a third party and/or build a profile about you." We found no mention of sensitive data use in the Sanofi privacy policy.

Confusing Do Not Sell mechanisms. If a business sells data or shares data for cross-contextual advertising, California law requires it to provide a Do Not Sell/Share opt-out mechanism. Because Dupixent.com links out to multiple privacy policies, California visitors would need to complete two separate Do Not Sell/Share workflows to be sure their request was received. The opt-out controls were not specific to the Dupixent website. And neither parent company offered any on-site cookie controls.⁴⁷ Regeneron's notice implied that it sells data under California's definition, but offered only generic methods for opting out, such as the Digital Ad Alliance's opt-out tool or disabling third-party cookies via the user's browser. We found Sanofi's privacy notice difficult to interpret; we were unable to find clear information about

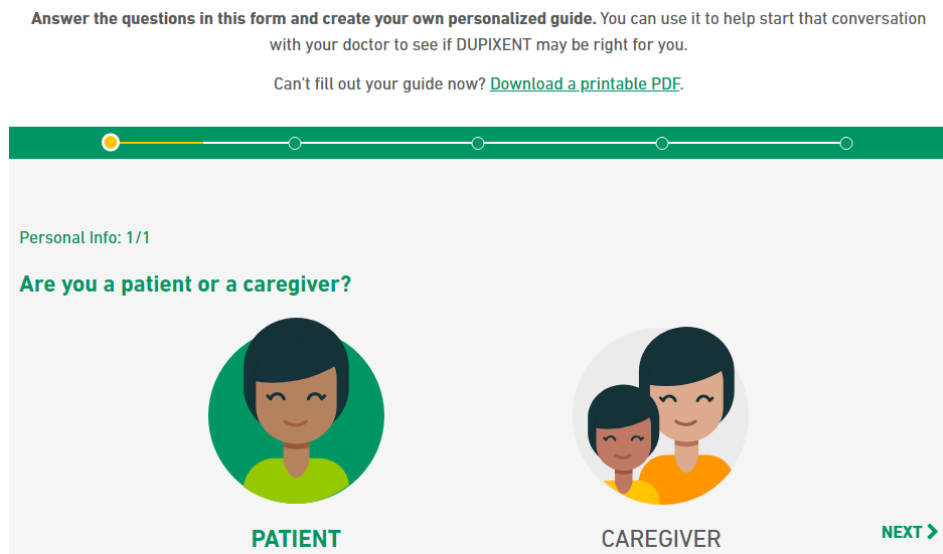
⁴⁷ At some point between our April 2023 data collection and June 2023, Regeneron added a cookie management platform to its site, though it's still unlikely that cookies would be properly managed across domains to apply to the Dupixent site.

whether Sanofi sells or shares data. Sanofi offered no specific Do Not Sell mechanism, and required multiple clicks to reach a generic web form that focused on European Union data rights.

In response to these findings, a spokesperson for Sanofi and Regeneron indicated in November 2023 that they were planning to add “a cookie banner and preference center to provide increased transparency and choice for visitors” on Dupixent.com. “This will give them the ability to manage cookie preferences and change advertising and analytics cookie tracking settings.”

Figure 4: Dupixent quiz for patients

A June 2023 screenshot of Question 1 from a quiz that generates a personalized guide to discussing medication with a doctor.



CASE 2

TakeCareOf: personalized vitamins

Care/of sells personalized vitamins and supplements at [TakeCareOf.com](https://www.TakeCareOf.com). Visitors are encouraged to take an extensive quiz to set up a personalized subscription.

Figure 5: TakeCareOf quiz question examples

Screenshots were taken May 2023.

The figure displays four screenshots of quiz questions from the TakeCareOf website. The first screenshot asks, "Do you use any of the following forms of birth control?" with two options: "Birth control pill (Estrogen, progestin, or both)" and "Other hormonal birth control (Patch, ring, or IUD)". The second screenshot asks, "Are you looking for support with any of the following?" with six radio button options: "Arousal", "Vaginal dryness", "Pain during intercourse", "Orgasm", "Sexual satisfaction", and "None". The third screenshot asks, "Are you interested in being asked questions about your reproductive health?" with a subtext "Including questions about: sexual function, menstrual cycle, and birth control" and two radio button options: "Yes" and "No". The fourth screenshot is titled "PRENATAL" and asks, "Which of these best describes you?" with three options: "I'm looking to become pregnant" (with a pregnancy test icon), "I'm currently pregnant" (with a pregnant woman icon), and "I'm looking for postnatal support" (with a woman icon).

Sensitive data collected without transparent protections. TakeCareOf collects detailed health-relevant data from visitors, including pregnancy status, health concerns, and reports of vaginal dryness and orgasm issues, alongside their names and e-mail addresses (Figure 5). The TakeCareOf privacy policy acknowledges that it shares data, including the possibility of sharing health quiz responses, with third-party marketing partners. Its California-specific policy states that identifying health information is not disclosed, but does not clarify what data is considered health data. In response to our report, a TakeCareOf representative stated that the responses to the quiz our personas took are not shared with any third-party marketing partners.

An unhelpful opt-in. For Virginia personas, TakeCareOf required visitors to consent to sensitive data collection before taking the vitamin quiz, making it the only site we studied that

had a dedicated Virginia-specific opt-in prompt ([Figure 6](#)).⁴⁸ However, the opt-in dialogue required users to acknowledge only that their data would be used “in accordance with our privacy statement,” and referred consumers to review the entire privacy policy for further information.

TakeCareOf’s site was one of only a few that explicitly mentioned the collection of sensitive data in its privacy policy. The quiz also used an effective protection mechanism for minors; if a visitor indicated their age was under 18, TakeCareOf prevented them from continuing the quiz and sharing sensitive data.

Risky cookies are present after opting out. After opting out, our Opt-Out persona saw a reduction in the number of cookies and tags set. However, even after going through the Do Not Sell process and opting out, the site still set eight first-party cookies⁴⁹ related to interest-based marketing, most related to tracking visitors across social media sites such as Facebook, Pinterest, TikTok, and Snapchat. A representative from TakeCareOf stated that while those cookies may persist, the site blocks data sharing to those third parties behind the scenes (however, as discussed below, our Opt-Out persona did see a seemingly re-targeted advertisement even after opting out).

Re-targeted ads found after opting out. After visiting TakeCareOf, our personas went on to browse the web, collecting data about the advertisements that were shown. TakeCareOf was the only site that we were served re-targeted ads about ([Figure 7](#)). Two ads persisted even for the Opt-Out persona. This suggests that TakeCareOf continued to share personal information with third parties after the opt-out, or that the company or its service providers were unable to effectuate the opt-out before the ad was displayed.

