Good Luck Opting Out

Manipulative Design Patterns in Opt-Out Processes

May 2026

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

ABOUT EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for privacy, algorithmic fairness, and government accountability. Learn more at **epic.org**.

AUTHORS

Caroline Kraczon, EPIC Counsel

Justin Sherman, EPIC Scholar In Residence

ACKNOWLEDGEMENTS

The authors would like to thank EPIC Counsel Kara Williams, Senior Counsel Sara Geoghegan, and Deputy Director and Policy Director Caitriona Fitzgerald for their comments on this report, as well as Deputy Director and Director of Enforcement John Davisson for his support throughout this research effort.

FUNDING STATEMENT

This project was supported by funding from the Foundation for Public Service (FPS)—a 501(c)(3) fiscally sponsored project of Global Impact.

HOW TO SUPPORT EPIC

EPIC's mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. As a fully independent non-profit, EPIC does not accept corporate or government sponsorships. We need your support.

Please consider donating online at **epic.org/donate**. To learn about about additional ways to support EPIC, such as donor-advised funds and qualified charitable donations, visit **epic.org/support-epic/**. Anonymous donations are accepted.

TABLE OF CONTENTS

Introduction....4

Literature Summary....8

Legal Summary....14

Methodology....17

Analysis....23

Overall Trends (Not Necessarily Manipulative)....23

Manipulative Design Patterns....27

Failing to Provide a Clear Mechanism to Opt Out of Sale and Sharing of Personal Information....27

Not Clearly Linking Opt-Out Form from Homepage and/or Privacy Policy....29

Requiring Consumers to Submit Multiple Separate Forms....29

Deceptive Statements About Opt-Outs and Their Success....30

Confusing or Misleading Language....31

Requiring Consumers to Log In or Pay for a Subscription Before Opting Out....33

Design Elements Hiding Important Opt-Out Information....34

Checkbox Options Preselected....36

Conclusion....39

Appendix A: State Privacy Law Language Regarding Opt-Outs....43

Introduction

Consumers face an incredible power imbalance when trying to opt out of the collection, use, transfer, or sale of their personal data. The average person uses many online platforms and applications, meaning there are many companies with which they directly interact that can store or transfer their data. On top of that, many other companies—including large language model (LLM) vendors that scrape the internet and data brokers that collect people's data without any actual, informed consent—store, transfer, and sell consumers' data, too. Submitting opt-out and other privacy request forms to all of these companies requires significant time and effort. Even as more states pass laws giving consumers more rights over their personal data, such as the right to opt out of the sale or sharing of their data, a consumer trying to limit their data exposure still faces a daunting task.

This problem is perhaps no clearer than in cases where individuals are at risk of physical violence, such as from online doxxing or stalking. Public servants across the country, at all levels of government, are facing an increase in violent threats to themselves and their families.[1] In plenty of cases, there is a direct connection to personal data exposure, such as when the individual who allegedly murdered Minnesota state legislator Melissa Hortman and her husband Mark in 2025—and shot and critically wounded another legislator and his wife—used "people search" data brokers to research his targets beforehand.[2] For decades, abusive individuals have likewise used technologies and data to locate, hunt down, and harass, intimidate, assault, and even murder other people, predominantly impacting women, women of color, and LGBTQ+ people.[3] For these individuals, reducing their data footprint can be time-intensive, informationally overwhelming, and even costly (including if one pays for online privacy, cybersecurity, and threat monitoring services). It is therefore essential for people's privacy and physical safety that opt-out paths are as accessible, easy to use, and efficient as possible.

In this study, we evaluate whether major data-collecting companies' opt-out paths for consumers utilize manipulative design practices. We do so by drawing on existing research and literature, state privacy laws, Federal Trade Commission

[1] *Data Broker Harms to Public Officials, EPIC* (Dec. 2025); Justin Sherman, Data Brokers and Threats to Government Employees, Lawfare (Oct. 22, 2024).

[2] Lily Hay Newman, *Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses*, Wired (June 16, 2025).

[3] *Data Broker Harms: Domestic Violence Survivors*, EPIC (Dec. 2025).

(FTC) enforcement actions, and our own experience to develop a list of specific design elements and behaviors that constitute manipulative design while navigating an opt-out process. Then, we apply those criteria to 38 companies: 15 data brokers, four social media companies, nine other Big Tech companies, six surveillance technology vendors, and four dating apps. Using detailed spreadsheets, online archiving services, and locally stored screenshots, we then measure and document the extent to which the companies' opt-out processes contain manipulative design elements.

We find at least eight major manipulative design patterns across the 38 companies' opt-out processes:

- Failing to provide a clear mechanism to opt out of sale and sharing of personal information
- Not clearly linking opt-out form from homepage and/or privacy policy
- Requiring consumers to submit multiple separate forms
- Deceptive statements about opt-outs and their success
- Confusing or misleading language
- Requiring consumers to log in or pay for a subscription before opting out
- Design elements hiding important opt-out information (including design elements inducing false beliefs, hiding or delaying disclosure of material information, or obscuring or subverting privacy choices)
- Checkbox options preselected

We also identified several other, overall trends (not necessarily manipulative). For example, many companies used the same vendor for their opt-out form or webpage; several companies, primarily the location data brokers, required consumers to submit mobile ad identifiers to opt out. Many websites are also difficult to archive on services such as the Internet Archive, raising critical transparency and accountability questions.

This is a serious problem for individuals at risk of violence. Individuals such as local public servants or federal civil servants who are doxxed and swatted; survivors of gendered violence and their children; targets of stalking; and other

people subject to targeting and violence based on their personal data are under a time crunch—often, life-or-death—to get their home address and other information removed from websites and company databases as quickly and thoroughly as possible. It is important for their physical safety to ensure that relevant data is removed from data broker websites and ceases to be transferred efficiently and effectively. As our research makes clear, however, many companies fail to make their opt-outs easy to use and effective.

We recommend:

- Companies should evaluate their opt-out processes and remove manipulative design features; clearly provide opt-out instructions and links in multiple places, including on their website homepage, within the privacy policy, and within other relevant locations and communications to users; make their opt-out processes simple, fast, and clearly described; clearly explain that certain types of data may be exempt from opt-outs, including publicly available data; and state any other limits related to the opt-out request, such as legally required retention timelines for certain data.
- After consumers submit an opt-out request, companies should ensure that they continually honor the opt-out request by conducting ongoing, periodic audits to ensure they are not selling or transferring data that has been the subject of an opt-out request.
- The FTC should consider using its Section 5 authority (that prohibits unfair and deceptive business acts or practices) to protect consumers from manipulative designs by bringing enforcement actions against companies with manipulative opt-out processes.
- State attorneys general—especially those in the states that have enacted privacy laws that include opt-out rights—should evaluate whether companies selling and transferring data about their constituents meet legal requirements relating to opt-outs. If state attorneys general find evidence that companies are not providing clear, easy-to-use opt-out processes because of manipulative design tactics, they should consider bringing enforcement actions against violating companies.
- More states should consider following California's lead to adopt a universal deletion mechanism, which makes it significantly easier for consumers to exercise their rights—especially in the face of manipulative, friction-laden

opt-out processes.

- More states should require companies to honor opt-out requests from universal opt-out mechanisms to allow consumers to automatically request to opt out from all websites they visit while they have a universal opt-out mechanism enabled.
- Above all, states should strengthen privacy protections for consumers by passing legislation that includes robust data minimization standards instead of relying on outdated notice-and-choice frameworks. As this report will show, consumers cannot effectively protect their own privacy by exercising opt-out rights. Strong data minimization standards would provide more meaningful privacy protections for consumers.

Literature Summary

There is extensive literature that discusses manipulative design patterns, often called "dark patterns." We did not aim for a comprehensive review of the literature. Instead, our goal was to highlight key trends and takeaways that were directly useful to building a list of criteria—enumerated in the next section—to evaluate manipulative design elements in an opt-out process.

A singular definition of a manipulative design practice (or a dark pattern) is difficult to develop. Identifying one definition is not our aim in this study. As an October 2022 report from the Organization for Economic Cooperation and Development (OECD) put it, "definitions developed in the academic and policy literature to date vary in terms of characteristics of the user interface of the website or app, mechanisms of effects on users, the role of user interface designers and the outcomes for the online business or the consumer."[4] But many definitions share common themes, including "deception, manipulation, coercion, or exploitation in the design of user interfaces that lead consumers to make decisions that may not reflect or engage their true preferences, intent, consent, autonomy or best interests."[5]

Harry Brignull, who has authored much of the foundational scholarship on this subject, writes in his 2023 book Deceptive Patterns that "[d]eceptive patterns disproportionately affect the most vulnerable groups in society, and the companies most willing to use deceptive patterns gain an unfair advantage against any competing companies that have a more ethical or user-centered mission."[6] Brignull also maintains a website that lists and defines deceptive patterns; 16 categories are currently listed on the site.[7] These are shown below with Brignull's verbatim definitions.

Category	Definition
Comparison prevention	The user struggles to compare products because features and prices are combined in a complex manner, or because essential information is hard to find.

[4] OECD, Dark Commercial Patterns, OECD Doc. 336, 13-14 (Oct. 2022).

[5] *Id.* at 14.

[6] Harry Brignull, *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You* 209 (2023).

[7] *Types of Deceptive Pattern*, Deceptive Patterns, (last accessed Apr. 16, 2026).

Category	Definition
Confirmshaming	The user is emotionally manipulated into doing something that they would not otherwise have done.
Disguised ads	The user mistakenly believes they are clicking on an interface element or native content, but it's actually a disguised advertisement.
Fake scarcity	The user is pressured into completing an action because they are presented with a fake indication of limited supply or popularity.
Fake social proof	The user is misled into believing a product is more popular or credible than it really is, because they were shown fake reviews, testimonials, or activity messages.
Fake urgency	The user is pressured into completing an action because they are presented with a fake time limitation.
Forced action	The user wants to do something, but they are required to do something else undesirable in return.
Hard to cancel	The user finds it easy to sign up or subscribe, but when they want to cancel they find it very hard.
Hidden costs	The user is enticed with a low advertised price. After investing time and effort, they discover unexpected fees and charges when they reach the checkout.
Hidden subscription	The user is unknowingly enrolled in a recurring subscription or payment plan without clear disclosure or their explicit consent.
Nagging	The user tries to do something, but they are persistently interrupted by requests to do something else that may not be in their best interests.

Category	Definition
Obstruction	The user is faced with barriers or hurdles, making it hard for them to complete their task or access information.
Preselection	The user is presented with a default option that has already been selected for them, in order to influence their decision-making.
Sneaking	The user is drawn into a transaction on false pretences, because pertinent information is hidden or delayed from being presented to them.
Trick wording	The user is misled into taking an action, due to the presentation of confusing or misleading language.
Visual interference	The user expects to see information presented in a clear and predictable way on the page, but it is hidden, obscured or disguised.

Across the literature, law, and policy, key criteria for manipulative design patterns span the characteristics of the user interface (e.g., coercive, deceptive, malicious, misleading, obnoxious, seductive, steering, trickery), mechanisms of effect on users (e.g., attack users, confuse users, deceive users, exploit users, manipulate users, mislead users, steer users, subvert user intent, subvert user preferences, trick users, undermine user autonomy, without user consent, without user knowledge), the role of user interface designers (e.g., abuse of designer knowledge, designer intent), and benefits and harms (e.g., benefit to service, harm to users).[8] For example, user interface designers could use their knowledge of technology and persuasion to sneak items into a user's basket through a small, selected-by-default checkbox or misdirect a user's attention to benefit the service, not the user.[9] Attention-capturing dark patterns span recommendations (e.g., recommender systems designed to trap users into making certain decisions), auto-

[8] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer, *What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods*, CHI '21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2 (2021).

[9] Colin M. Gray et al., *The Dark (Patterns) Side of UX Design*, CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 534 (Apr. 2018).

play (e.g., new content automatically and sequentially played without any user action), pull-to-refresh (e.g., using variable reward systems in human psychology to get users to constantly check for new content), infinite scrolling (e.g., variable reward exploitation that conveys to the user that new content will flow forever), and social investment (e.g., metrics such as views and likes that "bind" a use to a platform).[10]

Common examples of dark patterns across web and mobile include: requiring an account to use a service at all; making free and premium/app-only content visually indistinguishable from one another; using tiny close buttons/difficult to close ads; making it impossible for consumers to buy products or services as a guest (i.e., without an account); preselecting optional add-ons; sensing location by default without asking consent; time-delaying account deletion options; including provocative text to shame or guilt people into certain behavior; and giving some options visual precedence over others.[11] When it comes to the law, it can be challenging for enforcers, depending on the situation, to clearly connect dark patterns with factors like business intent.[12] But three common themes that enforcers could examine are (1) companies benefitting from consumers' illusion that they control digital interfaces, (2) exploiting consumers' online habits, and (3) targeting and eliciting vulnerability.[13]

Users of digital services with "mild" dark patterns are more than twice as likely to sign up for a dubious service than those in the control group—and without generating the backlash that more aggressive dark patterns do.[14] Companies also present manipulative design practices differently on web browsers, mobile browsers, and apps, which "saddle people with inconsistent experiences of autonomy, privacy, and control."[15] For example, a survey of approximately 53,000 product pages from approximately 11,000 shopping websites identified 1,818 instances of dark patterns across 15 specific types and seven broader categories,

[10] Alberto Monge Roffarello and Luigi De Russis, *Towards Understanding the Dark Patterns That Steal Our Attention*, CHI EA '22: CHI Conference on Human Factors in Computing Systems Extended Abstracts, 2-3 (2022).