Conclusion: While the brand clearly made changes to their site in response to state privacy laws, and made efforts to appropriately disable or block sharing via cookies after opt-out, we still received a re-targeted advertisement about the site, suggesting that a sharing leak may have occurred, or that the opt-out did not effectuate quickly. Privacy controls should function properly and in a timely manner, particularly when there is health-relevant or other sensitive data at stake. This case study illustrates that opt-out rights outlined in state laws may not be well suited to the realities of the digital advertising marketplace. Laws generally allow 30 days for opt-outs to take effect, but short-term re-targeted campaigns may not even persist for that time period, making an opt-out action largely moot.

⁴⁸ We focused our analysis on opt-in prompts our personas encountered. It’s possible other sites had generalized or Virginia-specific sensitive data opt-in prompts elsewhere on their sites.

⁴⁹ Often, privacy advocates are focused on tracking via third-party cookies. However, first-party cookies can also be used for re-targeted advertising. For one explanation, see Polewiak, “What Are First-Party Cookies, and How Can Brands Use Them to Reach Customers?” *RTB House*, April 24, 2024, <https://blog.rtbhouse.com/what-are-first-party-cookies-and-how-can-brands-use-them-to-reach-customers/>.

Figure 6: TakeCareOf opt-in screen

This consent pop-up appeared only for Virginia personas; screenshot collected June 2023.

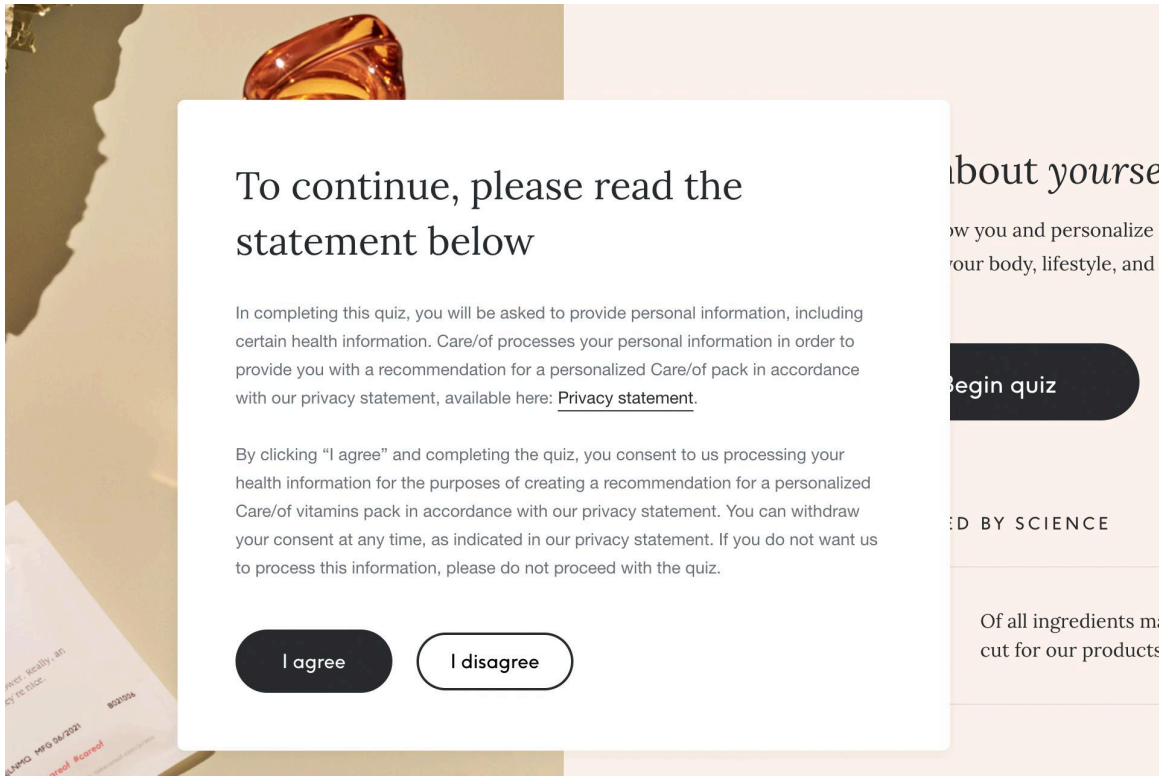
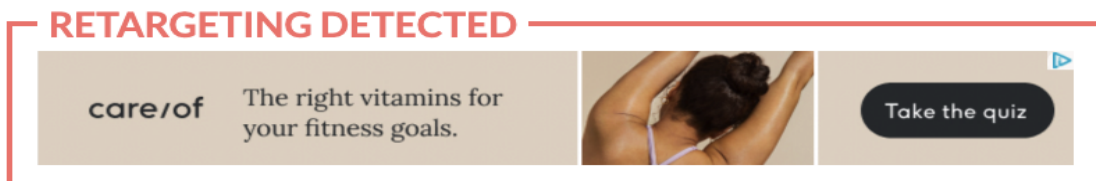


Figure 7: Re-targeted ad found after opting out

After completing an opt-out, the California Do Not Sell/Share persona was still served this ad on a third-party site while casually browsing the web. This ad had dozens of trackers attached to it. Collected April 2023.



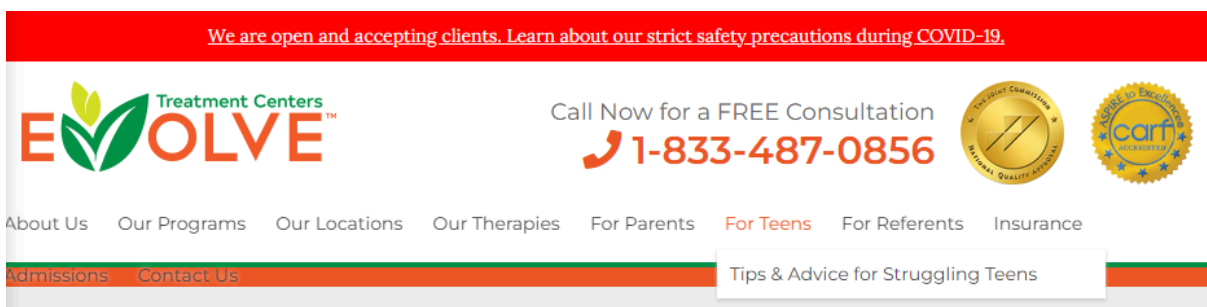
CASE 3

Evolve: treatment for teens

[Evolve Treatment Centers](#) is a chain of “teen mental health treatment and rehab centers” based in California.