[11] Johanna Gunawan et al., *A Comparative Study of Dark Patterns Across Web and Mobile Modalities*, Proceedings of the ACM on Human-Computer Interaction, vol. 5, issue CSCW2, 2 (2021).

[12] Lauren E. Willis, *Deception by Design*, 34 Harv. J. L. & Tech. 1, 115-190 (2020).

[13] *Id.* at 132, 134, 142.

[14] Jamie Luguri and Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. L. Analysis 1, 43-109 (Mar. 2021).

[15] Johanna Gunawan et al., *A Comparative Study of Dark Patterns Across Web and Mobile Modalities*, Proceedings of the ACM on Human-Computer Interaction 5, Issue CSCW2 (Oct. 2021).

with many websites using 22 third-party entities that "offer dark patterns as a turnkey solution."[16] Immersive environments, such as so-called virtual reality systems, pose their own manipulative design risks as well.[17]

The FTC published a detailed report in September 2022 on dark patterns.[18] It named the four main categories of dark patterns as design elements that: induce false beliefs, hide or delay disclosure of material information, lead to unauthorized changes, or obscure or subvert privacy choices.[19] The appendix to the report listed patterns in more detail. These spanned several categories:

- **Endorsements** (aka "social proof"), or false activity messages, deceptive consumer testimonials, deceptive celebrity endorsements, parasocial relationship pressure;
- **Scarcity**, or false low stock messages or false high demand messages;
- **Urgency**, or baseless countdown timers, false limited time messages, or false discount claims;
- **Obstruction**, or price comparison prevention, roadblocks to cancellation, or immortal accounts (e.g., making account deletion very difficult);
- **Sneaking** or **information hiding**, or sneaking items into user's carts ("sneak-into-basket"), hidden information, hidden costs, drip pricing (e.g., adding mandatory fees only later in the buying process), hidden subscription or forced continuity (e.g., unexpectedly charging recurring fees after a free trial ends), or intermediate currency (e.g., hiding real costs by asking users to pay in virtual currency);
- **Interface interference**, or misdirection, false hierarchy or pressured upselling, disguised ads, or bait and switch;
- **Coerced action**, or unauthorized transactions, auto-play, nagging, forced registration or enrollment, pay-to-play or grinding (e.g., making a free version so painful that a user pays for upgrades), friend spam, social pyramid schemes, or address book leeching (e.g., making users share

[16] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proceedings of the ACM on Human-Computer Interaction Vol. 3, Issue CSCW (Nov. 2019).

[17] Jameson Spivack, *Manipulative and Deceptive Design: New Challenges in Immersive Environments*, Future of Privacy Forum (Apr. 2024).

[18] *Bringing Dark Patterns to Light,* FTC (Sept. 2022).

[19] *Id.* at 4, 7, 10, 15.

contacts information); and

- **Asymmetric choice**, or trick questions, confirm sharing, preselection, or subverting privacy preferences (e.g., using confusing wording or shame to steer users toward certain choices).[20]

Beyond the United States, the UK Competition and Markets Authority published a discussion paper in April 2022 on what it called "online choice architecture."[21] The paper scoped online choice architecture to include design decisions that can be beneficial to consumers or harmful to them, the latter category encompassing "sludge," or friction such as barriers to cancellation, "dark patterns," such as drip pricing, and "dark nudges," such as subscription traps.[22] It further broke down online choice architecture into three buckets: choice structure, or how choices are presented to consumers; choice information, or the information provided to consumers when presenting choices; and choice pressure, or how consumers' choices may be indirectly influenced.[23] A European Commission report from that same year, to give another example, identified the five most prevalent dark patterns on 97% of the most popular websites and apps used by EU consumers: hidden information/false hierarchy, preselection, nagging, difficult cancellations, and forced registration.[24]

[20] *Id.* at 21-26.

[21] UK Competition & Markets Authority, *Online Choice Architecture: How Digital Design Can Harm Competition and Consumers*, UK Competition & Markets Authority (Apr. 2022)

[22] *Id.* at 16.

[23] *Id.* at 14.

[24] European Commission Directorate General for Justice and Consumers, *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation,* European Commission Directorate General for Justice and Consumers (Apr. 2022).

Legal Summary

Twenty-one U.S. states[25] have passed privacy legislation that enshrines consumer rights to opt out of certain types of collection, sale, and/or sharing of their personal data. The state laws vary in their approach to opt-out rights, and the specific provisions included in each state privacy law are included in Appendix A.

Most of the laws include the right to opt out of the sale and sharing of personal information and the right to opt out of the use of personal information for specific purposes like targeted advertising or profiling. All 21 laws include requirements for business to provide clear and conspicuous disclosures about consumers' opt-out rights and to ensure that the opt-out process is easy to use by the average consumer. The opt-out provisions also generally include other specific requirements related to the ease of use of opt-out processes. For example, California, Colorado, and New Jersey require that the opt-out preference signal must be "consumer friendly, clearly described, and easy to use." Similarly, Maryland law requires the opt-out process to "use clear, easy to understand, and unambiguous language." Further, state law provisions related to opt-out rights also often require businesses to provide a link to the opt-out page on the website homepage and within the privacy notice.

The presence of any manipulative design in consumer opt-out processes runs afoul of state law. Notably, state privacy laws' opt-out provisions often include exemptions for "publicly available" data,[26] deidentified data, and information regulated by other privacy laws, including credit reporting information, financial information subject to the Gramm-Leach-Bliley Act, health data, and education data. Some state attorneys general or other officials have recommended changes to these exemptions, however, such as the Connecticut Office of the Attorney General recommending the state legislature narrow the "publicly available" information exception, such as to cover data brokers collating information into

[25] Including Alabama, California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia.

[26] Defined by California law, for example, as "(I) Information that is lawfully made available from federal, state, or local government records; (II) 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; (III) 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. Cal. Civ. Code § 1798.140(v)(2)(B).

consumer profiles that they sell.[27] If a company that falls within the scope of state privacy laws collects and processes only exempted data, it may not be required to honor consumer opt-out requests, but covered companies must comply with opt-out requirements if they collect any non-exempt information or make inferences using exempted data that are reasonably linkable to an individual.

Twelve states[28] also require companies to honor universal opt-out mechanisms, which are tools that consumers can use to automatically indicate their preference to opt out of the sale or disclosure of their personal information with all online companies they encounter while browsing the web. The Global Privacy Control (GPC) is the leading universal opt-out mechanism. Several browsers and browser extensions incorporate the GPC to send an opt-out signal to each website visited by someone with a GPC-enabled browser or browser extension.[29] There are a variety of other universal opt-out mechanism tools available to consumers, too, and they usually operate as browser extensions or smartphone apps.[30] Universal opt-out mechanisms make opting out much easier for consumers because instead of going through the opt-out process for every website, consumers can install a universal opt-out mechanism tool one time that will allow them to automatically opt out of sale and disclosure for all online companies they encounter. However, not every state requires companies to honor opt-out requests from universal opt-out mechanisms, so companies can legally ignore these opt-out requests from consumers in most states. Given that not all consumers install universal opt-out mechanisms and that only a subset of states make universal opt-out mechanisms legally enforceable, our analysis focuses only on the opt-out processes provided by individual companies' websites (not what may or may not happen when a consumer visits one of these websites with a universal opt-out mechanism enabled).

At the federal regulatory level, the FTC's 2022 report on dark patterns details how the use of dark patterns may violate Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices [UDAP] in or affecting commerce."[31] The

[27] Connecticut Office of the Attorney General, *Updated Enforcement Report Pursuant to Connecticut Data Privacy Act, Conn. Gen. Stat. § 42-515, et seq*, 12 (Apr. 17, 2025).

[28] Including California, Colorado, Connecticut, Delaware, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, and Texas.

[29] *About*, Global Privacy Control (last visited May 6, 2026).

[30] Samuel Adams & Stacey Gray, *Survey of Current Universal Opt-Out Mechanisms*, Future of Privacy Forum (Oct. 12, 2023).

[31] FTC, *supra* note 18.

report details FTC enforcement actions against companies that utilized dark patterns to deceive or manipulate consumers. Further, the FTC also published an enforcement policy statement in October 2021 on illegal dark patterns.[32] While it focused on dark patterns that trick or trap consumers into subscriptions, several elements of the policy statement may be abstracted as principles that could apply to opt-out paths, too. This includes sentences in the FTC's (again, subscription-focused) enforcement policy statement such as:

- "In any communication using an interactive electronic medium, such as the Internet or software, the disclosure should be unavoidable. A disclosure is not clear and conspicuous if a consumer needs to take any action, such as clicking on a hyperlink or hovering over an icon, to see it."[33]
- "The disclosure should use diction and syntax understandable to ordinary consumers and should appear in each language in which the representation that requires the disclosure appears."[34]
- "For all telephone and other oral offers, the disclosures should not contain any other information that interferes with, detracts from, contradicts, or otherwise undermines the ability of consumers to understand the disclosures, including any information not directly related to the material terms and conditions of any negative option feature."[35]

[32] *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*, FTC (Oct. 28, 2021).

[33] *Enforcement Policy Statement Regarding Negative Option Marketing*, FTC, 11 (Oct. 2021).

[34] *Id.* at 12.

[35] *Id.* at 13.

Methodology

We proceeded in two parts: 1) identifying the 38 companies to investigate and 2) building a literature review- and state law-driven methodology to scan websites, systematically map evidence of manipulative design practices or a lack thereof, and combine the coded data to enable analysis. For this report, we focused on the processes by which companies enable consumers to opt out of the sale and transfer of their personal data because this aligns with opt-out rights included in most of the state privacy laws detailed in the previous section.

Companies

We identified companies for the website scans by first coming up with categories of data-collecting and -transmitting entities whose activities create particular risks to privacy and physical safety, including for populations that are increasingly at-risk for doxxing and targeted violence, like public servants as well as targets and survivors of stalking and gendered violence (predominantly impacting women, women of color, LGBTQ+ people, and children). We focused mostly on larger companies but strove for some variation in market cap as well as type of data business (e.g., data advertising, data sale, surveillance tooling) and type of data at issue (e.g., social media, credit, location, public records).

Using these three criteria—market cap, type of data business, and type of data collected and used—and an emphasis on data that can put people at particular privacy and physical safety risk, we identified the following 38 companies to scan:

Company Category	Total Number	Company Names
Data Brokers	15	Acxiom, Experian, TransUnion, Equifax, Epsilon, Cotality (formerly CoreLogic), Spokeo, Whitepages, LiveRamp, National Public Data, Venntel, Unacast (formerly Gravy Analytics), X-Mode/Outlogic, Near Intelligence, Nielsen
Social Media	4	Meta (incl. Facebook, Instagram), Google (incl. YouTube), TikTok, X
Other Big Tech	9	Uber, Lyft, OpenAI, Anthropic (Claude), Google (Gemini), Meta (Llama), Mistral AI, Tesla, Amazon

Company Category	Total Number	Company Names
Surveillance Tech Vendors	6	Palantir, Clearview, DataTrust, Flock, SoundThinking (formerly ShotSpotter), Hirevue
Dating Apps	4	Grindr, Tinder, Bumble, Hinge

Reviewing for Manipulative Design Practices

We developed a methodology for how we would review the identified companies' websites by creating a list of manipulative design criteria, then creating a review process for us to carry out independently, and then conducting reviews and comparing our respective findings.

First, we came up with manipulative design criteria drawing on four sources: (1) the academic literature on manipulative design practices; (2) prior FTC guidance and regulatory actions related to manipulative design practices; (3) state laws' language related to manipulative design practices; and (4) the criteria, based on our own experience and work, most relevant to opt-out paths, manipulative design practices, and consumer privacy, especially for individuals who are particularly vulnerable and/or at risk of physical violence.

Initial Criteria Source	Initial Criteria Identified
Literature Review	• Account is required to use service at all • Location sensed by default without asking consent • No bulk options for settings • Setting changes do not actually save • No logout option if login was possible • No account deletion option if account creation was possible • Account deletion options are time delayed • General pop-up nags • Provocative text to shame or guilt people into certain behavior • Confusing text, like double negatives, or verbally confusing toggles • Some options are given visual precedence over others, e.g., larger buttons • Checkbox options are preselected

Initial Criteria Source	Initial Criteria Identified
Prior FTC Guidance and Actions	• Design elements that induce false beliefs • Design elements that hide or delay disclosure of material information • Design elements that lead to unauthorized changes • Design elements that obscure or subvert privacy choices
State Laws' Requirements	• Consumer has the right, at any time, to opt out of sale/sharing • "the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer" • Businesses' opt-out procedures must clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent • The opt-out method is clearly and conspicuously linked in any privacy notice required to be provided to consumers, and provided in a clear, conspicuous, and readily accessible location outside the privacy notice • Opt out mechanism "clearly communicates a consumer's affirmative, freely given, and unambiguous choice to opt out"

Initial Criteria Source	Initial Criteria Identified
Our Additional List	• Confusing language • Abuse of defaults — e.g., pre-checked selection options that push a user to limit the scope of an opt-out by leaving certain settings checked or unchecked • Forcing a user to create an account unnecessarily • Scary language (e.g., unnecessarily scary language about fraud/need to ID verify) • Having multiple opt-out pages/channels that are each different depending on type of data opt-out or some other criteria, forcing consumers who want to utilize all available opt-out options to find and navigate through multiple pages/ paths • Deceptive statements about what opt-outs will or will not do/how well the company effectuates a user request/submission • Opt-out page is not clearly linked from website homepage (including menu or footer)

Then, we converted the above criteria into the below list to guide our review throughout the opt-out process for each company's website. The final criteria were:

- **Account required** to use service at any phase of opt-out process
- **Location sensed by default** without asking consent
- **No bulk setting options** — i.e., no ability to toggle all options on/off at once
- **Setting changes don't save** from one phase to the next
- **No logout after logging in**, if login is possible
- **No account deletion after creation**, if account creation is possible
- **Account deletion options are time-delayed**, if account creation is possible
- **General pop-up nags** at any phase of opt-out process

- **Provocative text to shame or guilt people into certain behavior** at any phase of opt-out process
- **Confusing text or verbally confusing toggles** at any phase of opt-out process — e.g., double negatives
- **Some options given visual precedence over others** at any phase of opt-out process — e.g., larger buttons
- **Checkbox options preselected** at any phase of opt-out process
- **Design elements inducing false beliefs** at any phase of opt-out process
- **Design elements hiding or delaying disclosure of material information** at any phase of opt-out process
- **Design elements leading to unauthorized changes** at any phase of opt-out process
- **Design elements obscuring or subverting privacy choices** at any phase of opt-out process
- **Confusing language** at any phase of opt-out process
- **Abuse of defaults** at any phase of opt-out process — e.g., pre-checked selection options that push a user to limit the scope of an opt-out by leaving certain settings checked or unchecked
- **Scary language** at any phase of opt-out process — e.g., unnecessarily scary language about opting out causing a fraud risk to you or needing to submit several forms of ID to verify a request
- **Multiple, separate processes needed for full opt-out** —e.g., having multiple opt-out pages/channels that are each different depending on type of data opt-out or some other criteria, forcing consumers who want to utilize all available opt-out options to find and navigate through multiple pages/paths
- **Deceptive statements about opt-outs and their success** at any phase of opt-out process — e.g., misleading representations of what an opt-out request will or will not do, or how well the company effectuates to a user request

- **Opt-out page not clearly linked from homepage** (including menu or footer)
- **Opt-out page not clearly linked from privacy policy**
- **Opt-out process is easy to use** — e.g., considering the overall process' (or processes') time, complexity, clarity, etc.