Figure 8: The “For Teens” menu on the Evolve site

Screenshot collected May 2023.



Possibility of tracking minors. Our personas did a web search for “teen detox california evolve,” visited Evolve’s site, and then browsed content explicitly aimed at teenagers ([Figure 8](#)). Evolve’s privacy policy indicates that it may share or sell this type of browsing history. Tags and cookies placed on the pages can indirectly collect sensitive information, such as the browsing habits of teenagers interested in drug and mental health treatment. While it is possible that Evolve constrains the use of this data to appropriate or expected uses, teens seeking information in a particularly vulnerable moment might object to having their data shared with others.

Difficult to tell when visitors have HIPAA protections. As a healthcare provider, Evolve collects data that may be considered protected health information (PHI) under HIPAA. While we didn’t focus on this topic for this research, it would be helpful if Evolve (and all sometimes-HIPAA hybrid providers) were more clear about when a site visitor has HIPAA protections versus the more generic protections from the privacy notice. For example, when a visitor uses the live chat to ask about insurance, fills out a general-interest form (see example in [Appendix B4](#)), or fills out a questionnaire on insurance, it is difficult even for experts to tell whether the data is being designated as PHI.

Acknowledgment of state laws. Evolve provides information specific to California and Nevada, and provides instructions for Californians who might want to limit the use of their sensitive data. The privacy policy clearly outlines what types of sensitive data may be shared. Unlike TakeCareOf ([Case 2](#)), Evolve states in its policy that it will voluntarily extend rights to visitors in

states without privacy laws, though at their discretion. The policy does not provide information specific to Virginia, though it is possible that Evolve does not interact with enough Virginians to trigger the VCDPA. We did not receive a reply when we reached out to Evolve for clarification.

Better cookie controls, but some risky cookies persist after opt-out. Evolve has some of the more user-friendly cookie settings we encountered in our research. Unlike many sites, Evolve allows users to easily revisit and change their cookie settings rather than removing the banner after a selection is made. The Do Not Sell/Share and other opt-out options have easy-to-use opt-out buttons. However, as with nearly all the sites we examined, the cookie controls seem to allow the sharing of data even after opt-out. After opting out, 19 tags related to interest-based advertising were fired, all associated with Facebook, DoubleClick, or Google. Because most trackers are black boxes, we can't know whether those tags were used to serve interest-based ads or for some other, permissible purposes.

Conclusion: This site at least attempts to offer usable opt-outs and instructions for how to exercise data rights. But a site focused on the mental health of teens should strive for the strongest privacy protections. And users who opt out still might be surprised that browsing data could be shared with social media platforms and advertisers.

Discussion and Recommendations

We began this project with the intention of understanding the opt-out tools, data sharing, and compliance practices of sites that might collect health-related data. Although we found plenty of questionable behavior by the websites themselves, many of our findings point toward policy gaps in well-intentioned sensitive data provisions in privacy laws.

New laws do not seem to be effective at constraining data sharing

As our findings illustrate, on health-related websites the sharing of data with third parties seems to be the standard practice. While much of the Web is covered with third-party trackers, we hoped that the sites that directly focus on health-relevant data would take a more consumer-protective approach in their marketing practices. We don't have full transparency into the behind-the-scenes data practices of each company, but we're still concerned about the quantity of tags and cookies associated with health sites, especially for consumers who choose to opt out.

New laws focused on sensitive data sharing do not seem to be effective in constraining data sharing or promoting transparency. In some cases, carve-outs may allow sites to continue with the status quo. In other cases, companies may believe these new laws do not apply to their practices. In the few cases where companies offered controls or notices related to sensitive data, they did not necessarily provide clear or usable information. Without any relevant enforcement of these new laws to date, it could also be that businesses have not been incentivized to treat sensitive data with extra care. Regardless of the underlying reasons, our findings suggest that the current state of health-related data leaves consumers in a vulnerable state. Below, we present recommendations that would move regulators and businesses toward a more consumer-friendly environment.

Recommendations for policymakers

Narrow the loopholes

Define “sensitive” to match consumer expectations. “Sensitive” data definitions should better match consumer expectations with regard to information about their health and well-being. For health-related data, Virginia’s definition of “sensitive” covers only data revealing a “mental or physical health diagnosis,” possibly leaving out topics such as symptoms, conditions, sexual history, and weight. We encourage broader definitions, such as those used in California’s comprehensive law and Washington State’s My Health My Data legislation. In order for consumers and researchers to understand what protections are available, businesses should be required to disclose whether sensitive data is collected and how it is used.

If opt-in is required, make it useful. If policymakers want to follow Virginia and use an opt-in model for the processing of sensitive data, consent requirements should be usable and meaningful for consumers. Even though Virginia businesses must obtain opt-in consent before collecting sensitive data ([Appendix C1](#)), they are permitted to make access to the site or service conditional on that consent, reducing the consumer’s effective ability to control their experience within a site. Further, the requirements for consent aren’t entirely clear: Businesses may be able to claim consent based on non-specific blanket requests that consumers may not understand as privacy-related, such as “Do you agree with our policies?” If businesses can simply bundle your consent to collect sensitive information into general terms of service that must be accepted in order to access the site or service in the first place, the new rules offer little protection for consumers.

Cover more than just inferences. California’s right to limit sensitive information is an unnecessarily confusing framework; even our team of experts struggled to make sense of the provisions. Californians have the right to limit data collection only when businesses use their sensitive information in unexpected ways or to make “inferences” about them ([Appendix C2](#)). This limitation is vague and opens loopholes to potential exploitation by bad actors. Businesses should be prevented by default from using sensitive data (even if it is not used to make an inference about the user) for extraneous secondary purposes.

Put stricter limits on permitted secondary processing. Even when personas were able to opt out of the sharing of their health-related data, companies continued to share data with third parties. While some of this sharing may be noncompliant with various privacy laws, in other cases the companies may be taking advantage of broad loopholes in the law that allow sharing for operational purposes. While there are performance benefits to outsourcing certain functionality to third parties, widespread sharing may be inconsistent with the expectations of consumers who go out of their way to exercise their right to opt out of data sharing.

Make data minimization the default, limit notice and choice

New and existing laws should incorporate stronger default protections that do not force consumers to make all-or-nothing privacy choices. Ideally, privacy laws would include **strict data minimization provisions** that prevent companies from collecting information they do not need to provide the product or service. At the very least, consumers should be able to withhold their permission for secondary use of their sensitive data and still access the website or service.

In some cases where data is collected directly from a consumer, consent is implicit in the context. For example, a consumer answering a recommendation quiz question expects their health answer to be used to generate a recommendation. But without strong data minimization requirements, that data could be used for other purposes that the consumer did not anticipate. Companies that collect data for a core operational purpose should be broadly prohibited from reusing data for unrelated purposes, with some narrow, carefully tailored exceptions. Companies should not be permitted to indirectly collect or infer sensitive data unless they do so

in furtherance of a consumer request, and even then they should be required to ensure that consumers understand how their data is being used. Washington’s My Health My Data Act is a strong start toward meaningful default protections for the processing of sensitive data.

Beef up enforcement

We are not aware of any state enforcement actions taken by California or Virginia that are focused on sensitive data under the new laws. We found one instance of re-targeted advertising ([Case 2](#)) after opting out of sharing, which might run counter to (at least) the spirit of the protections provided by California’s Do Not Sell/Share right. We also found several instances where site privacy policies did not seem to disclose clearly whether collected sensitive data was used to make inferences or for other purposes. These cases suggest that some sites might not be fully in compliance with new privacy laws.

For states that are introducing new legislation, we encourage policymakers to allow private enforcement. While state enforcement offices are dedicated to protecting consumers, they are also often constrained by a lack of resources. Our research suggests that compliance may be lagging behind the timelines required by regulation, and that the complexity of the data sharing and processing ecosystems prevents privacy enforcers from completing investigations at the speed needed to enforce those timelines. At the very least, we strongly encourage more funding for privacy enforcers, particularly funding that allots technological expertise and tools to tackle sophisticated investigations such as those involving cookie management.

Educate businesses

As previously discussed, even our team of experts struggled to apply certain sections of new privacy law—so we are sympathetic to businesses that call for additional clarity. As U.S. data rights evolve, regulators should develop educational materials and conduct outreach to help well-intentioned businesses better understand their obligations. Regulations should provide clear examples of what constitutes a health “condition,” and indicate to what extent incidental or indirect collection of sensitive information is covered.

Recommendations for businesses

Think before you collect. There are many legitimate reasons for businesses to collect sensitive data. But there are less compelling use cases as well. Do you *really* need to know a consumer’s specific health condition to recommend a relevant product? Can you achieve the consumer’s goals without additional information? With regards to health-relevant information, always aim to minimize data specificity, identifiability, and quantity. Even if sharing with service providers is legally defensible, it may surprise and potentially alienate your customers.

Limit third-party sharing. Relying heavily on third-party marketing, analytics, and social media tools can make site development simpler. But each additional piece of software adds complexity and makes your site more vulnerable to data leaks or shares. Before implementing on a site, ensure each pixel, tag, cookie, or SDK has a specific, documented purpose, and consider whether a less intrusive method exists to address the business goal.

Audit vendors, especially ads and analytics. If you do need to rely on third-party service providers, make sure they are prioritizing data privacy. Before onboarding a vendor, perform due diligence. Consider incorporating privacy protections into procurement contracts. After onboarding a vendor, make a plan for regular monitoring and auditing. Technical tools exist for this exact purpose. In this study, we used Boltive’s auditing tool to find that targeting-related tags and cookies often persisted after consumer opt-outs. Even if many of those objects may be an unintentional result of a configuration error or an overeager marketing team member, they can compromise the privacy of sensitive data for thousands of consumers. As stated by the FTC and U.S. Department of Health and Human Services, “it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app.”⁵⁰

Check on your consent systems. Different jurisdictions have different requirements around disclosures of data use, consent before collection, and opt-out rights for some uses of data. Several states now require that businesses honor opt-outs of sale and targeted ads through universal privacy controls or authorized agents. Ensure your consent management platforms are properly expressing consumer preferences downstream of back-end tools and third-party vendors. As more states pass privacy laws, businesses may be able to simplify compliance by using a holistic approach that covers all relevant laws, rather than attempting to implement dozens of different consent flows that are geofenced by state.

Stay up-to-date on rules. The U.S. privacy landscape is in flux, and regulations can be confusing. Businesses nevertheless have a clear responsibility to keep up with the latest regulations. Make sure your technology teams receive updates regarding state regulations and federal guidance from agencies like the Federal Trade Commission, Office for Civil Rights, and Health and Human Services, and stay abreast of relevant class-action outcomes. Consult experts to better understand complex and evolving definitions of terms such as “sale” and

⁵⁰ FTC and U.S. Department of Health and Human Services Office for Civil Rights, “Re: Use of Online Tracking Technologies,” July 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

“sensitive.” A simple first step is to sign up for newsletters from privacy industry organizations and relevant agencies. Do not be surprised by an uptick in government enforcement of data privacy laws. Guidance, warnings, and letters from the FTC suggest the agency plans to continue enforcement actions on these topics.

Appendix A: Research Methods

Appendix A1: Target sites, buy signals, and consent signals

Target site	Description and topics	Buy signal	Persona opt-in mechanism	Persona opt-out mechanism
Barnes & Noble barnesandnoble.com	Retail bookstore, invisible disabilities	<ol style="list-style-type: none"> 1. In the search bar, type "Chronic Fatigue Syndrome" 2. Select a book, add to cart 3. Select second book, add to cart 4. Select third book, add to cart 	Disclosure banner with "Accept All Cookies"	<p>Disclosure banner with 2 buttons: Manage Preferences and Accept All Cookies</p> <p>Can withdraw consent for on-site data collection in link at end of cookie policy</p> <p>Do Not Sell link goes to web form that requires entry of PII</p>
Dupixent dupixent.com	Medication information site, jointly operated by Sanofi and Regeneron	<ol style="list-style-type: none"> 1. On the homepage, choose a condition (asthma) 2. In the top nav, go to: Patient Resources >> Doctor Discussion Guide 3. Click I'm Ready 4. Fill out the questionnaire 	None	<p>Refers users to separate policies of parent companies:</p> <p>Sanofi: multiple clicks to get to a web form that does not apply to on-site collection</p> <p>Regeneron: no opt-out for on-site collection, referral to DAA for ad opt-out and to download Google Analytics browser plug-in⁵¹</p>
Everlywell everlywell.com	Testing services, STD testing	<ol style="list-style-type: none"> 1. On the homepage, click Shop in the top nav 2. Click Sexual Health 3. Click STD Test - Female 4. Click Add to Cart 	None	Email to opt out of email marketing
Evolve evolvreatment.com	Residential treatment center, addiction, teens	<ol style="list-style-type: none"> 1. Google "teen detox California Evolve" 2. Click on Evolve Treatment Centers in Google results 3. Click For Teens >> Tips & Advice for Struggling Teens 4. Turn 10 pages under Tips & Advice 	Disclosure banner with Accept All Cookies	<p>Disclosure banner with two buttons: Do Not Sell My Personal Information and Accept All Cookies</p> <p>Withdraw consent by clicking Do Not Sell My Personal Information button in footer</p>
Fertility Out Loud fertilityoutloud.com	Fertility treatment info, run by Ferring	<ol style="list-style-type: none"> 1. Click Find Specialist in the top nav 2. Click Find a Specialist Near You 3. Click Give Me the Guide 	Disclosure banner with one button: Okay	Privacy notice refers consumers to the Digital Ad Alliance opt-out tool