For the review itself, we separately went through the same list of target companies in the same order, navigated to their websites in a clean, or incognito, browser session, located the relevant consumer rights request webpage (by searching for it in a search engine if not clearly or easily locatable), and followed the process through to its near-completion, right before submitting. At every stage of our separate processes, we took notes on the criteria above. We also archived, to the extent possible, the webpages at each distinct phase both online (e.g., via the Internet Archive) and in local screenshots. Once all reviews were completed, we then reconvened to share our respective notes with one another, compare findings, and start producing the analysis.

Analysis

We identified at least eight major manipulative design patterns across a number of the companies' websites. They are the following:

- Failing to provide a clear mechanism to opt out of sale and sharing of personal information
- Not clearly linking opt-out form from homepage and/or privacy policy
- Requiring consumers to submit multiple separate forms
- Deceptive statements about opt-outs and their success
- Confusing or misleading language
- Requiring consumers to log in or pay for a subscription before opting out
- Design elements hiding important opt-out information (including design elements inducing false beliefs, hiding or delaying disclosure of material information, or obscuring or subverting privacy choices)
- Checkbox options preselected

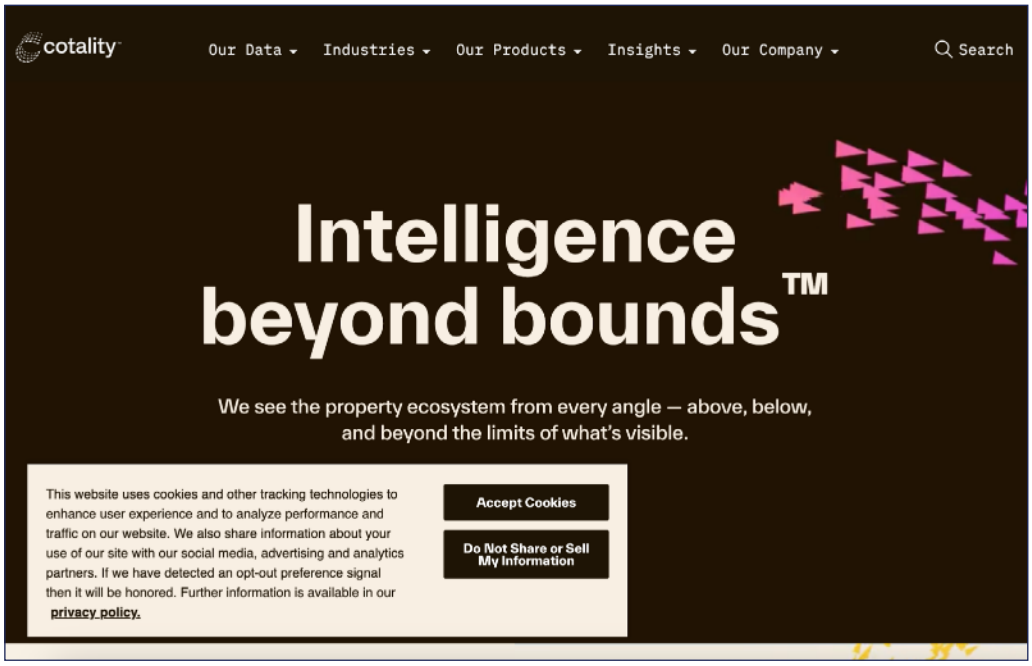
We also identified several other, overall trends (not necessarily manipulative). For example, some companies used the same third-party vendor to power their opt-out form or webpage. Several companies, primarily the location data brokers, required consumers to submit mobile advertising identifiers to opt out. Many websites are also difficult to archive on services such as the Internet Archive, raising critical transparency and accountability questions given their prominent data businesses. Note that below, where we say "at least" in front of a number of companies that had a certain design practice, this is because we had some issues with various companies' websites (e.g., broken links, unclear if they had opt-out forms, etc.). This suggests that the actual number might be higher.

Overall Trends (Not Necessarily Manipulative)

Before describing the manipulative design patterns we found, we note some trends observed across many of the target companies' website opt-out processes. Sixteen of the companies we reviewed utilize a form that allows consumers to indicate their choice to opt out of the sale and sharing of their personal data and other types of data collection, processing, and transferring. Many companies use

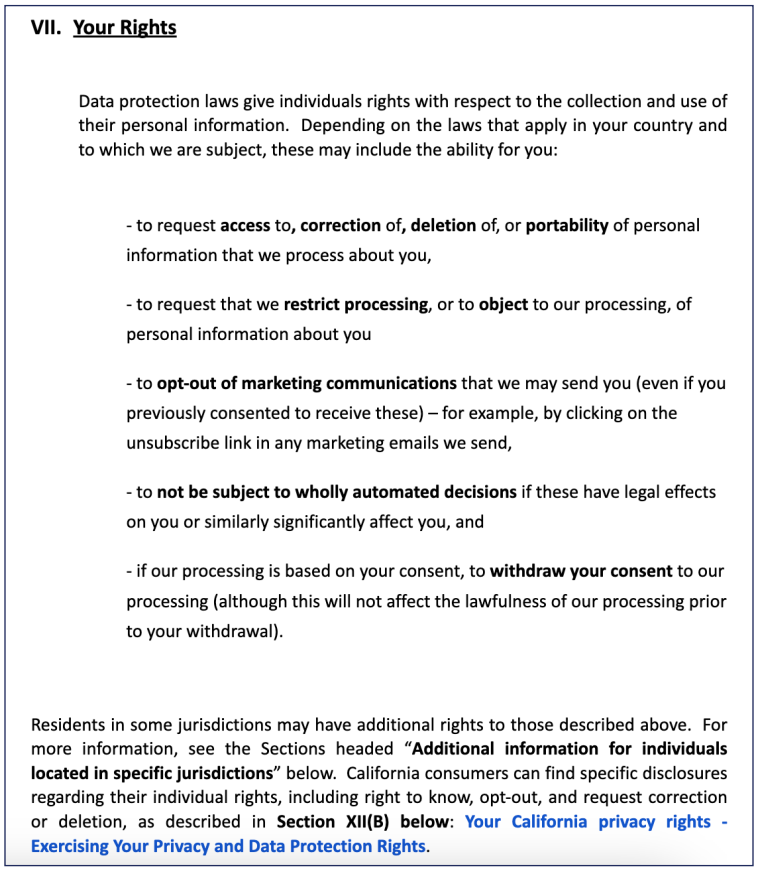
the vendor OneTrust (based on their own website statements or visualizations) to power the form or webpage used to present a website visitor with opt-out settings. Sometimes, a company has a OneTrust form embedded within their webpage, and other times, the company links to an external page that was similarly labeled as being powered by OneTrust.

Four of the companies we reviewed had no form for privacy rights requests, but they each provided instructions about how to opt out of the sale and sharing of personal data. For example, when we navigated to the Cotality website, a pop-up banner, shown below, provided options to either "Accept Cookies" or "Do Not Share or Sell My Information."



Screenshot of Cotality's Homepage, taken April 20, 2026.

Cotality stated that consumers may use an opt-out preference signal such as the Global Privacy Control or contact Cotality via phone or email to exercise opt-out rights. Anthropic also did not provide an opt-out form, but it instructed consumers to exercise their privacy rights by changing privacy settings, rejecting cookies, and enabling global privacy controls. Tesla directed users to exercise opt-out rights by submitting a contact form, emailing Tesla, or mailing a letter. As shown in the screenshots below, HireVue did not have an opt-out form, but it provided an email for California residents to opt out of the sale and sharing of personal information and exercise other California privacy rights. HireVue did not provide instructions to residents of other states to exercise their opt-out rights.



VII. Your Rights

Data protection laws give individuals rights with respect to the collection and use of their personal information. Depending on the laws that apply in your country and to which we are subject, these may include the ability for you:

- to request **access** to**, correction** of**, deletion** of, or **portability** of personal information that we process about you,

- to request that we **restrict processing**, or to **object** to our processing, of personal information about you

- to **opt-out of marketing communications** that we may send you (even if you previously consented to receive these) – for example, by clicking on the unsubscribe link in any marketing emails we send,

- to **not be subject to wholly automated decisions** if these have legal effects on you or similarly significantly affect you, and

- if our processing is based on your consent, to **withdraw your consent** to our processing (although this will not affect the lawfulness of our processing prior to your withdrawal).

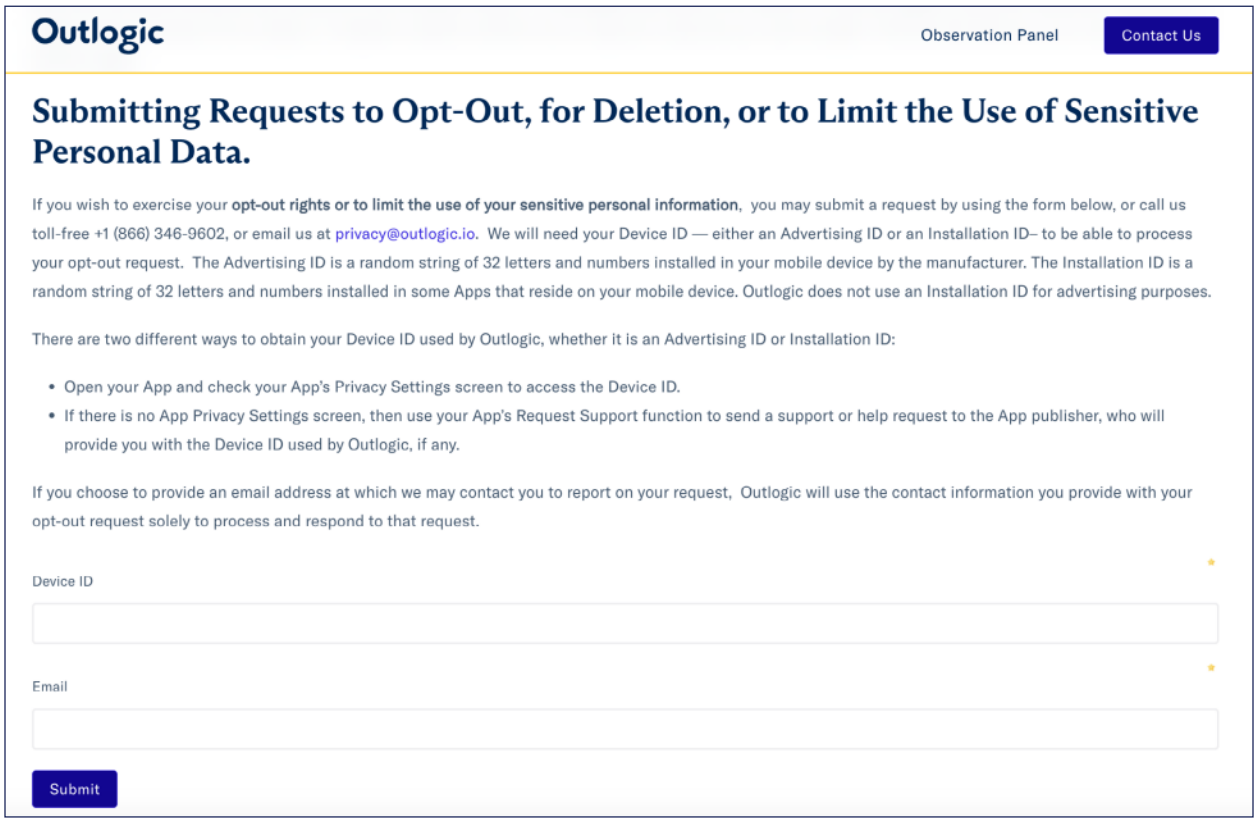
Residents in some jurisdictions may have additional rights to those described above. For more information, see the Sections headed "**Additional information for individuals located in specific jurisdictions**" below. California consumers can find specific disclosures regarding their individual rights, including right to know, opt-out, and request correction or deletion, as described in **Section XII(B) below**: **Your California privacy rights - Exercising Your Privacy and Data Protection Rights**.