⁵¹ Note: Because there were no direct opt-out mechanisms, our Do Not Sell/Share persona did not attempt to follow these instructions. At some point after our data collection concluded, Regeneron updated its site to include an Opt Out of Sale option in a cookie banner.

Target site	Description and topics	Buy signal	Persona opt-in mechanism	Persona opt-out mechanism
	Pharmaceuticals	4. Scroll to Not Your First Appointment? and click the first radio button		
LoveWellness lovewellness.com	Female health, vaginal products	1. On the homepage, click Take the Quiz 2. Take the quiz, including questions on vaginal health 3. Click the recommended product and add to cart 4. View cart	Disclosure banner with 2 buttons: Preferences and Accept	Disclosure banner with 2 buttons: Preferences and Accept No way to withdraw consent
MaxiAids maxiaids.com	Disability aids, vision impairments, blindness	1. Click Vision & Blind in top nav 2. Click Braille Products >> Braille Printers 3. Add EZ Form Braille-Tactile-Braille Duplicator USA to cart 4. Click Vision & Blind >> Low Vision Clocks 5. Add Atomic 2-inch LCD Number Clock with Temperature to cart	None	None
Newport Academy www.newportacademy.com	Residential treatment center, mental health	1. Google "Teen depression california newport" 2. Click on Newport Academy ad in Google Search 3. Browse content on teen depression, residential programs, and therapies in treatment (turn 10 pages)	None	None
TakeCareOf takecareof.com	Personalized vitamins	1. On the homepage, click Take the Quiz 2. Complete the quiz, choose questions that cover digestive and sexual issues 3. Click on Learn More for one of the recommended products 4. Click Check Out	A statement about data collection with an I Agree button, required to continue	No way to opt out of on-site collection Do Not Sell link in footer leads to privacy policy that directs consumer to a DataGrail form that requires entry of PII
Viking Man vikingman.com	Male health, erectile dysfunction, hair loss, vitamins	1. On the homepage, click Love Better 2. Click Our Treatment Plans 3. Click Viagra Generic 4. Click Start My Visit	None	None for on-site data collection Email to opt out of email and SMS marketing

Appendix A2: Cookie, ad, and tag data collected

For each target site and persona, cookies and tags were collected and counted on the initial page load. For Do Not Sell/Share and No Opt-In personas, cookies and tags were collected and counted after the opt-out was completed.

We categorized each cookie and tag with a good-faith guess of the intended purpose of the object. For example, a tag from advertising company DoubleClick (originating from “doubleclick.net”) on one site was classified as “interest-based advertising.” Another tag from the content delivery provider “cloudflare.com” was categorized as “necessary.” For categorization, we relied on a combination of domain expertise, developer documentation, and proprietary methods developed by Boltive.

The collection of interest-based ads was performed using Boltive’s patented scanning technology, which uses AI to recognize brands’ advertising campaigns, capturing screenshots and details about the ads as they are served to the user. More information is available in the Methods section under “[Categorizing tags and cookies](#)” and “[Limitations](#).”

Appendix A3: Outreach to companies

In October 2023, we attempted to contact via email all 10 companies included in our analysis, asking for comments on our findings and clarifications of their data practices. We received responses from Barnes & Noble, Dupixent, Everlywell, and TakeCareOf. We received only an automated message from LoveWellness. We received no response from Evolve, Fertility Out Loud, MaxiAids, Newport Academy, or Viking Man.

Appendix B: Findings

Appendix B1: Is collected data “sensitive”?

Privacy policies were analyzed mid May to mid June 2023. More information about the consent mechanisms of each site is available in [Appendix A1](#). Note on HIPAA: While some of the businesses we researched are covered entities under HIPAA in some contexts, we suspect that none of the information collected for our research is considered Protected Health Information.

Target site	Data collected (during Buy Signal, not exhaustive)	“Sensitive” in CA?	“Sensitive” in VA?	Discloses whether/how sensitive data is used?	Mentions CA right to limit sensitive data? ⁵²	Offers explicit opt-in mechanism? ⁵³ (during the buy signal)
Barnes & Noble	Keyword search history, usage data, purchase interest	Unlikely, as book interest is indirect; possibly sensitive if health-relevant inferences are made from that data ⁵⁴	Unlikely	No	No	Yes; cookie manager has Accept button
Dupixent	Medical condition (asthma), medications, usage data, cookies	Likely; collects a specific medical condition	Likely; collects a specific medical diagnosis	Sanofi: No; has no information about sensitive data Regeneron: Yes; says, “...we will not disclose your personal data to a third party and/or build a profile about you or otherwise alter your experience outside the current interaction with the business”	No	No

⁵² California only requires businesses to provide the right to limit processing of sensitive data if the data is used to generate inferences or is used for a purpose other than those listed as permitted uses in regulation. See [Appendix C2](#) for details.

⁵³ We focused our analysis on the parts of the site our personas interacted with during their buy signal actions. Sites may provide opt-in mechanisms elsewhere on the site. A consent mechanism is required for sensitive data collection by Virginia law. Some sites might not be covered by Virginia law, or may not be collecting data considered sensitive. See Appendix C1.

⁵⁴ In a November 2023 comment, Barnes & Noble stated that they “do not collect any sensitive information” from customers.