Exercising Your California Privacy and Data Protection Rights

To provide, correct, or delete specific pieces of personal information we will need to verify your identity to the degree of certainty required by law. We will verify your request by asking you to send it from the email address associated with your account or requiring you to provide information necessary to verify your account to privacy@hirevue.com. For some types of personal information we may have, such as unauthenticated web browsing data, there is no reasonable method by which we can verify your identity as the person to whom that data relates.

Screenshots of Hirevue's Privacy Policy, taken May 12, 2026

Several of the companies, primarily the location data sellers, required a website visitor to submit their mobile advertising identifier (MAID) to process an opt-out request. In the instances in which the websites required a MAID, they listed instructions within the same webpage for how to do so. For example, the screenshot below shows that Outlogic's opt-out form requires users to submit their Device ID and provides instructions to find your Device ID.



Screenshot of Outlogic's Opt-Out Form, taken May 12, 2026.

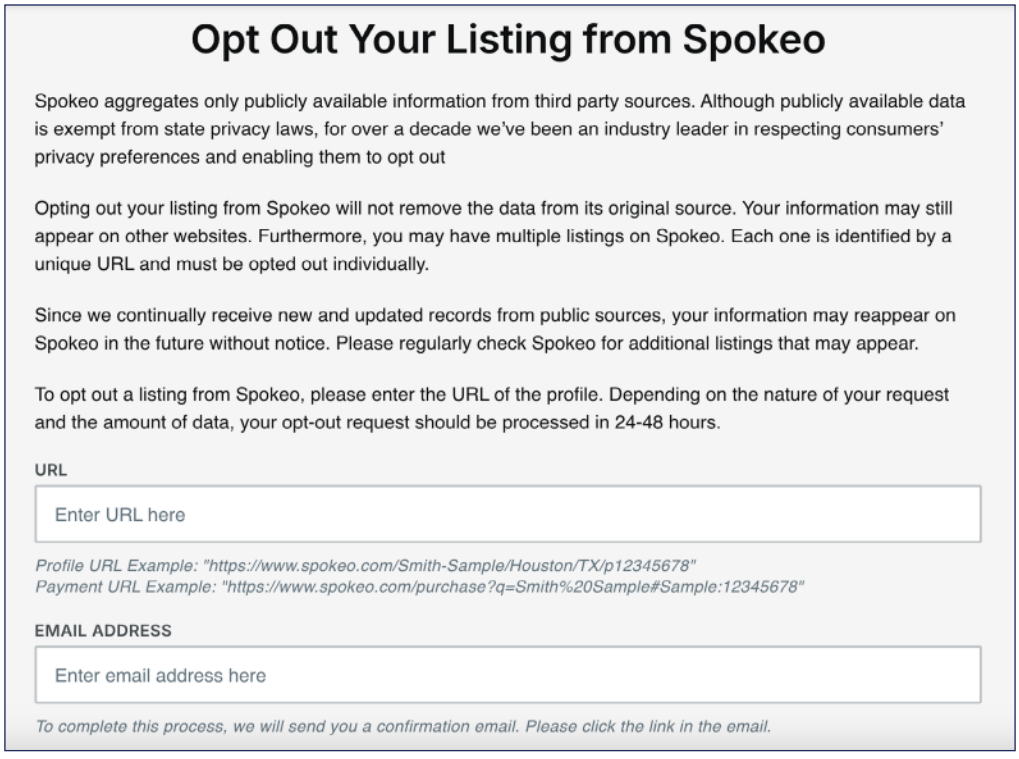
At least 12 companies required the visitor to create an account or log into an account to submit an opt-out form, meaning that 26, based on our tabulation, did not require it. For the websites that did link to the opt-out request form on their homepage, many did so in the footer and titled the link "Your Privacy Choices" rather than "Opt Out" per se. And some websites had state-specific requirements in their opt-out processes, requiring a website visitor to select the state in which they reside in order to show or describe to them particular opt-out options.

On a transparency and accountability note, many of the companies surveyed in this study have websites that are incredibly difficult to archive using popular website archiving platforms, such as the Internet Archive. Many of these archiving issues are most likely driven, in the authors' experience, by security configurations on the companies' websites designed to prevent web scraping, thus prohibiting the tools powering popular website archiving platforms from carrying out their archiving processes of the URLs. These impediments raise transparency and accountability questions when they create barriers to researchers, journalists, and regulators creating clear, public archives of the websites of major corporations. (And there is, of course, the irony of a company involved in mass-scraping

people's data from various websites and other sources, without their actual, full consent, blocking researchers and members of the public from using free tools to capture a virtual screenshot of one of their own webpages.)

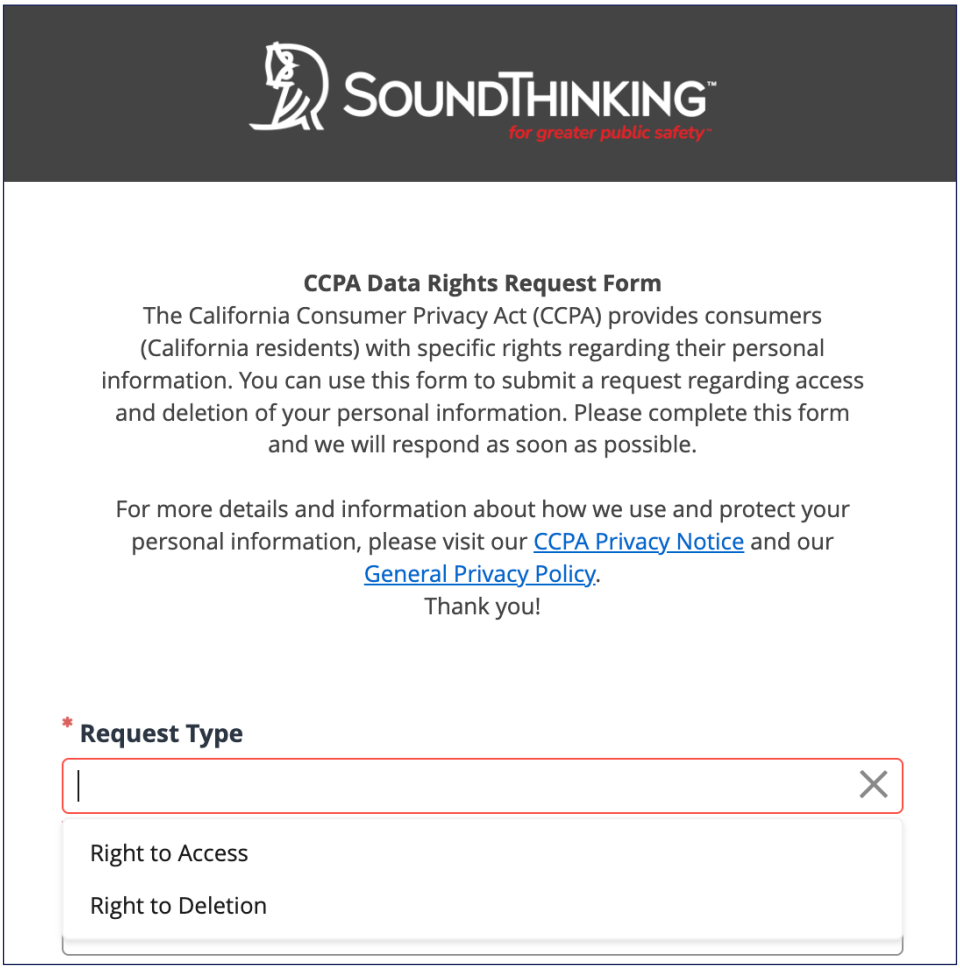
Manipulative Design Pattern: Failing to Provide a Clear Mechanism to Opt Out of Sale and Sharing of Personal Information

Six of the companies we reviewed had a privacy form on their websites, but the form did not specifically provide a choice to opt out of the sale and sharing of personal information. For example, Spokeo, a "people search" data broker, has a privacy form that only allows people to opt out of specific listings on Spokeo, requiring people to provide URLs of specific profiles. As shown in the screenshot below, Spokeo also does not provide any assurances that it will continue to honor opt-out requests in the future, noting "[s]ince we continually receive new and updated records from public sources, your information may reappear on Spokeo in the future without notice. Please regularly check Spokeo for additional listings that may appear." Whitepages, a "people search" data broker, likewise requires consumers to provide the company with a URL to their own profile on the website to fulfill an opt-out request.



Screenshot of Spokeo's Opt-Out Page, taken May 11, 2026.

National Public Data, another "people search" website, also required consumers to provide a link to their profile, but did not indicate whether removing a consumer's profile will opt them out of the sale and sharing of their data in the future. TikTok, Palantir, and Amazon had a privacy form, but none of the forms provided a specific option to opt out of the sale and sharing of personal data. SoundThinking provided a form to opt out of communications from the company and a form for California residents to access or delete their data, as shown in the screenshot below, but the form did not provide an option to opt out of the sale and sharing of personal information.



Screenshot of SoundThinking's CCPA Data Rights Request form, taken April 20, 2026.

Additionally, some of the companies seemed to provide no instructions to opt out of selling and sharing at all, including Meta, X, OpenAI, and Tinder—or at least, the opt-out processes were impossible for us to find without logging in.

Manipulative Design Pattern: Not Clearly Linking Opt-Out Form from Homepage and/or Privacy Policy

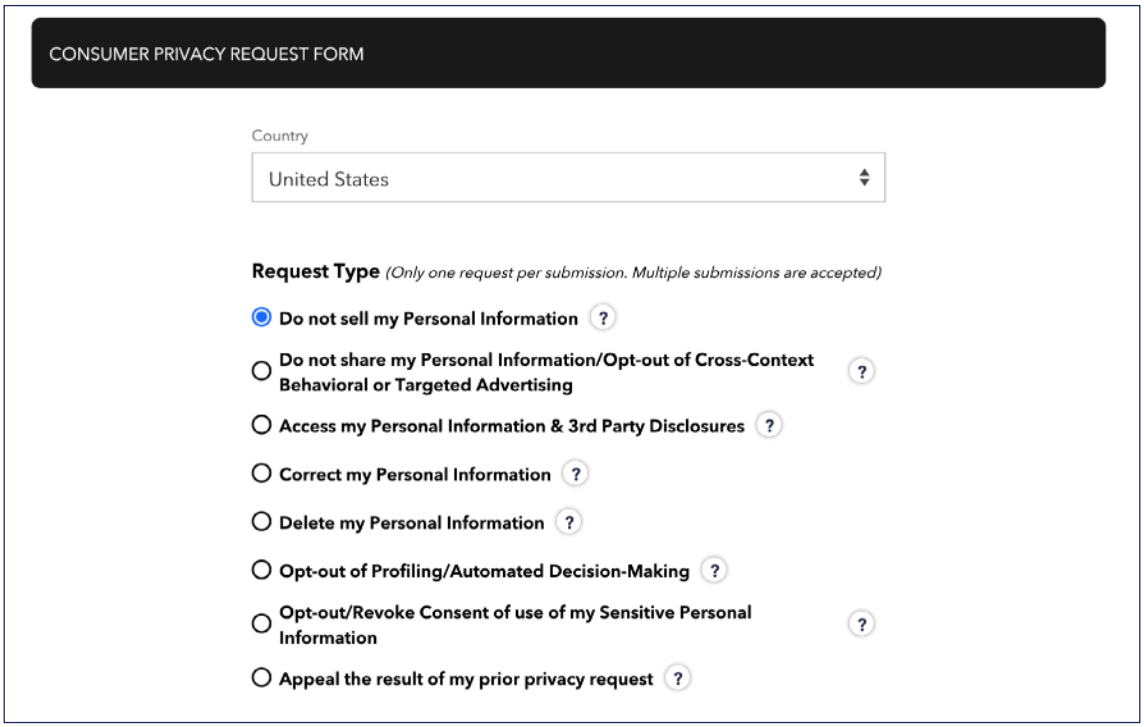
At least 15 of the companies did not clearly link their opt-out form from the homepage: Cotality, Whitepages, Meta, Google, TikTok, X, OpenAI, Anthropic, Google: Gemini, Meta: Llama, Mistral AI, Tesla, Palantir, HireVue, and Tinder.[36] This raises the barrier for consumers visiting a website to exercise their privacy rights. At least 17 of the companies did not clearly link their opt-out form from the privacy policy: Cotality, Liveramp, Meta, Google, TikTok, Lyft, Anthropic, Google: Gemini, Meta: Llama, Mistral AI, Tesla, Amazon, Palantir, HireVue, Grindr, Tinder, and Bumble. Sometimes, the companies failed to include the link at all, and other times, the link may have been included but was labelled unclearly or buried among many other links as to be functionally overwhelming or difficult to understand.

This failure further undermines consumers' ability to easily access pages where they can submit opt-out requests to companies, and may raise questions about companies' compliance with federal and state regulatory requirements. As detailed in Appendix A, state privacy laws typically require companies to include clear and conspicuous directions for consumers about how to opt out on the homepage and within the privacy policy. When companies fail to provide clear links to the opt-out page or other opt-out instructions, they are not only making it harder for consumers to opt out, but they also may be violating state privacy laws.

Manipulative Design Pattern: Requiring Consumers to Submit Multiple Separate Forms

At least 15 of the companies required consumers to submit multiple separate forms to fully opt out: TransUnion, Epsilon, Cotality, Spokeo, Whitepages, National Public Data, Outlogic, Meta, Google, Open AI, Anthropic, Google: Gemini, Mistral AI, Nielsen, and DataTrust. For example, the data brokers Epsilon and LiveRamp required a website visitor to submit multiple forms in order to achieve the full scope of opt-outs offered. As shown below, Epsilon only allowed consumers to select one request type per form submission, and "Do not share" and "Do not sell" required separate submissions.

[36] This includes one company whose opt-out link on the homepage did not work and a few companies whose opt-out links on the homepage were California-specific, therefore failing to meet the criteria.



Screenshot of Epsilon's Consumer Privacy Request Form, taken April 20, 2026.

This practice raises the barrier to consumers exercising their rights by increasing the amount of time and effort required to submit privacy requests. Telling consumers up front that only one request type can be submitted at a time may appear to offer transparency, but this practice can create a disincentive for consumers to go through with submitting said forms. Instead of enabling consumers to quickly exercise all of their privacy rights, requiring multiple form submissions effectively operates as another barrier for consumers to easily and quickly submit opt-out requests.

Related to this manipulative design practice, although in some ways distinct, we also observed several websites that did not appear to offer a bulk setting option in an opt-out path. This means, for example, that someone opting out of the collection of multiple data types would have to go down a list and manually check each of them, with no option to "Select All."

Manipulative Design Pattern: Deceptive Statements About Opt-Outs and Their Success

At least 14 of the companies did not clearly, explicitly state the limits of the opt-outs they offered, such as not explaining to consumers in a clear, understandable way that the companies may only allow consumers to opt out of various data

practices to the extent afforded to the consumer by a state law. For example, TransUnion, like many other companies, does not explicitly state to the user that there may be constraints on the scope of their opt-out requests (e.g., in line with FCRA rules or the fact that state privacy laws exempt public records from opt-out rights and requests). Whitepages.com states, "Please be aware that we do not have the ability to hide your information on databases we don't control, such as public records." While an important clarification, this language does not make clear to the visiting consumer that the broker could choose to stop ingesting someone's data from a public record even if it was available. And OpenAI, to give another example, fails to explicitly state the limit of its opt-out processes, including not clarifying in plain language to the consumer that the company may very well have already collected their personal information as part of scraping data to train its models—and will not remove any of that data from its systems, even if it could be filtered out of chatbot responses to queries.

Manipulative Design Pattern: Confusing or Misleading Language

Over 20 of the companies we reviewed included some kind of confusing language in their opt-out processes. First, we often encountered confusing language when determining whether the opt-out process provided by companies would actually allow consumers to opt out of the sale and transfer of personal information. For example, Spokeo, Whitepages, and National Public Data, all "people search" data brokers, have processes for consumers to remove listings about themselves from the sites, but it is unclear if removing public listings about you also opts you out of the sale and transfer of your data. Some, such as Whitepages, discuss public records as if the companies do not have any choice but to continue ingesting public records and selling the related data and consumer profiles.

Second, sometimes companies' opt-out form or privacy form did not provide a clear option to opt out of the sale and transfer of personal data. For example, TikTok's privacy form had a drop down list requiring individuals to select a type of privacy request, and none of the options provided a choice to opt out of sale or transfer of personal data. Similarly, OpenAI's form did not provide a specific choice to opt out of sale or transfer, but it only allowed consumers to "remove personal information from ChatGPT responses." Epsilon's displayed list of opt-out and data request options, as shown in the screenshot above, is quite confusing, with overlapping terms and options that overwhelm the consumer. TransUnion, despite providing consumers with an opt-out form, also stated that companies it

owns require their own, separate opt-out forms, and its privacy policy does not clearly explain to consumers how exercising their "privacy rights" differs from submitting opt-out requests, insofar as it lists the two as distinct categories. Many sites fail to make similar distinctions clear. DataTrust's privacy policy was laid out in a confusing fashion, such as by suggesting to consumers higher up in the privacy policy that their privacy rights are constrained to certain areas (e.g., Global Privacy Control) before later down listing several rights that apply in several states.

Even worse, some companies include misleading language in their opt-out process that suggests that opt-outs themselves will not even work to delete their personal information from public websites. For example, Spokeo's opt-out page includes the following disclaimers:

> "Spokeo aggregates only publicly available information from third party sources. Although publicly available data is exempt from state privacy laws, for over a decade we've been an industry leader in respecting consumers' privacy preferences and enabling them to opt out
>
> Opting out your listing from Spokeo will not remove the data from its original source. Your information may still appear on other websites. Furthermore, you may have multiple listings on Spokeo. Each one is identified by a unique URL and must be opted out individually.
>
> Since we continually receive new and updated records from public sources, your information may reappear on Spokeo in the future without notice. Please regularly check Spokeo for additional listings that may appear."

This language is discouraging to consumers seeking to opt out from Spokeo data sales or transfers. First, the disclaimers seem to indicate that Spokeo is not legally required to process opt-out requests, which may not necessarily be true.[37] The disclaimers also state that consumers must find all the URLs with information about themselves and then continually monitor Spokeo to see if information

[37] Note: Spokeo states that it only shares publicly available data, making it exempt from certain state privacy law requirements. However, Spokeo states that its reports include information beyond what would likely qualify as "publicly available" data (as in, derived from public records), including data like estimated salary, language proficiency levels, and information on hob bies, interests, lifestyle, travel, fitness, and collections. *What Services Does Spokeo Offer?*, Spokeo (Sept. 24, 2025).

reappears. Spokeo's disclaimers make it seem like submitting an opt-out request to Spokeo is a waste of time instead of empowering consumers to exercise their privacy rights. Many people may need to remove their information from Spokeo for safety reasons, such as domestic violence survivors or public officials and their families. By providing such a burdensome and unreliable opt-out process, and by making such seriously slanted statements to consumers, Spokeo may put people's physical safety at further risk.

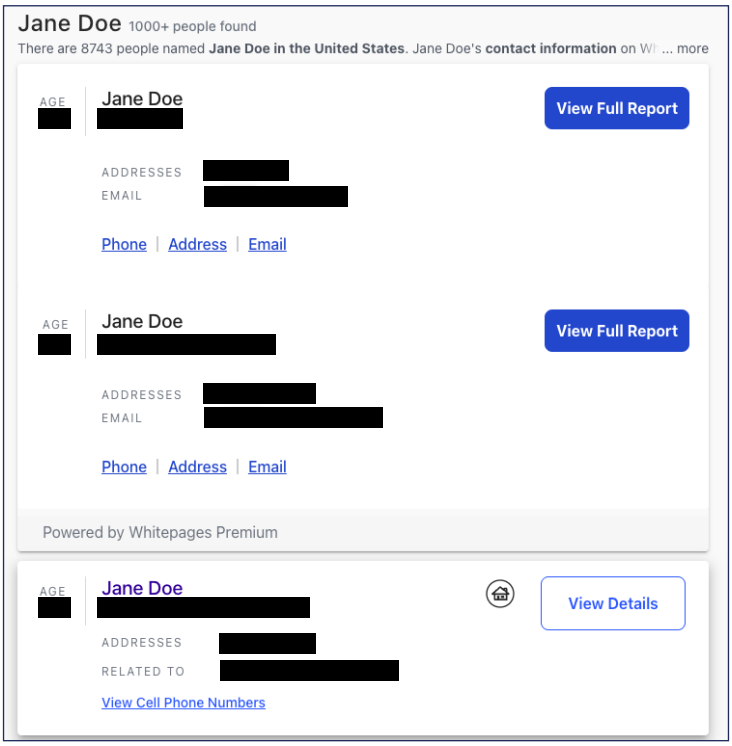
The inclusion of confusing language reduces the likelihood that consumers will understand and be able to complete the opt-out process, and the use of misleading language may discourage consumers from even trying to opt out. State privacy laws require companies to provide clear, conspicuous, and accessible opt-out processes, and the use of confusing or misleading language does not comply with these requirements.

Manipulative Design Pattern: Requiring Consumers to Log In or Pay for a Subscription Before Opting Out

At least 11 of the companies we reviewed required consumers to log in or even pay for a subscription before opting out, including Whitepages, Meta, Google, X, Uber, Lyft, OpenAI, Google: Gemini, Meta: Llama, Mistral AI, and Tinder. Requiring users to log in to an account introduces friction to the opt-out process by making the process more lengthy and extensive, but it may also present a barrier to the process for privacy-conscious consumers. If consumers want to make sure these companies do not sell or transfer any information about them, they likely do not want to create an account, which requires sharing certain information with the company and agreeing to the company's terms of use. While many state privacy laws permit companies to require existing users to log in before submitting an opt-out request, some of the literature on deceptive designs classifies the mandatory use of an account as a manipulative design pattern. The only opt-out processes we could find for the 12 companies listed above required that the visitor log into an account, even if that meant creating one.

Whitepages' opt-out process requires individuals to input the URLs of specific profiles containing information about themselves. However, when you search your name on Whitepages, you may have to pay for a Whitepages subscription to view the full report about yourself. The screenshots below show that when you search for a name on Whitepages, the first results are in a box labelled "Powered by Whitepages Premium." If you click "View Full Report," you are directed to a page

to pay for a Whitepages premium subscription before viewing the report. The next results in the list can be opened without paying for a subscription by clicking "View Details." Whitepages hides some of the pages behind a paywall, effectively requiring consumers to pay to navigate to certain pages with their own information before they can fully opt out all listings about themselves, including the full reports available to Whitepages Premium members. This introduces a financial barrier to the opt-out process, as well as being time-intensive.

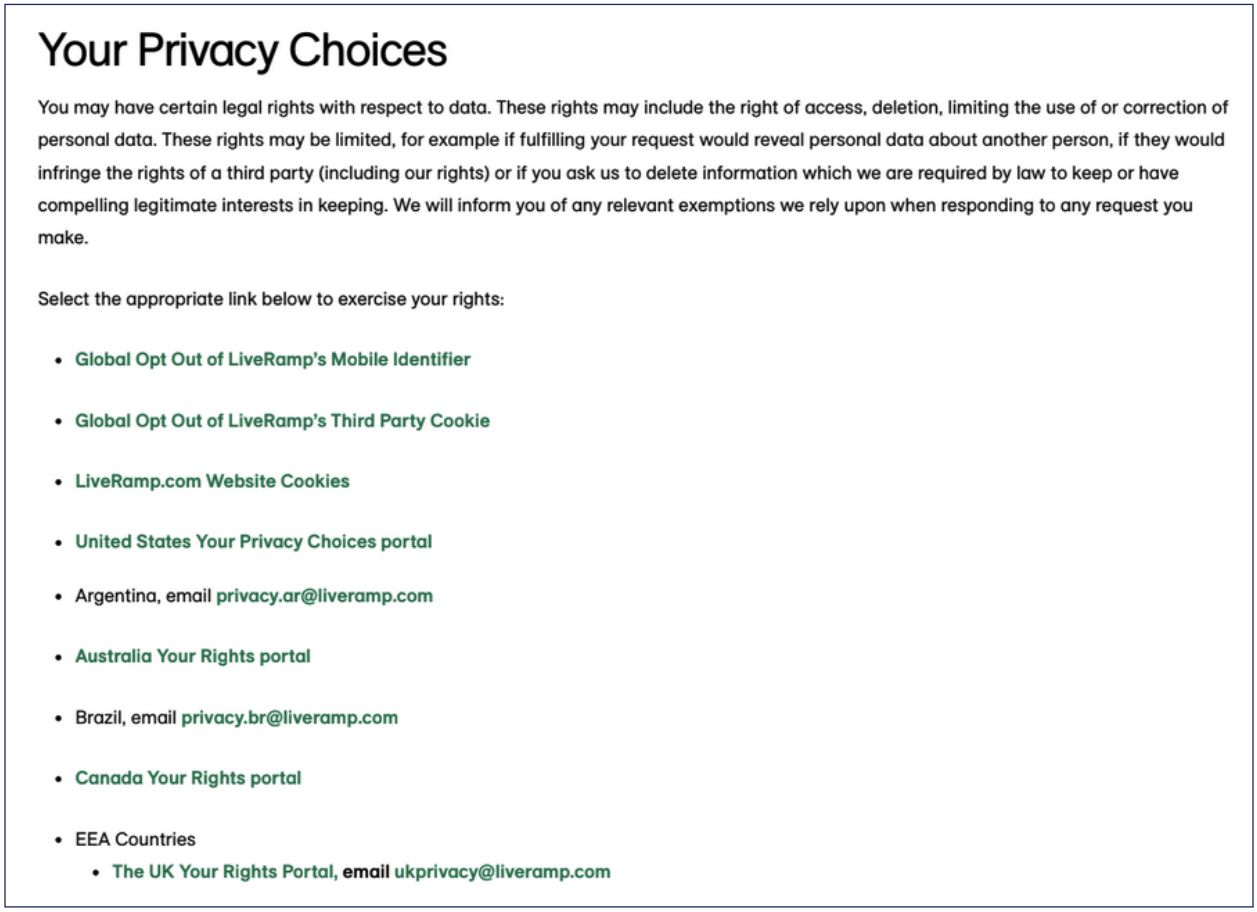


Redacted screenshot of Search Results for "Jane Doe" on Whitepages.com, taken May 12, 2026.

Manipulative Design Pattern: Design Elements Hiding Important Opt-Out Information (including Design Elements Inducing False Beliefs, Hiding or Delaying Disclosure of Material Information, or Obscuring or Subverting Privacy Choices)

Many of the companies we reviewed used manipulative design elements that induce false beliefs, hide or delay the disclosure of material information, or obscure or subvert consumers' privacy choices. For example, as described above, Whitepages did not allow consumers to see the full profile about themselves without paying for a subscription. By hiding information from consumers, Whitepages made it effectively impossible for consumers to fully opt out. In doing so, it suggested to the consumer that they should pay the company selling their

personal data, potentially without their actual consent to begin with, in order to opt out from its continued sale. LiveRamp also had an overly confusing opt-out process, especially if a consumer tries to navigate it by visiting the website, by making the consumer manually click each individual expansion button on the "Your Privacy Choices" page to see all the information, only to then require the consumer to click on every "choice" separately to learn more or initiate the process in question.