Target site	Data collected (during Buy Signal, not exhaustive)	“Sensitive” in CA?	“Sensitive” in VA?	Discloses whether/how sensitive data is used?	Mentions CA right to limit sensitive data? ⁵²	Offers explicit opt-in mechanism? ⁵³ (during the buy signal)
Everlywell	Identifiers, purchases considered, browsing history, location data, inferences, cookies	Likely; information implies sexual activity, probably used for inferences	Unlikely; implies symptoms or sexual activity	Yes; “Sensitive personal information” is used for “Internal reporting and analytics purposes....and to facilitate more targeted marketing”	Yes; unclear instructions for enacting right, likely via email	No
Evolve	Browsing data, health info targeted to teens	Maybe; the pages that you visit may indirectly indicate age, intention for treatment, interest in a diagnosis	Unlikely; the pages that you visit may indirectly indicate age, intention for treatment, interest in a diagnosis	Yes, though they claim not to sell or share sensitive health information; they mention selling/sharing inferences but it is unclear if they use sensitive information to do so	Yes; enact right via email	Unclear; cookie banner with Accept button, but users can proceed without clicking Accept
Fertility Out Loud	Browsing data, nonspecific fertility treatment history	Likely; collects non-specific information about fertility status and treatment history	Maybe; collects fertility status and treatment history, but indirectly	Yes; “We do not use or disclose sensitive personal information outside of the purposes for which it was collected”	No	No; cookie disclosure banner has 1 button – Okay– but users can proceed without agreeing
LoveWellness	Take the Quiz email, name, phone, supplement usage, health area concern (“vaginal” or “gut”), number of interactions with gynecologist, specific vaginal symptoms and disorders (yeast infections, BV, UTIs)	Likely; includes sexual information, specific conditions	Likely; includes sexual information, specific conditions	Vague; says they collect sensitive information and that they make inferences from personal information, but does not clarify if that includes sensitive information	No	Unclear; consent management platform is used for opt-in consent, but quiz can be submitted without clicking Accept

Target site	Data collected (during Buy Signal, not exhaustive)	“Sensitive” in CA?	“Sensitive” in VA?	Discloses whether/how sensitive data is used?	Mentions CA right to limit sensitive data? ⁵²	Offers explicit opt-in mechanism? ⁵³ (during the buy signal)
MaxiAids	Browsing data, purchase interests	Maybe; purchases are likely to concern health and imply a specific condition	Unlikely; some purchases are likely to imply a specific diagnosis, but somewhat indirect	No; only mentions sensitive information in the context of discussing security protocols for credit card numbers	No	No
Newport Academy	Usage data, cookies, interest in teen mental health	Maybe; pages visited may indirectly indicate age, intention for treatment, interest in a diagnosis	Unlikely; pages visited may indirectly indicate age, intention for treatment, interest in a diagnosis	No	No	No
TakeCareOf	Name, age, sex, email, history with wellness products, non-specific medication history, transit use, general health goals, eating and exercise habits, allergies, celiac status	Likely; includes information that concerns health, used for quiz generation	Likely; celiac is a specific diagnosis	Yes; “Although some of the information we collect and process about you may be considered sensitive personal information, we only process such information for purposes authorized by law, such as to provide services you request from us or to verify your information” ⁵⁵	No	Yes; for VA, a specific notice is presented before quiz collection and user must click Agree
Viking Man	Usage data, location information, IP information, email, name, interest in erectile dysfunction treatment	Maybe; pages visited may indicate intention for treatment of ED	Unlikely; pages visited may indirectly indicate intention for treatment of ED	Vague; vendors are contractually bound to keep “Sensitive Personal Information confidential and use it only for the purposes for which we disclose it to them.”	No	No

⁵⁵ In a November 2023 statement, TakeCareOf stated that they do not share quiz response data with third parties for the purposes of marketing.



Appendix B2: Does business claim to sell/share data?

Target site	Sells/shares data (some sharing considered "sale")	On-site cookie controls	CA Do Not Sell method	Other privacy notes
Barnes & Noble	Yes	Yes	Form or phone	Seems to voluntarily offer DSR ⁵⁶ to all states
Dupixent	Regeneron: Yes Sanofi: Unclear	No; redirects to parent companies ⁵⁷	Regeneron: disable cookies in browser Sanofi: unclear web form ⁵⁸	Directs to two separate policies, Sanofi (updated 2020) and Regeneron
Everlywell	Yes	No ⁵⁹	Disable cookies in browser	VA sensitive data rights are conflated with CA "right to limit" in the privacy notice. VA residents have no such right to limit.
Evolve	Yes	Yes	Cookie	Offers DSR at their discretion to residents of states without rights
Fertility Out Loud	Yes	No	Unclear; form and Disable Cookies in browser	Cookie notice has no choice options
LoveWellness	Yes	Yes	Disable cookies in browser	VA privacy link broken (404 error)
MaxiAids	Claims no sale	No	None	Privacy notice does not mention any state privacy rights
Newport Academy	Claims no sale	No	None	-
TakeCareOf	Yes	No	Form or email	-
Viking Man	Yes	No	None	Offers opt out of third-party email promotions; only mention of CA rights is "Shine the Light"

⁵⁶ "Data subject request" is a general term for consumer requests related to legal data rights

⁵⁷ In response to our findings, a spokesperson for Sanofi and Regeneron indicated in November 2023 that they were planning to add "a cookie banner and preference center to provide increased transparency and choice for visitors" on Dupixent.com.

⁵⁸ See [Appendix A1](#) for more details on Regeneron's mechanisms.

⁵⁹ A representative from Everlywell stated that in September 2023 the site added on-site cookie controls after our data collection had been completed.

Appendix B3: Cookies and tags fired after opt-outs

See [Appendix A2](#) for details on data collection. Data for cookie and tag firings were very similar between California- and Virginia-based personas. We report the rates of cookies and tags firing after opt-out in [Table 1](#). For space reasons, we're not including the cookie/tag results for all 10 companies. As an illustrative example of data collected, we're including some of the cookie data collected from one of the sites (TakeCareOf).

Table A: Example. Counts of cookie objects collected from one site across personas

Intended as an illustrative example, here are the counts of categorized cookies collected for TakeCareOf. As expected, the number of cookie objects decreases after opting out of cookies. However, some unexpected cookies related to marketing profiles and IBA persisted even after opting out. In a November 2023 statement, TakeCareOf stated that while these cookies do persist, the site is configured to block data sharing with third parties after opt-out. If their system is implemented correctly, the cookies we categorized as related to interest-based advertising do not represent a risk of sharing data for interest-based advertising.

Cookie Classification	CA No Opt-Out	CA Do Not Sell/Share	VA No Opt-Out
Functional	44	17	20
Interest-Based Advertising	20	8	20
Necessary	0	1	0
Other Marketing	4	2	4
Performance	16	8	14
Grand Total	84	36	58

Table B: Example. Sample of cookie objects collected from one site across personas

As shown in [Table A](#), personas saw from 36 to 84 cookie objects total when visiting TakeCareOf. To further illustrate the objects, here is a small selection of 11 types of specific cookie-related data and object counts collected from TakeCareOf.com.