Your Privacy Choices

You may have certain legal rights with respect to data. These rights may include the right of access, deletion, limiting the use of or correction of personal data. These rights may be limited, for example if fulfilling your request would reveal personal data about another person, if they would infringe the rights of a third party (including our rights) or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping. We will inform you of any relevant exemptions we rely upon when responding to any request you make.

Select the appropriate link below to exercise your rights:

- **Global Opt Out of LiveRamp's Mobile Identifier**
- **Global Opt Out of LiveRamp's Third Party Cookie**
- **LiveRamp.com Website Cookies**
- **United States Your Privacy Choices portal**
- Argentina, email **privacy.ar@liveramp.com**
- **Australia Your Rights portal**
- Brazil, email **privacy.br@liveramp.com**
- **Canada Your Rights portal**
- EEA Countries
  - **The UK Your Rights Portal, email ukprivacy@liveramp.com**

Screenshot of LiveRamp's Privacy Policy, taken March 8, 2026.

All of these smaller design elements build up to create more friction for consumers attempting to exercise their legal rights or simply inform a company of their non-consent to sell or transfer data.

Additionally, some of the companies seemingly provided no form or instructions to opt out of selling and transferring personal data, including Spokeo, Whitepages, National Public Data, Amazon, Meta, X, OpenAI, Palantir, TikTok, SoundThinking, and Tinder, or at least the opt-out processes were impossible for us to find without logging in. By failing to clearly tell consumers how to opt out, companies hide

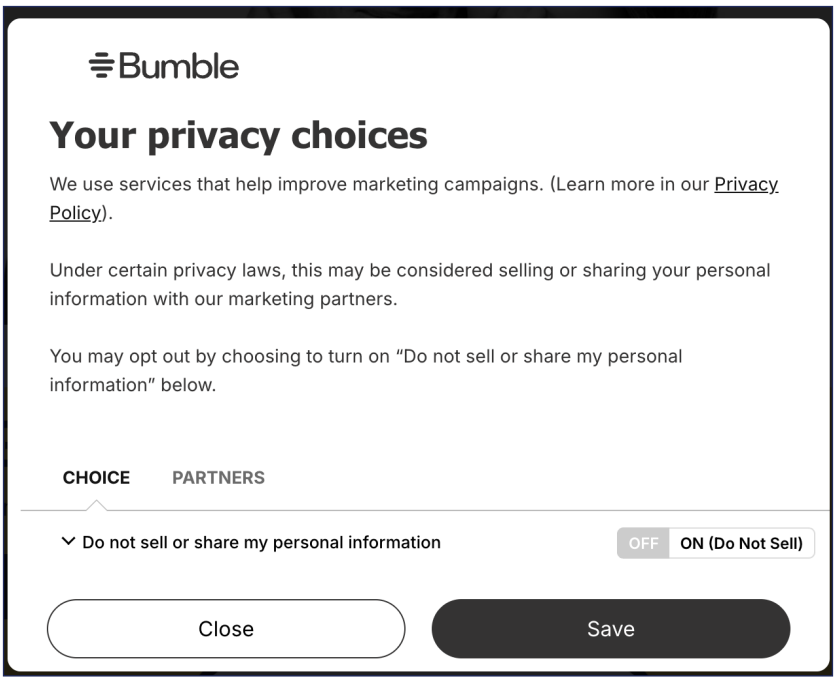
information that they are legally required to share with consumers about how to opt out, and they also obscure consumers' privacy rights. Some of the companies, including HireVue, provided instructions for California residents to opt out of sale and sharing, but they failed to provide opt-out instructions to residents of other states. This could cause a consumer to falsely believe that only Californians have opt-out rights, even though many other states have passed privacy laws that include opt-out rights. Other websites, as mentioned, such as DataTrust, broke out the states' rights in such a way that consumers may only see California first and then wrongly think they do not have rights in other states—because that information was buried lower down on the webpage.

Manipulative Design Pattern: Checkbox Options Preselected

Four companies' opt-out processes included checkboxes with preselected options: Uber, Lyft, Grindr, and Bumble. When navigating through the opt-out process, a checkbox or toggle displays the opt-in option as the default, and consumers must click the toggle or checkbox to opt out. Preselected boxes or toggles are considered manipulative design patterns because consumers may experience the default effect cognitive bias when encountering preselected boxes or toggles.[38] Preselection introduces friction into the opt-out process because users must notice the preselected box and understand that the box or toggle needs to be changed to effectuate their opt-out choice.[39]

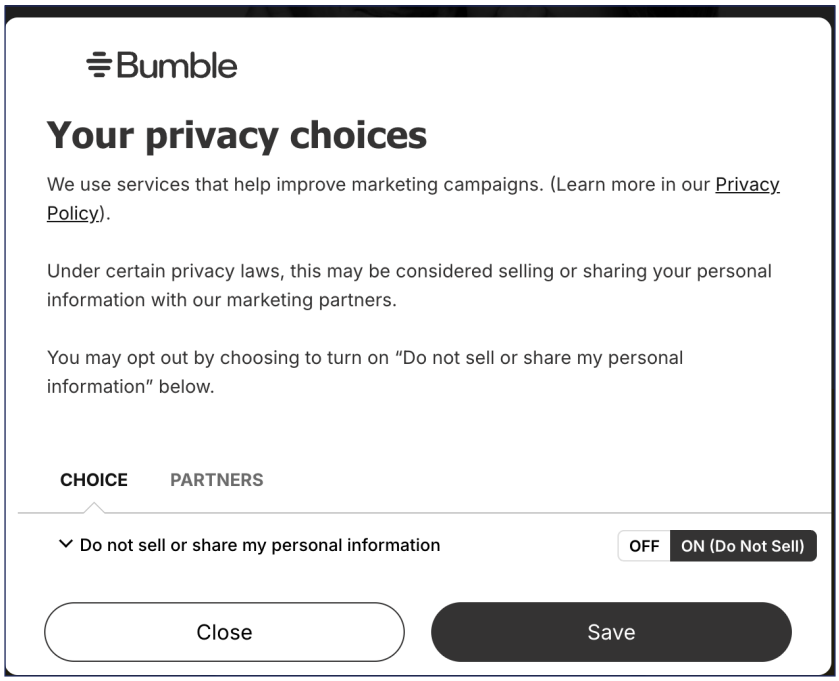
Sometimes, companies even use confusing colors or designs alongside preselected toggles that may make it difficult for consumers to understand whether they are opted in or out. For example, Bumble's opt-out process used a preselected toggle. The default option was for consumers to be opted in to allow Bumble to sell or share their personal information. Bumble's opt-out pop-up is shown below. When "Do not sell or share my personal information" is set to the default "OFF" position (which means the user is opted in to selling and sharing), the "OFF" option is greyed out and the "ON (Do Not Sell)" option is white with black letters.

[38] *Preselection*, Deceptive Patterns (last visited Apr. 15, 2026).
[39] *Id*.



Screenshot of Bumble's "Your Privacy Choices" pop-up, taken April 15, 2026.

In contrast, when the consumer clicked on toggle, the "ON (Do Not Sell)" option is black with white letters while the "OFF" option is white with black letters, as shown below.



Screenshot of Bumble's "Your Privacy Choices" pop-up, taken April 15, 2026.

Bumble's toggle design choices were not intuitive. Consumers may assume that they are already opted out when the "OFF" option is grayed out and the "ON (Do Not Sell)" option is shown as white with black letters, but in fact, this toggle position indicates that users are opted in. Included preselected boxes or toggles introduces friction into the opt-out process and also introduces an opportunity for consumer confusion when design and color choices are not clear.

Conclusion

Despite the growing swath of states passing privacy legislation that requires companies to provide clear, easy-to-use, and accessible opt-out mechanisms to allow consumers to opt out of the selling and sharing of their personal information, many companies—even large companies with significant resources—still fail to provide opt-out processes that are free from manipulative design. When companies use manipulative design practices, the opt-out process only becomes more time-consuming and confusing for consumers, making the barrier to exercising opt-out rights even higher. In some cases, companies used so many manipulative design tactics that many consumers would likely not be able to exercise their opt-out rights at all.

This is a serious problem, particularly for individuals at risk of violence. Certain people, such as local public servants or federal civil servants who may be doxxed and swatted; survivors of gendered violence and their children; targets of stalking; and other people subject to targeting and violence based on their personal data are under a time crunch—often, life-or-death—to get their home address and other information removed from as many websites and company databases as possible. It is important for their physical safety to ensure that relevant data is removed from data broker websites and ceases to be shared efficiently and effectively. As evidenced above, however, many companies fail to make their opt-outs easy to use and effective. Such design decisions—what are really design failures, from the perspective of helping consumers—can increase data exposure and therefore risks to people's safety.

People search data brokers and other data brokers remain serious problems with respect to effectuating opt-out requests. Data brokers such as Spokeo essentially outright tell consumers that they can go through an elaborate, time-intensive process to submit opt-out requests—only for the company to effectively dishonor the request by proceeding to repopulate its systems with that same person's data. This violates every notion of consumer consent that drives both the law and the principle of allowing consumers to express their non-consent to data use and submit opt-out requests from the sale or sharing of their data. Troublingly, this practice is not isolated to Spokeo. For years and still today, people search data brokers have catalyzed interpersonal, often gender-based violence against women, women of color, LGBTQ+ people, and others in a stalking context. Increasingly, people search data brokers have enabled the doxxing and targeting

of public servants and others. Their manipulatively designed or highly ineffective opt-out processes raise serious safety concerns.[40]

To mitigate these physical safety risks, companies should evaluate their opt-out processes and remove manipulative design features. Doing so is not only the right thing to do to respect the privacy rights of their users and customers, but having a clear, easy-to-use opt-out process is also required by law. Companies should clearly provide opt-out instructions and links in multiple places, including on their website homepage, within their privacy policies, and within other relevant locations and communications to users. The opt-out process should be simple, fast, and clearly described. When consumers submit an opt-out request, companies should clearly explain that certain types of data may be exempt from the opt-out, including publicly available data, and companies should also state any other limits of the opt-out request, such as legally required retention timelines for certain data. In fact, this should be a best practice and legal requirement: that companies must explicitly state the limits of their opt-outs, relative to the totality of the data they collect, store, infer, use, sell, or share, in plain language. After consumers submit an opt-out request, companies should ensure that they continually honor the opt-out request by conducting ongoing, periodic audits to ensure they are not selling or transferring data that has been the subject of an opt-out request.

State and federal regulators must step up to protect consumer opt-out rights. The FTC has used its Section 5 authority in the past to bring enforcement actions against companies using manipulative design to deceive consumers.[41] The FTC could continue to protect consumers from manipulative design by bringing enforcement actions against companies with manipulative opt-out processes. Now that many states have enacted privacy laws that include opt-out rights, state attorneys general should evaluate whether companies selling and sharing data about their constituents meet legal requirements relating to opt-outs. If state attorneys general find evidence that companies are not providing clear, easy-to-use opt-out processes because of manipulative design tactics, they should bring enforcement actions against violating companies.

[40] Justin Sherman, *People Search Data Brokers, Stalking, and 'Publicly Available Information' Carveouts*, Lawfare (Oct. 30, 2023).

[41] *See, e.g.*, *Press Release: FTC Takes Action Against Amazon for Enrolling Consumers in Amazon Prime Without Consent and Sabotaging Their Attempts to Cancel*, FTC (Jun. 21, 2023).

More states should also consider following California's lead to adopt a universal deletion mechanism. California's Delete Request and Opt-out Platform (DROP) allows consumers to submit one request for all data brokers registered in California to permanently delete their personal information. More states establishing a mechanism like DROP that allows consumers to make one request for companies to delete their data or opt them out of selling and sharing would make it significantly easier for consumers to exercise their privacy rights.

Related, federal and state laws and regulations that establish universal opt-out mechanisms would standardize these (often broken) opt-out processes across companies and contexts. The Global Privacy Control (GPC) is a well-known opt-out mechanism that allows consumers to install a simple browser extension that runs in the background and signals to websites that the consumer does not want to be tracked, enforced under state laws like California's privacy regime.[42] Several states already require companies to honor opt-out requests by universal opt-out mechanisms like GPC, and more states should follow suit. Establishing a standard mechanism for how consumers could opt out from data collection, sale, and so forth from any company covered by consumer privacy laws—no matter how big or what types of data it collects—would reduce the risk of variably deceptive designs across companies.

Even with the most consumer-friendly opt-out processes free from manipulation, consumers would still have to spend significant time to opt out from all of the companies that collect their data, sell their data to third parties, and transfer their data to third parties. Ultimately, legislators should not place the burden on consumers to protect their own privacy by having to opt out from every company that collects, sells, and transfers their personal information. Instead, policymakers should include data minimization requirements[43] in privacy legislation that only allow companies to "collect, use, and transfer personal data that is 'reasonably necessary and proportionate' to provide or maintain a product or service requested by the individual."[44] While opt-out rights are a step toward empowering consumers to protect their own privacy, strong data minimization standards provide more robust privacy protections before data is even gathered in the first

[42] *About*, Global Privacy Control, (last accessed May 8, 2026).
[43] *Data Minimization Requirements*, EPIC, (last accessed May 4, 2026).
[44] *Id*.

place.[45]

Manipulative design has no place in opt-out requests. It is already a near-impossible task to identify all of the companies that hold our data, and the presence of manipulative design in opt-out processes makes protecting our privacy even more difficult. Manipulative design undermines consumers' autonomy over their own personal information, and it may also violate state and federal laws. In situations when opt-outs are necessary for individuals to protect themselves and their loved ones against doxxing and interpersonal violence, manipulative and broken opt-out processes put people's lives at greater risk. Companies must design opt-out processes with respect toward consumers' rights, and if they do not, regulators at the state and federal level should step in to defend consumer rights to opt out.