Vendor	Cookie Name	Cookie Domain	Cookie Classification	CA No Opt Out	CA Do Not Sell/Share	VA No Opt Out
Adobe Analytics	mboxEdge Cluster	.espn.com	Performance		1	
Bing/Microsoft	MR	.bat.bing.com	Other Marketing	1		1

Vendor	Cookie Name	Cookie Domain	Cookie Classification	CA No Opt Out	CA Do Not Sell/Share	VA No Opt Out
Bing/Microsoft	MUID	.bing.com	Other Marketing	1		1
Google Ads	IDE	.doubleclick.net	Interest-Based Advertising	1		1
Google Ads	NID	.google.com	Interest-Based Advertising			1
Pinterest	_pinterest_ct_ua	.ct.pinterest.com	Interest-Based Advertising	3		2
Pinterest	_pin_unauth	.takecareof.com	Interest-Based Advertising	1	1	1
Quantcast	mc	.quantserve.com	Performance	1		1
TakeCareOf	login_id	takecareof.com	Functional	1	1	1
Twitter	muc_ads	.t.co	Interest-Based Advertising	1		1
Twitter	personalization_id	.twitter.com	Interest-Based Advertising	1		1

Table C: Dates of data collection

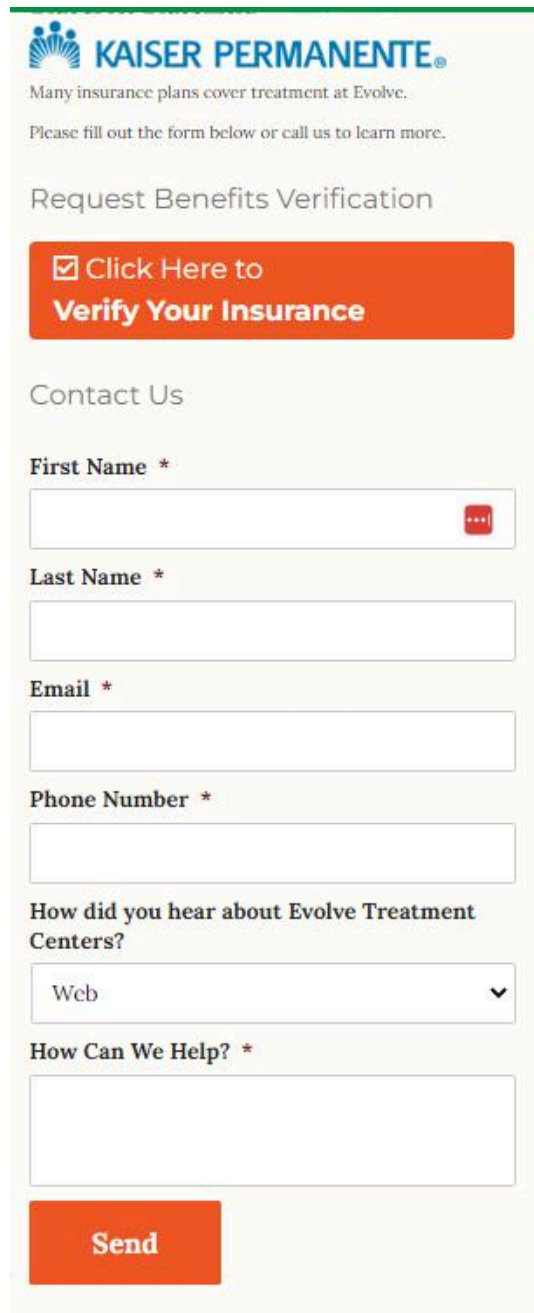
Data was collected over the span of a few weeks in Spring 2023. The date in the table below is the date that each persona was created and completed its consent signal (see [Appendix A1](#)). Targeted ads were collected over the following two weeks. A few personas had delayed run dates due to technical difficulties. Analysis of privacy policies and site content was conducted between April and July 2023.

	California Personas	Virginia Personas
Barnes & Noble	3/31/23	4/24/23
Dupixent	3/29/23	4/24/23
Everlywell	3/29/23	4/24/23
Evolve	4/5/23	4/24/23
Fertility Out Loud	3/31/23	4/24/23
LoveWellness	3/29/23	4/24/23
MaxiAids	3/30/23	4/24/23
Newport Academy	3/29/23	4/24/23
TakeCareOf	3/29/23	6/2/23
Viking Man	6/25/23	4/24/23

Appendix B4: Ambiguity in HIPAA coverage

Figure A: A confusing form on Evolve

This May 2023 screenshot illustrates that it is sometimes confusing whether data on the site is being collected and processed as a covered HIPAA entity. The form collects largely generic identifiers but it also seems like it might be used for insurance verification purposes.



The screenshot shows a Kaiser Permanente web form. At the top is the Kaiser Permanente logo and the text: "Many insurance plans cover treatment at Evolve. Please fill out the form below or call us to learn more." Below this is the heading "Request Benefits Verification". A prominent orange button with a checkmark icon contains the text "Click Here to Verify Your Insurance". Underneath is a "Contact Us" section with several required fields: "First Name *", "Last Name *", "Email *", and "Phone Number *", each with a corresponding text input box. There is also a dropdown menu for "How did you hear about Evolve Treatment Centers?" with "Web" selected. A final required field "How Can We Help? *" is a larger text area. At the bottom is an orange "Send" button.

Appendix C: Relevant Regulations

Appendix C1: Virginia Consumer Data Protection Act

Narrative Summary

The Virginia Consumer Data Protection Act (VCDPA)⁶⁰ went into effect January 1, 2023. The law affords protections for the data of Virginia residents who are acting as consumers or civilians (not in their role as employees or in business).

The VCDPA declares that residents have several data rights, including the right to opt out of the sale of their data, opt out of targeted advertising, and opt out of being profiled. Most relevant to this work, the act defines a class of “sensitive data” that carries extra protections. For sensitive data, businesses must get specific affirmative consent before collection and processing. While we don’t have much guidance yet about what regulators consider adequate consent, common dark practices like pre-checked cookie banners probably won’t cut it.

Selected Definitions from the VCDPA

“Consent” means a clear affirmative act signifying a consumer’s freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

“Process” or “processing” means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

“Sale of personal data” means the exchange of personal data for monetary consideration by the controller to a third party. “Sale of personal data” does not include:

1. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;
2. The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
3. The disclosure or transfer of personal data to an affiliate of the controller;

⁶⁰Consumer Data Protection Act, Chapter 53, Code of Virginia § 59.1-575, 2023, <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>.

4. The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or
5. The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

"Sensitive data" means a category of personal data that includes:

1. Personal data revealing racial or ethnic origin, religious beliefs, **mental or physical health diagnosis**, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data.

Selected Provisions from the VCDPA

§ 59.1-576. Scope; exemptions.

A. This chapter applies to persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.

B. This chapter shall not apply to any...(iii) covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5) ...

C. The following information and data is exempt from this chapter:

1. Protected health information under HIPAA;
2. Health records for purposes of Title 32.1;
3. Patient identifying information for purposes of 42 U.S.C. § 290dd-2;

...

7. Information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

8. Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under this subsection that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2...

D. Controllers and processors that comply with the verifiable parental consent requirements of the Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.) shall be deemed compliant with any obligation to obtain parental consent under this chapter.

§ 59.1-578. Data controller responsibilities; transparency.

A. A controller shall:

2. Except as otherwise provided in this chapter, not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent;

...

5. not process sensitive data concerning a consumer without obtaining the consumer's consent, or, in the case of the processing of sensitive data concerning a known child, without processing such data in accordance with the federal Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).

...

C. Controllers shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes:

1. The categories of personal data processed by the controller;
2. The purpose for processing personal data;
3. How consumers may exercise their consumer rights pursuant § 59.1-577, including how a consumer may appeal a controller's decision with regard to the consumer's request;
4. The categories of personal data that the controller shares with third parties, if any; and
5. The categories of third parties, if any, with whom the controller shares personal data.

Appendix C2: California Laws and Regulations

Narrative Summary

In California, both the California Consumer Privacy Act (CCPA)⁶¹ and the Confidentiality of Medical Information Act (CMIA) have provisions related to sensitive or health-related data.

CCPA's definition of "sensitive data" includes biometric information used for unique identification, data "collected and analyzed concerning a consumer's health," and data "collected and analyzed concerning a consumer's sex life or sexual orientation."

Businesses can collect sensitive data without many extra rules so long as it's used for select legitimate business purposes or isn't being used to make any inferences about the consumer. Business purposes include security and data integrity, customer service or business transactions, product warranties, and necessary use that an average consumer would expect from the service. Regulations offer this example: "a business that sells religious books can use information about its customers' interest in its religious content to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business" doesn't use that data for profiling or share it with third parties.

All businesses collecting sensitive data must include a basic disclosure of how that sensitive data is used. If sensitive data is used for profiling or making inferences, the consumer has the right to limit the use of their sensitive data. In this case, businesses must either display a conspicuous Limit the Use of My Sensitive Personal Information link or support relevant global opt-out signals. Those businesses must also disclose additional general information about the collection, purpose, and sharing of sensitive data in their privacy notice.

CCPA regulations released by the Privacy Protection Agency in March 2023 further specify that generic cookie banners don't count as sufficient notice and choice; notices related to sensitive data must specifically address the use and disclosure of sensitive personal information.

Selected Definitions from the CCPA

1798.140. Definitions.

(d)(1) "Business" means: A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal

⁶¹ California Consumer Privacy Act of 2018, Title 1.81.5 § 11798, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or, households.

(C) Derives 50 percent or more of its annual revenues from selling, or sharing consumers' personal information.

....

(e) "Business purpose" means the use of personal information for the business's operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including but not limited to non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer, provided that for the purpose of advertising and marketing,

a service provider or contractor shall not combine the personal information of opted-out consumers which the service provider or contractor receives from or on behalf of the business with personal information which the service provider or contractor receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

....

(r) “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

....

(v)(1) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

...

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

...

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement.

...

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

(v)(2) “Personal information” does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, “publicly available” means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. “Publicly

available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. “Personal information” does not include consumer information that is deidentified or aggregate consumer information.

....

(ae) “Sensitive personal information” means:

(1) personal information that reveals

- (A) a consumer’s social security, driver’s license, state identification card, or passport number;
- (B) a consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- (C) a consumer’s precise geolocation;
- (D) a consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership;
- (E) the contents of a consumer’s mail, email and text messages, unless the business is the intended recipient of the communication;
- (F) a consumer’s genetic data; and

(2)

- (A) the processing of biometric information for the purpose of uniquely identifying a consumer;
- (B) personal information collected and analyzed concerning a consumer’s health; or**
- (C) personal information collected and analyzed concerning a consumer’s sex life or sexual orientation.**

Sensitive personal information that is “publicly available” pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal information or personal information.

....

(ah)

(1) “Share,” “shared,” or “sharing” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

(2) For purposes of this title, a business does not share personal information when:

- (A) A consumer uses or directs the business to:
 - (i) intentionally disclose personal information; or
 - (ii) intentionally interact with one or more third parties;

Selected Provisions from the CCPA

1798.100. General Duties of Businesses that Collect Personal Information

(a) A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers as to:

(1) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section.

(2) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice consistent with this section.

1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

(a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services, to perform the services set forth in paragraphs (2), (4), (5), and (8) of ["Business purposes"], and as authorized by regulations adopted [by California regulators]. **A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.**

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction, unless the consumer subsequently provides consent for the use or disclosure of the consumer's sensitive personal information for additional purposes.

(c) [Summary: Service providers must also limit use of sensitive data when instructed.]

(d) **Sensitive Personal information that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this Section**, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.

....

1798.135. Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

(a) A business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 shall, in a form that is reasonably accessible to consumers:

...

(2) Provide a clear and conspicuous link on the business's internet homepage(s), titled "Limit the Use of My Sensitive Personal Information" that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business's discretion, utilize a single, clearly-labeled link on the business's internet homepage(s), in lieu of complying with paragraphs (1) and (2), if such link easily allows a consumer to opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

...

(b)(1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt-out of the business's sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

Selected Regulations related to the CCPA

§ 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link

(g) A business does not need to provide a Notice of Right to Limit or the "Limit the Use of My Sensitive Personal Information" link if:

(1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or

(2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.

...

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

(b)(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

....

(m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. **A business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.**

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to a specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) [Summary: For security and fraud.]

(3) [Summary: To resist malicious, deceptive, fraudulent, or illegal actions.]

(4) [Summary: For physical safety.]

(5) **For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' interest in its religious content to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use sensitive personal information to create a profile about an individual consumer or disclose personal information that reveals consumers' religious beliefs to third parties.**

(6) To perform services on behalf of the business. For example, a business may use information for maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing

storage, or providing similar services on behalf of the business.

(7) To verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.

(8) To collect or process sensitive personal information where the collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.