[45] Caitriona Fitzgerald, Kara Williams, R.J. Cross, & Ellen Hengesbach, *The State of Privacy Laws 2025: How State 'Privacy' Laws Fail to Protect Privacy and What They Can Do Better*, EPIC (Jan. 2025).

Appendix: State Privacy Law Language Regarding Opt-Outs

State	Opt-Out Provision Citation	Opt-Out Provision Language
Alabama	Al. Enr. H.B. No. 351 § 5(a)(5); 6(b); 7(a)(3); 7(c); 7(d)	5(a)(5) "Subject to authentication and any other conditions or limitations provided by this act, a consumer may invoke the rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer right the consumer seeks to invoke. A controller shall comply with an authenticated request to do any of the Following: ... (5) Opt out of the processing of the consumer's personal data for any of the following purposes: a. Targeted advertising. b. The sale of the consumer's personal data. c. Profiling in furtherance of solely automated significant decisions concerning the consumer." 6(b) "(b) A controller must allow a consumer to opt-out by providing a **clear and conspicuous link** on the controller's Internet website to an Internet web page that enables a consumer directly to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or sale of the consumer's personal data, or provides up-to-date contact information for a consumer to submit the opt-out request." 7(a)(3) "(a) A controller shall do all of the following: ... (3) Provide an effective mechanism for a consumer to revoke the consumer's consent under this act that is **at least as easy** as the mechanism by which the consumer provided the consumer's consent on revocation of the consent, cease to further process the personal data as soon as practicable, but no later than 45 days after complying with the consumer's opt-out request consistent with this act." 7(c) "(c) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing."

State	Opt-Out Provision Citation	Opt-Out Provision Language
Alabama, *continued*	Al. Enr. H.B. No. 351 § 5(a)(5); 6(b); 7(a)(3); 7(c); 7(d)	7(d) "(d) A controller shall provide consumers with a **reasonably accurate, clear, and meaningful** privacy notice that includes all of the following: ... (6) How consumers may exercise their consumer rights, including a link or contact information for availing themselves of the opt-out method provided in Section 6."
California	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	1798.120(a)(1) "A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information." 1798.120(b) "A business that sells consumers' personal information to, or shares it with, third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold or shared and that consumers have the "right to opt out" of the sale or sharing of their personal information." 1798.135 "(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: (1) Provide a **clear and conspicuous link** on the business' internet homepages, titled "Do Not Sell or Share My Personal Information," to an internet web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale or sharing of the consumer's personal information. (2) Provide a **clear and conspicuous link** on the business' internet homepages, 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.

State	Opt-Out Provision Citation	Opt-Out Provision Language
California, *continued*	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	(3) At the business' discretion, utilize a **single, clearly labeled link** on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that 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. (4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's 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 (19) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' 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. (2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that: (A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

State	Opt-Out Provision Citation	Opt-Out Provision Language
California, *continued*	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	(B) **The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.** (C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (19) of subdivision (a) of Section 1798.185. (3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b). (c) A business that is subject to this section shall: 1) Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information. (2) Include a description of a consumer's rights pursuant to Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" internet web page and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), in: (A) Its online privacy policy or policies if the business has an online privacy policy or policies. (B) Any California-specific description of consumers' privacy rights. (3) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.120, 1798.121, and this section and how to direct consumers to exercise their rights under those sections.

State	Opt-Out Provision Citation	Opt-Out Provision Language
California, *continued*	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	(4) For consumers who exercise their right to opt out of the sale or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations. (5) For consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age. (6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request. (d) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally. of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out request consistently with Section 1798.125.

State	Opt-Out Provision Citation	Opt-Out Provision Language
California, *continued*	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	(e) A consumer may authorize another person to opt out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General (f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from: (1) Selling or sharing the personal information. (2) Retaining, using, or disclosing that consumer's personal information. (A) For any purpose other than for the specific purpose of performing the services offered to the business. (B) Outside of the direct business relationship between the person and the business. (C) For a commercial purpose other than providing the services to the business. (g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable." 1798.185(18)(A) "The requirements and specifications for the ***opt-out preference signal should be updated from time to time*** to reflect the means by which consumers interact with businesses, and should:

State	Opt-Out Provision Citation	Opt-Out Provision Language
California, *continued*	Cal. Civ. Code § 1798.120; 1798.135; 1798.185(18)	(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business. (ii) Ensure that the opt-out preference signal is **consumer-friendly, clearly described, and easy to use by an average consumer** and does not require that the consumer provide additional information beyond what is necessary. (iii) **Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.** (iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ. (v) Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally. (vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out preference signal, the consumer should see up to three choices, including: (I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information. (II) Choice to "Limit the Use of My Sensitive Personal Information." (III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."
Colorado	Colo. Rev. Stat. § 6-1-1306(1)(a); 6-1-1313(2)(2)	6-1-1306(1)(a)(I) "A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of: (A) Targeted advertising; (B) The sale of personal data; or (C) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.

State	Opt-Out Provision Citation	Opt-Out Provision Language
Colorado, *continued*	Colo. Rev. Stat. § 6-1-1306(1)(a); 6-1-1313(2)(2)	6-1-1306(1)(a)(III) "The controller shall provide the opt-out method **clearly and conspicuously** in any privacy notice required to be provided to consumers under this part 13, and in a **clear, conspicuous, and readily accessible location** outside the privacy notice." 6-1-1313(2) "By July 1, 2023, the attorney general shall adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that **clearly communicate a consumer's affirmative, freely given, and unambiguous choice** to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B). The attorney general may update the rules that detail the technical specifications for the mechanisms from time to time to reflect the means by which consumers interact with controllers. The rules must: (a) Not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller; (b) **Require controllers to inform consumers about the opt-out choices** available under section 6-1-1306 (1)(a)(I); (c) **Not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice** to opt out of the processing of personal data pursuant to section 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B); (d) Adopt a mechanism that is **consumer-friendly, clearly described, and easy to use by the average consumer**; (e) Adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States; and (f) Permit the controller to accurately authenticate the consumer as a resident of this state and determine that the mechanism represents a legitimate request to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B)."

State	Opt-Out Provision Citation	Opt-Out Provision Language
Connecticut	Conn. Gen. Stat. § 42-520	42-520(d) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing." 42-520(e)(A) "(i)Providing **a clear and conspicuous link** on the controller's Internet web site to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and (ii) Not later than January 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology or mechanism shall: (I) Not unfairly disadvantage another controller; (II) **Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given and unambiguous choice** to opt out of any processing of such consumer's personal data pursuant to sections 42-515 to 42-525, inclusive; (III) **Be consumer-friendly and easy to use by the average consumer**; (IV) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and (V) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising."
Delaware	6 Del. Code § 12D-104(a); 106(e)	12D-104(a) "A consumer has the right to do all of the following: … (6) Opt out of the processing of the personal data for purposes of any of the following:

State	Opt-Out Provision Citation	Opt-Out Provision Language
Delaware, *continued*	6 Del. Code § 12D-104(a); 106(e)	a. Targeted advertising. b. The sale of personal data, except as provided in § 12D-106(b) of this title. c. Profiling in furtherance of solely-automated decisions that produce legal or similarly significant effects concerning the consumer." 12D-106(d) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing." 12D-106(e) "... Any such means shall include all of the following: 1. Providing a **clear and conspicuous link** on the controller's Internet website to an Internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or the sale of the consumer's personal data. 2. Not later than January 1, 2026, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt out of any such processing or sale. Such platform, technology, or mechanism shall do all of the following: A. Not unfairly disadvantage another controller. B. **Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given, and unambiguous choice** to opt out of any processing of such consumer's personal data pursuant to this chapter. C. **Be consumer friendly and easy to use by the average consumer.** D. Be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation.

State	Opt-Out Provision Citation	Opt-Out Provision Language
Delaware, *continued*	6 Del. Code § 12D-104(a); 106(e)	E. Enable the controller to reasonably determine whether the consumer is a resident of the State and whether the consumer has made a legitimate request to opt out of any sale of such consumer's personal data or targeted advertising."
Indiana	Ind. Code § 24-15-3-1(b); 24-15-4-4	24-15-3-1(b) "A consumer has the following rights: ... (5) To opt out of the processing of the consumer's personal data for purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." 24-15-4-4 "If a controller sells a consumer's personal data to third parties or uses a consumer's personal data for targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such sales or use."
Iowa	Iowa Code § 715D.3; 715D.4	715D.3 "(1) ... A controller shall comply with an authenticated consumer request to exercise all of the following: ... d. To opt out of the sale of personal data." 715D.4 "2. A controller shall not process sensitive data collected from a consumer for a nonexempt purpose without the consumer having been presented with clear notice and an opportunity to opt out of such processing... " 715D.4 "5. A controller shall provide consumers with a reasonably accessible, clear, and meaningful privacy notice that includes the following: ... (e)6. If a controller sells a consumer's personal data to third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of such activity ... "
Kentucky	Ky. Rev. Stat. § 367.3615; 367.3617	367.3615(2) "A controller shall comply with an authenticated consumer request to exercise the right to: ... (e) Opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

State	Opt-Out Provision Citation	Opt-Out Provision Language
Kentucky, *continued*	Ky. Rev. Stat. § 367.3615; 367.3617	367.3617(4) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose such activity, as well as the manner in which a consumer may exercise the right to opt out of processing
Maryland	Md. Code, Com. Law § 14-4705(b); 14-4707(e); 14-4607(f)	14-4705(b) "A consumer shall have the right to: … (7) Opt out of the processing of personal data for purposes of: (I) Targeted advertising; (II) The sale of personal data; or (III) Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer." 14-4707(e) "(1) If a controller sells personal data to third parties or processes personal data for targeted advertising or for the purposes of profiling the consumer in furtherance of decisions that produce legal or similarly significant effects, the controller shall **clearly and conspicuously disclose** the sale or processing, as well as the manner in which a consumer may exercise the right to opt out of the sale or processing. (2) The disclosure required under paragraph (1) of this subsection shall be **prominently displayed**, and **use clear, easy to understand, and unambiguous language**, to state whether the consumer's information will be sold or shared with a third party." 14-4707(f) "(3) A controller may utilize the following methods to satisfy paragraph (1) of this subsection: (i) Providing a **clear and conspicuous link** on the controller's website to a webpage that allows a consumer, or an authorized agent of the consumer, to opt out of the targeted advertising or the sale of the consumer's personal data; or (ii) On or before October 1, 2025, allowing a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of personal data, through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale.

State	Opt-Out Provision Citation	Opt-Out Provision Language
Maryland *continued*	Md. Code, Com. Law § 14-4705(b); 14-4707(e); 14-4607(f)	(4) A platform, technology, or mechanism used in accordance with paragraph (3) of this subsection shall: (i) **Be consumer-friendly and easy to use by the average consumer;** (ii) Use **clear, easy to understand, and unambiguous language**; (iii) Be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or State law or regulation; (iv) Enable the controller to reasonably determine whether the consumer: 1. Is a resident of the State; and 2. Has made a legitimate request to opt out of any sale of the consumer's personal data or targeted advertising; and (v) Require a consumer to make an affirmative, unambiguous, and voluntary choice in order to opt out of any processing of the consumer's personal data."
Minnesota	Minn. Stat. § 325M.14(1)(f); 325M.14(3); 325M.16(1)(b)	325M.14(1)(f) "A consumer has the right to opt out of the processing of personal data concerning the consumer for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of automated decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer." 325M.14(3)(a) "A controller must allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of the consumer's personal data through an opt-out preference signal sent, with the consumer's consent, by a platform, technology, or mechanism to the controller indicating the consumer's intent to opt out of the processing or sale. The platform, technology, or mechanism must: (1) not unfairly disadvantage another controller; (2) **not make use of a default setting, but require the consumer to make an affirmative, freely given, and unambiguous choice** to opt out of the processing of the consumer's

State	Opt-Out Provision Citation	Opt-Out Provision Language
Minnesota *continued*	Minn. Stat. § 325M.14(1)(f); 325M.14(3); 325M.16(1)(b)	personal data; (3) **be consumer-friendly and easy to use by the average consumer**; (4) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation; and (5) enable the controller to accurately determine whether the consumer is a Minnesota resident and whether the consumer has made a legitimate request to opt out of any sale of the consumer's personal data or targeted advertising. For purposes of this paragraph, the use of an Internet protocol address to estimate the consumer's location is sufficient to determine the consumer's residence." 325M.16(1)(b) "If a controller sells personal data to third parties, processes personal data for targeted advertising, or engages in profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer, the controller must disclose the processing in the privacy notice and provide access to a **clear and conspicuous method outside the privacy notice** for a consumer to opt out of the sale, processing, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer. **This method may include but is not limited to an Internet hyperlink clearly labeled "Your Opt-Out Rights" or "Your Privacy Rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request."**
Montana	Mont. Code § 30-14-2808; 30-14-2809(1-3); 30-14-2812(4)	30-14-2808 "(1) A consumer must have the right to: … (e) opt out of the processing of the consumer's personal data for the purposes of: (i) targeted advertising; (ii) the sale of the consumer's personal data, except as provided in 30-14-2812(2); or (iii) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."

State	Opt-Out Provision Citation	Opt-Out Provision Language
Montana *continued*	Mont. Code § 30-14-2808; 30-14-2809(1-3); 30-14-2812(4)	30-14-2809(1-3) "(1) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data for one or more of the purposes specified in 30-14-2808(1)(e). The consumer may designate an authorized agent by way of a technology, including but not limited to an internet link or a browser setting, browser extension, or global device setting indicating a customer's intent to opt out of such processing. (2) A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. (3) Opt-out methods must: (a) provide a **clear and conspicuous link** on the controller's internet website to an internet web page that enables a consumer, or an agent of the consumer, to opt out of the targeted advertising or sale of the consumer's personal data; and (b) by no later than January 1, 2025, allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data through an opt-out preference signal sent with the consumer's consent, to the controller by a platform, technology, or mechanism that: (i) may not unfairly disadvantage another controller; (ii) **may not make use of a default setting, but require the consumer to make an affirmative, freely given and unambiguous choice to opt out** of any processing of a customer's personal data pursuant to this part; (iii) **must be consumer-friendly and easy to use by the average consumer**; (iv) must be consistent with any federal or state law or regulation; and (v) must allow the controller to accurately determine

State	Opt-Out Provision Citation	Opt-Out Provision Language
Montana *continued*	Mont. Code § 30-14-2808; 30-14-2809(1-3); 30-14-2812(4)	whether the consumer is a resident of the state and whether the consumer has made a legitimate request to opt out of any sale of a consumer's personal data or targeted advertising." 30-14-2812 "(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose the processing, as well as the way a consumer may exercise the right to opt out of the processing. **This method may include but is not limited to an internet hyperlink clearly labeled "your opt-out rights" or "your privacy rights" that directly effectuates the opt-out request or takes consumers to a web page where the consumer can make the opt-out request."** 30-14-2812 "(5) A controller shall provide consumers with a reasonably **accessible, clear, and meaningful privacy notice** that includes: ... (f) an explanation of the rights provided by **30-14-2808**(1) and how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision regarding the consumer's request; ...
Nebraska	Neb. Rev. Stat. § 87-1107; 87-1111(5); 87-1114	87-1107 "(2) A controller shall comply with an authenticated consumer request to exercise the right to: ... (e) Opt out of the processing of the personal data for purposes of: (i) Targeted advertising; (ii) The sale of personal data; or (iii) Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer." 87-1111(5) "(5) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under subdivisions (2)(e)(i) and (ii) of section 87-1107. A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing of the consumer's personal data under subdivisions (2)(e)(i) and (ii) of section 87-1107. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller

State	Opt-Out Provision Citation	Opt-Out Provision Language
Nebraska, *continued*	Neb. Rev. Stat. § 87-1107; 87-1111(5); 87-1114	is able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if: (a) The authorized agent does not communicate the request to the controller in a clear and unambiguous manner; (b) The controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state; (c) The controller does not possess the ability to process the request; or (d) The controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state. (6) A technology described by subsection (5) of this section: (a) Shall not unfairly disadvantage another controller; (b) **Shall not make use of a default setting, but shall require the consumer to make an affirmative, freely given, and unambiguous choice** to indicate the consumer's intent to opt out of any processing of a consumer's personal data; and (c) Shall be **consumer-friendly and easy to use by the average consumer.**" 87-1114 "If a controller sells personal data to any third party or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose that process and the manner in which a consumer may exercise the right to opt out of that process."
New Hampshire	N.H. Rev. Stat. § 507-H:4(I)(e); 507-H:6	507-H:4(I) "A consumer shall have the right to: ... (e) Opt-out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, except as provided in RSA 507-H:6, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."

State	Opt-Out Provision Citation	Opt-Out Provision Language
New Hampshire *continued*	N.H. Rev. Stat. § 507-H:4(I)(e); 507-H:6	507-H:6(IV) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose such processing, as well as the manner in which a consumer may exercise the right to opt-out of such processing." 507-H:6(V)(a) "... Any such means shall include: (1)(A) Providing a **clear and conspicuous link** on the controller's Internet website to an Internet webpage that enables a consumer, or an agent of the consumer, to opt-out of the targeted advertising or sale of the consumer's personal data; and (B) Not later than January 1, 2025, allowing a consumer to opt-out of any processing of the consumer's personal data for the purposes of targeted advertising, or any sale of such personal data, through an opt-out preference signal sent, with such consumer's consent, by a platform, technology, or mechanism to the controller indicating such consumer's intent to opt-out of any such processing or sale. Such platform, technology, or mechanism shall: (i) Not unfairly disadvantage another controller; (ii) **Not make use of a default setting, but, rather, require the consumer to make an affirmative, freely given, and unambiguous choice** to opt-out of any processing of such consumer's personal data pursuant to this chapter; (iii) **Be consumer-friendly and easy to use by the average consume**r; (iv) Be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation; and (v) Enable the controller to accurately determine whether the consumer is a resident of this state and whether the consumer has made a legitimate request to opt-out of any sale of such consumer's personal data or targeted advertising."

State	Opt-Out Provision Citation	Opt-Out Provision Language
New Jersey	N.J. Stat. § 56:8-166.6(3)(b); 56:8-166.10(7)(a)(5); 56:8-166.11(8)(b)	"56:8-166.6(3)(b) "If a controller sells personal data to third parties or processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, the controller shall clearly and conspicuously disclose such sale or processing, as well as the manner in which a consumer may exercise the right to opt out of such sale or processing." 56:8-166.10(7)(a) "A consumer shall have the right to: … (5) opt out of the processing of personal data for the purposes of (a) targeted advertising; (b) the sale of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." 56:8-166.11(8)(b) "(1) Beginning not later than six months following the effective date of P.L.2023, c.266 (C.56:8-166.4 et seq.), a controller that processes personal data for purposes of targeted advertising, or the sale of personal data shall allow consumers to exercise the right to opt out of such processing through a user-selected universal opt-out mechanism. (2) The platform, technology, or mechanism shall: (a) not permit its manufacturer to unfairly disadvantage another controller; (b) not make use of a default setting that opts in a consumer to the processing or sale of personal data, unless the controller has determined that the consumer has selected such default setting and the selection clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt into any processing of such consumer's personal data pursuant to P.L.2023, c.266 (C.56:8-166.4 et seq.); (c) be consumer-friendly, clearly described, and easy to use by the average consumer; (d) be as consistent as possible with any other similar platform, technology, or mechanism required by any federal or state law or regulation; and (e) enable the controller to accurately determine whether the consumer is a resident of this State and whether the

State	Opt-Out Provision Citation	Opt-Out Provision Language
New Jersey, *continued*	N.J. Stat. § 56:8-166.6(3)(b); 56:8-166.10(7)(a)(5); 56:8-166.11(8)(b)	consumer has made a legitimate request to opt out of the processing of personal data for the purposes of any sale of such consumer's personal data or targeted advertising."
Oklahoma	Ok. Enr. S.B. No. 546 § 2(B); 8(B)	2(B) "A controller shall comply with an authenticated consumer request to exercise the right to: ... 5. Opt out of the processing of the personal data for purposes of: a. targeted advertising, b. the sale of personal data, or c. profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the Consumer." 8(B) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose on the notice required by subsection A of this section such process and the manner in which a consumer may exercise the right to opt out of such process."
Oregon	Or. Rev. Stat. § 646A.574(1); 646A.578(4); 646A.578(5)	646A.574(1) "Subject to ORS 646A.576, a consumer may: ...(d) Opt out from a controller's processing of personal data of the consumer that the controller processes for any of the following purposes: (A) Targeted advertising; (B) Selling the personal data; or (C) Profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance." 646A.578(4) "A controller shall provide to consumers a **reasonably accessible, clear and meaningful privacy notice** that: ... (h) Provides a **clear and conspicuous** description of any processing of personal data in which the controller engages for the purpose of targeted advertising or for the purpose of profiling the consumer in furtherance of decisions that produce legal effects or effects of similar significance, and a procedure by which the consumer may opt out of this type of processing."

State	Opt-Out Provision Citation	Opt-Out Provision Language
Oregon, *continued*	Or. Rev. Stat. § 646A.574(1); 646A.578(4); 646A.578(5)	646A.578(5) "The method or methods described in subsection (4)(i) of this section for submitting a consumer's request to a controller must: ... (b) Provide a **clear and conspicuous link** to a webpage where the consumer or an authorized agent may opt out from a controller's processing of the consumer's personal data as described in ORS 646A.574 (1)(d) or, solely if the controller does not have a capacity needed for linking to a webpage, provide another method the consumer can use to opt out. (c) Allow a consumer or authorized agent to send a signal to the controller that indicates the consumer's preference to opt out of the sale of personal data or targeted advertising under ORS 646A.574 (1)(d) by means of a platform, technology or mechanism that: (A) Does not unfairly disadvantage another controller; (B) **Does not use a default setting but instead requires the consumer or authorized agent to make an affirmative, voluntary and unambiguous choice to opt out;** (C) **Is consumer friendly and easy for an average consumer to use**; (D) Is as consistent as possible with similar platforms, technologies or mechanisms required under federal or state laws or regulations; and (E) Enables the controller to accurately determine whether the consumer is a resident of this state and has made a legitimate request under ORS 646A.576 to opt out as described in ORS 646A.574 (1)(d)."
Rhode Island	R.I. Gen. Laws § 6-48.1-5(e); 6-48.1-5(f)	6-48.1-5(e) "A customer shall have the right to: ...(4) Opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer." 6-48.1-5(f) "A customer may exercise rights under this section by secure and reliable means established by the controller and **described to the customer in the controller's privacy notice**. A customer may designate an authorized agent to exercise the rights to opt out on their behalf. In the case of proce-

State	Opt-Out Provision Citation	Opt-Out Provision Language
Rhode Island, *continued*	R.I. Gen. Laws § 6-48.1-5(e); 6-48.1-5(f)	processing personal data of a known child, the parent or legal guardian may exercise such customer rights on the child's behalf. In the case of processing personal data concerning a customer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the customer may exercise such rights on the customer's behalf."
Tennessee	Tenn. Code § 47-18-3304(a)(2); 47-18-3305(d)	47-18-3304(a)(2) "A controller shall comply with an authenticated consumer request to exercise the right to: … (E) Opt out of a controller's processing of personal information for purposes of: (i) Selling personal information about the consumer; (ii) Targeted advertising; or (iii) Profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." 47-18-3305(d) "If a controller sells personal information to third parties or processes personal information for targeted advertising, then the controller shall **clearly and conspicuously** disclose the processing, as well as the manner in which a consumer may exercise the right to opt out of the processing."
Texas	Tex. Bus. & Com.Code § 541.051(b); 541.055(e-f); 541.103;	541.051(b) "A controller shall comply with an authenticated consumer request to exercise the right to: … (5) opt out of the processing of the personal data for purposes of: (A) targeted advertising; (B) the sale of personal data; or (C) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer." 541.055(e-f) "(e) A consumer may designate another person to serve as the consumer's authorized agent and act on the consumer's behalf to opt out of the processing of the consumer's personal data under Sections 541.051(b)(5)(A) and (B). A consumer may designate an authorized agent using a technology, including a link to an Internet website, an Internet browser setting or extension, or a global setting on an electronic device, that allows the consumer to indicate the consumer's intent to opt out of the processing. A controller shall comply with an opt-out request received from an authorized agent under this subsection if the controller is able to verify,

State	Opt-Out Provision Citation	Opt-Out Provision Language
Texas, *continued*	Tex. Bus. & Com.Code § 541.051(b); 541.055(e-f); 541.103;	with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf. A controller is not required to comply with an opt-out request received from an authorized agent under this subsection if: (1) the authorized agent does not communicate the request to the controller in a clear and unambiguous manner; (2) the controller is not able to verify, with commercially reasonable effort, that the consumer is a resident of this state; (3) the controller does not possess the ability to process the request; or (4) the controller does not process similar or identical requests the controller receives from consumers for the purpose of complying with similar or identical laws or regulations of another state. (f) A technology described by Subsection (e): (1) may not unfairly disadvantage another controller; (2) may not make use of a default setting, but must require the consumer to make an affirmative, freely given, and unambiguous choice to indicate the consumer's intent to opt out of any processing of a consumer's personal data; and (3) must be consumer-friendly and easy to use by the average consumer." 541.103 "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process."
Utah	Utah Code § 13-61-201(4); 13-61-302(1)(b); 13-61-302(3)	13-61-201(4) "A consumer has the right to opt out of the processing of the consumer's personal data for purposes of: (a) targeted advertising; or (b) the sale of personal data." 13-61-302(1)(b) "If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall **clearly and conspicuously** disclose to

State	Opt-Out Provision Citation	Opt-Out Provision Language
Utah, *continued*	Utah Code § 13-61-201(4); 13-61-302(1)(b); 13-61-302(3)	the consumer the manner in which the consumer may exercise the right to opt out of the: (i) sale of the consumer's personal data; or (ii) processing for targeted advertising." 13-61-302(3) "Except as otherwise provided in this chapter, a controller may not process sensitive data collected from a consumer without: (a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or (b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions."
Virginia	Va. Code § 59.1-577(A); 59.1-578(D)	59.1-577(A) "A consumer may invoke the consumer rights authorized pursuant to this subsection at any time by submitting a request to a controller specifying the consumer rights the consumer wishes to invoke. A known child's parent or legal guardian may invoke such consumer rights on behalf of the child regarding processing personal data belonging to the known child. A controller shall comply with an authenticated consumer request to exercise the right: … 5. To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." 59.1-578(D) "If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller shall **clearly and conspicuously** disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing."