

AdTech and Data Privacy

David Zetoony, Shareholder & Co-Chair of US Data Privacy and Security Team

Agenda

1. What is AdTech?
2. What are the modern state privacy laws?
3. What are the implications for browser-based targeting technologies?
4. What are the implications for CRM-Based targeting technologies?
5. Industry trends, plaintiffs bar, regulators, and dark patterns
6. Practical suggestions for compliance

1. What is AdTech?

Official Definition

“AdTech”

The word you've entered isn't in the dictionary. Click on a spelling suggestion below or try again using the search bar above.

Unofficial Definition

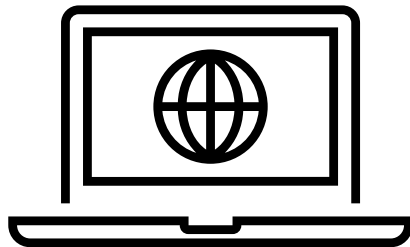
“AdTech”

Adtech or Advertising Technology encompasses **all the technologies associated with advertising campaigns, as well as all information, processes, and performance measurement metrics.**

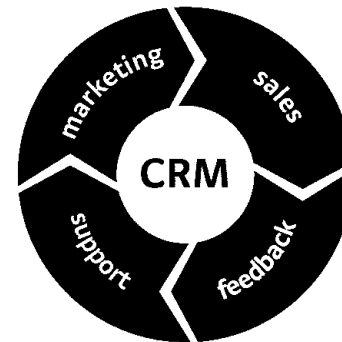
1. What is AdTech?

Given the breadth of the term its impossible to discuss all AdTech technologies or explain the legal implications of every permutation of AdTech. That said, the most common technologies can be divided into two groups:

Browser-Based Technologies

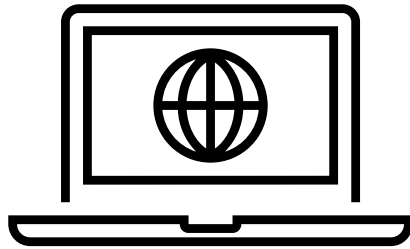


Customer Relationship Manager (CRM) Based Technologies



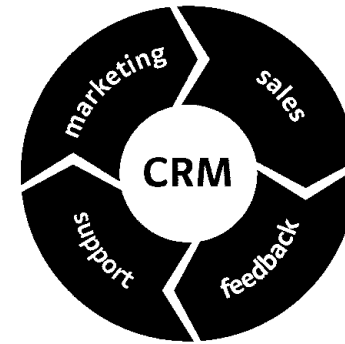
1. What is AdTech?

Browser-Based Technologies



- Cookies
- Pixels
- Tracking Scripts
- SDKs

Customer Relationship Manager (CRM) Based Technologies

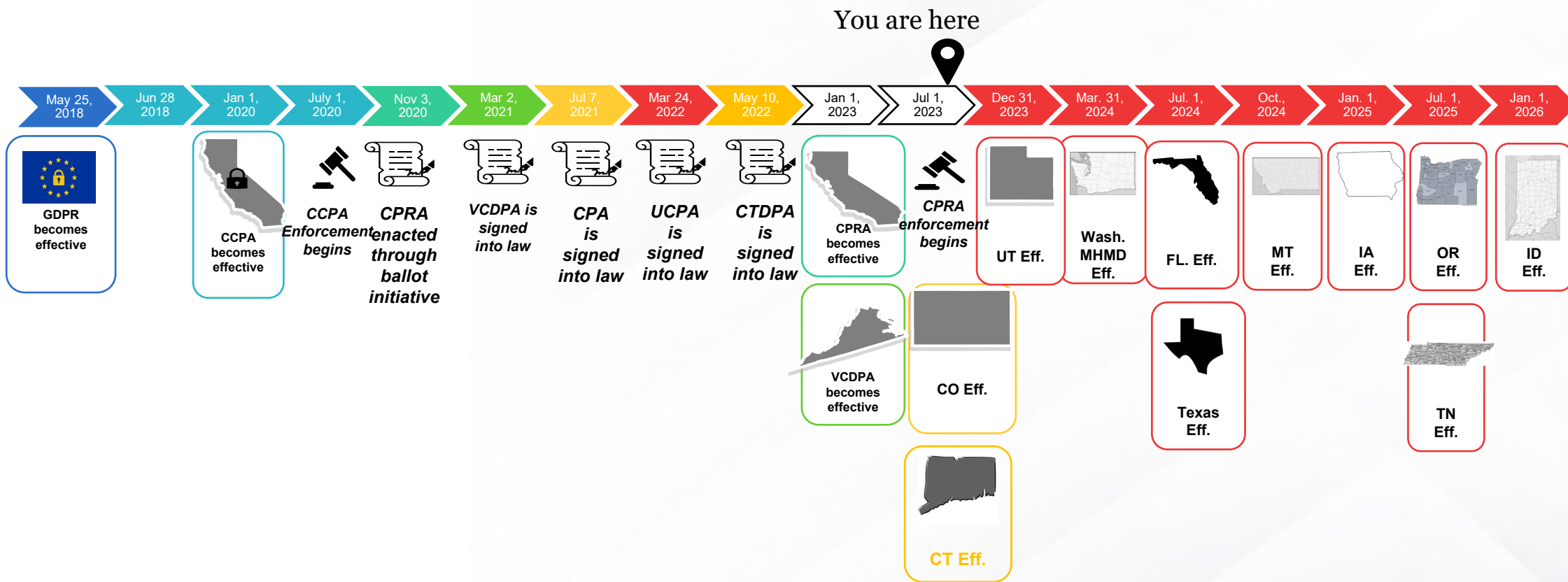


- Custom Audience
- Lookalike Audience

2. What are the modern state privacy laws?

A Crash Course on Modern US Data Privacy Law . . .

2. What are the modern state privacy laws?



2. What are the modern state privacy laws?

		California Consumer Protection Act (CCPA) <i>Eff. Jan. 1, 2020</i>	California Privacy Rights Act (CPRA) <i>Eff. Jan. 1, 2023</i>	Virginia Consumer Data Protection Act (VCDPA) <i>Eff. Jan. 1, 2023</i>	Colorado Privacy Act (CPA) <i>Eff. Jul. 1, 2023</i>	Connecticut Data Privacy Act (CTDPA) <i>Eff. Jul. 1, 2023</i>	Utah Consumer Privacy Act (UCPA) <i>Eff. Dec. 31, 2023</i>	Washington My Health My Data (WVMD) <i>Eff. Mar. 31, 2024</i>	Florida Digital Bill of Rights (FDBR) <i>Eff. Jul. 1, 2024</i>	Texas Data Privacy and Security Act (TDPSA) <i>Eff. Jul. 1, 2024^d</i>	Montana Consumer Data Privacy Act (MCDDPA) <i>Eff. Oct. 1, 2024</i>	Iowa Consumer Data Protection Act (IPA) <i>Eff. Jan. 1, 2025</i>	Tennessee Information Protection Act (TIIPA) <i>Eff. July 1, 2025</i>	Indiana Consumer Data Protection Act (ICDPA) <i>Eff. Jan. 1, 2026</i>
Scope	Consumer Data	✓	✓	✓	✓	✓	✓	✓ / ✗ <i>(Only Consumer Health)</i>	✓ / ✗ ⁱⁱ <i>(only certain businesses see (iv))</i>	✓ / ✗ ⁱⁱⁱ <i>(only certain businesses see (iv))</i>	✓	✓	✓	✓
	HR Data	<i>deferred</i>	✓											
	B2B Data	<i>deferred</i>	✓											
Ability to Process Data	Consent for Processing Sensitive Data		<i>Notice & Opt-out Rqmt</i>	✓	✓	✓	<i>Notice & Opt-out Rqmt</i>	✓ ^{iv}	✓ ^v	✓	✓	<i>Notice & Opt-out Rqmt</i>	✓	✓
	Data Minimization		✓ <i>(Retention)</i>	✓ <i>(Collection)</i>	✓ <i>(Collection & Retention)</i>	✓ <i>(Collection)</i>			✓ <i>(Collection & Retention)^{vi}</i>	✓ <i>(Collection & Retention)^{vi}</i>	✓ <i>(Collection)</i>	✓ ^{vii}	✓ <i>(Collection)</i>	✓ <i>(Collection)</i>
Individual Rights	Notices to Data Subjects	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Financial Incentive Disclosure	✓	✓		✓ ^x									
	Right to Access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ ^x	✓
	Right to Correction (aka Right to Fix Errors)		✓	✓	✓	✓			✓	✓	✓		✓	✓
	Right to Deletion (aka Right to Be Forgotten)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Right to Opt-Out of Behavioral Advertising		✓	✓	✓	✓	✓	<i>Opt-in with right to withdraw consent</i>	✓	✓	✓	✓ ^{xi}	✓	✓
	Right to Opt-Out of Sale	✓	✓	✓	✓	✓	✓	<i>Opt-in with right to withdraw consent</i>	✓	✓	✓	✓	✓	✓
	Right to Opt-Out of Profiling & Automated Decision Making		<i>To be addressed by regulations</i>	✓	✓	✓	✓		✓	✓	✓		✓	✓
	Right to Limit Use of Sensitive Information ⁱⁱ		✓					✓	✓	✓	✓	✓	✓	✓
	Right to Appeal			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Right to Nondiscrimination	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Honor opt-out signals (E.g., GPC)	✓ ^{xiii}	✓		✓	✓	✓			✓	✓		✓	✓	
Accountability & Governance		<i>✓ To be addressed by regulations</i>	✓	✓	✓	✓			✓	✓		✓	✓	
Security	Appropriate Data Security to Safeguard Information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Breach Notification	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]	✓ [*]
Transfers to Third Parties	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

2. What are the modern state privacy laws?

Right to Deletion (aka Right to Be Forgotten)	✓	✓	✓	✓	✓	✓	✓
Right to Opt Out of Sale	✓*	✓	✓	✓	✓	✓	✓
Right to Opt Out of Behavioral Advertising	✓*		✓	✓	✓	✓	✓
Right to Object to Use of Sensitive Information	✓		✓		✓		✓
Right to Object to Automated Decision Making & Profiling	✓		✓		✓		✓

- The original state privacy law (CCPA) had a right to opt-out of the sale of data which was defined as disclosing data for money or other valuable consideration.
- The California Attorney General has taken the position that many forms of AdTech involve the transfer of personal information from one company (e.g., publisher or advertiser) to another company (advertising network or social media platform), and that activity constitutes a “Sale.”
- Significant ambiguity exists as to whether a court would agree with that interpretation.
- In response,
 - The CPRA was amended by privacy advocates to require that companies provide a right for consumers to opt-out of “sharing,” a term which was defined as giving data for “cross-context behavioral advertising.”
 - Other states provide a right for consumers to opt-out of “targeted advertising” and require that companies conduct data protection impact assessments (DPIAs) if they engage in targeted advertising.

2. What are the modern state privacy laws?

Va. Code. Ann. 59.1-575
(similar to CPA/CTDPA/UPA):

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from the consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

Cal. Civ. Code 1798.140(k), (ah)(1)

"Sharing" means . . . disclosing . . . or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

"Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

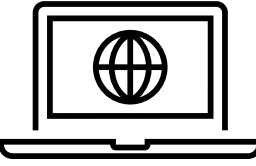
2. What are the modern state privacy laws?

Definition Explicitly Requires	Virginia 2023 VCDPA	Colorado 2023 CPA	Utah 2023 UCPA	Conn. 2023 CTDPA	California 2023 CPRA
Ads are displayed to a consumer	✓ ³⁴²	✓ ³⁴³	✓ ³⁴⁴	✓ ³⁴⁵	✓ ³⁴⁶
Selection based on activities over time	✓ ³⁴⁷	✓ ³⁴⁸	✓ ³⁴⁹	✓ ³⁵⁰	✗
Selection based on activities across nonaffiliated website or online applications	✓ ³⁵¹	✓ ³⁵²	✓ ³⁵³	✓ ³⁵⁴	✓ ³⁵⁵
Selection based upon prediction of consumer's preferences or interests	✓ ³⁵⁶	✓ ³⁵⁷	✓ ³⁵⁸	✓ ³⁵⁹	✗

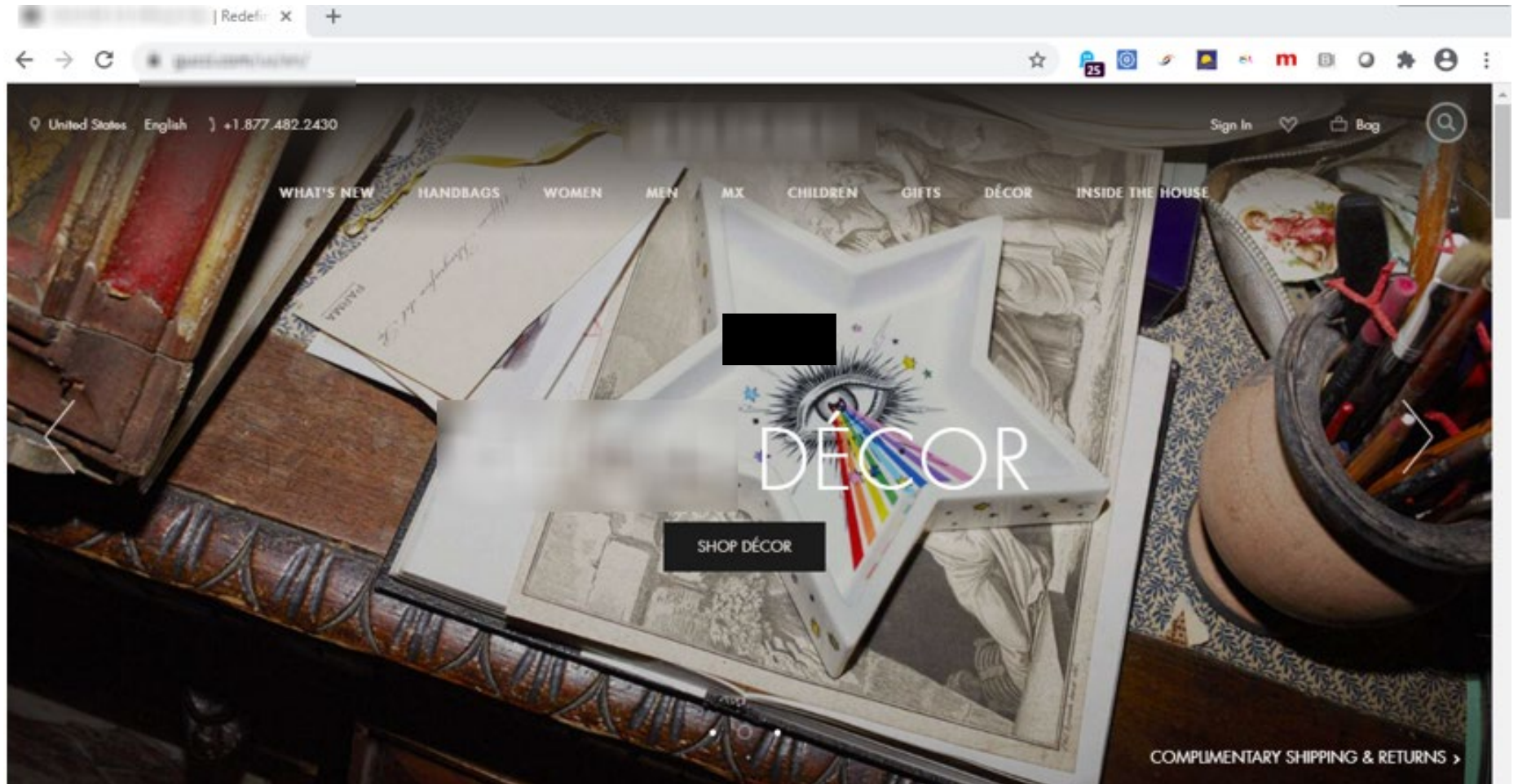
Things to remember:

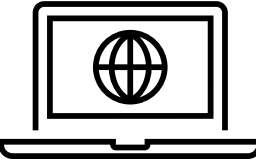
- Whether the definition of “targeted advertising,” “sharing,” or “selling” applies to specific AdTech technologies and practices is a fact-based question that has yet to be explored by courts.
- Each statute has different exceptions to their definition. One of the main differences is that California has an exception for information that is shared at the consumers “direction” (i.e., with consumer consent). The other states have that exception for “selling” but not for “targeted advertising.”

3. Implications for browser-based targeting technologies?



What the consumer sees:





3. Implications for browser-based targeting technologies?

What the consumer does not see:

The screenshot shows a browser window with a network developer tool open. The page content includes a navigation menu with categories like 'WHAT'S NEW', 'HANDBAGS', 'WOMEN', 'MEN', 'KID', 'CHILDREN', 'GIFTS', 'DÉCOR', and 'INSIDE THE HOUSE'. A large 'DÉCOR' banner is visible, along with a 'STORES ARE OPEN' notification. The network log below shows a list of requests with columns for Name, Status, Domain, Type, Initiator, Size, and T. A specific request is highlighted in red, indicating it was blocked: 'adscpt?type=javascript&version=1.1.0&...' from 'analytics.twitter.com' with a status of '(blocked/other)'. Other requests include various document and HTML files from '4565108.fls.doubleclick.net' and '9122529.fls.doubleclick.net', and GIFs from 'adservice.google.com'. The summary at the bottom indicates 289 requests, 12.8 MB transferred, and 23.5 MB resources.

Name	Status	Domain	Type	Initiator	Size	T.	Waterfall
activity:dc_pre=CKe9op_d2OscFdlSsw...	200	4565108.fls.doubleclick.net	document	activity:src=4565108?type=visit:cat=home:ord=1:num=4410033...	1.4 kB	5...	
activity:src=4565108?type=visit:cat=ho...	302	4565108.fls.doubleclick.net	text/html	1eeb427...:i7	1.0 kB	1...	
activity:dc_pre=CJLHrj_d2OscFdlSswQ...	200	4565108.fls.doubleclick.net	document	activity:src=4565108?type=visit:cat=arrival:ord=1:num=4088622...	1.4 kB	4...	
activity:src=4565108?type=visit:cat=ar...	302	4565108.fls.doubleclick.net	text/html	1eeb427...:i7	1.0 kB	5...	
activity:dc_pre=CJOu3KDd2OscFdlSswQ...	200	9122529.fls.doubleclick.net	document	9122529.fls.doubleclick.net/activity:src=9122529?type=keringas...	1.2 kB	8...	
activity:src=9122529?type=keringas:ca...	302	9122529.fls.doubleclick.net	text/html	1eeb427...:i7	1.0 kB	1...	
dc_pre=CJOu3KDd2OscFdlSswQodwAL...	200	adservice.google.com	gif	activity:dc_pre=CJOu3KDd2OscFdlSswQodwALLeQ:src=9122529...	1.1 kB	6...	
dc_pre=CKe9op_d2OscFdlSswQodg6gE...	200	adservice.google.com	gif	activity:dc_pre=CKe9op_d2OscFdlSswQodg6gE5w:src=4565108;t...	1.1 kB	5...	
dc_pre=CJLHrj_d2OscFdlSswQody0sF...	200	adservice.google.com	gif	activity:dc_pre=CJLHrj_d2OscFdlSswQody0sF_A:src=4565108;ty...	1.1 kB	2...	
adscpt?type=javascript&version=1.1.0&...	(blocked/other)	analytics.twitter.com	script	1eeb427...:i7	0 B	8...	
0?ti=30000172&Ver=2&mid=b88d7c1...	(pending)	bat.bing.com	text/plain;charset=...	/static/1eeb427...:i7	0 B	P...	



3. Implications for browser-based targeting technologies?

What the consumer does not see:

The screenshot shows a browser's developer console with a network tab open. A table of network requests is visible, with a red box highlighting the following data:

<input type="checkbox"/>	dc_pre=CKe9op_d2OscFdiSwQodg6gE...	200	adservice.google.com
<input type="checkbox"/>	dc_pre=CJLHrJ_d2OscFf2wQody0sF_...	200	adservice.google.com
<input type="checkbox"/>	adscrt?type=javascript&version=1.1.0&...	(blocked:other)	analytics.twitter.com
<input type="checkbox"/>	0?ti=30000172&Ver=2&mid=b88d7c1...	(pending)	bat.bing.com

Below the table, a red box highlights a summary row:

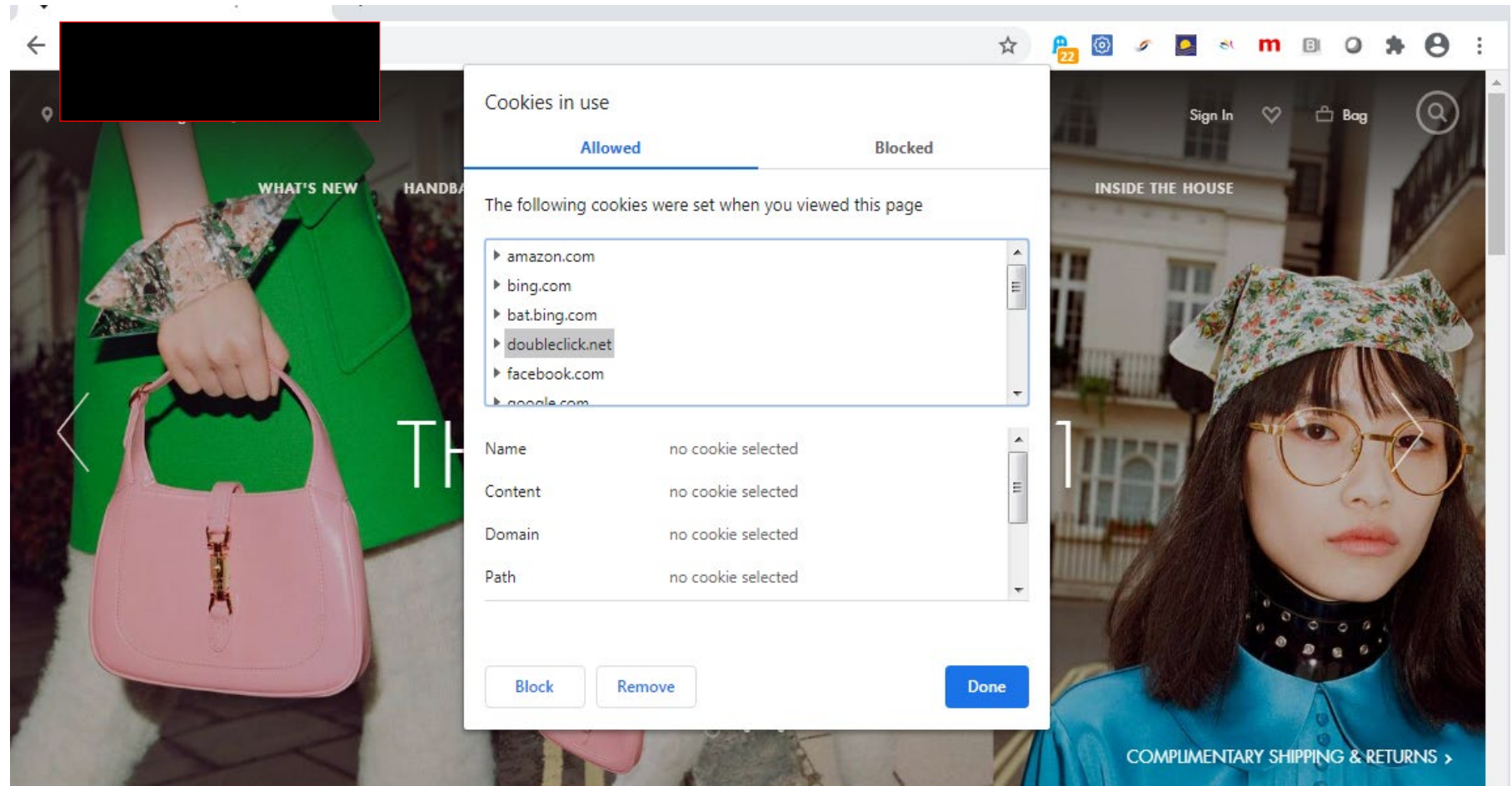
289 requests	12.8 MB transferred	23.5 MB resources	Finish: 1.3 min	DOMContentLo
--------------	---------------------	-------------------	-----------------	--------------

The console also shows a 'Console' tab with a search bar and a 'What's New' notification. A red arrow points to the '289 requests' value in the summary row.

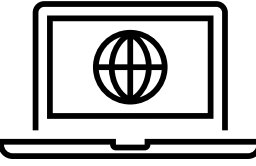


3. Implications for browser-based targeting technologies?

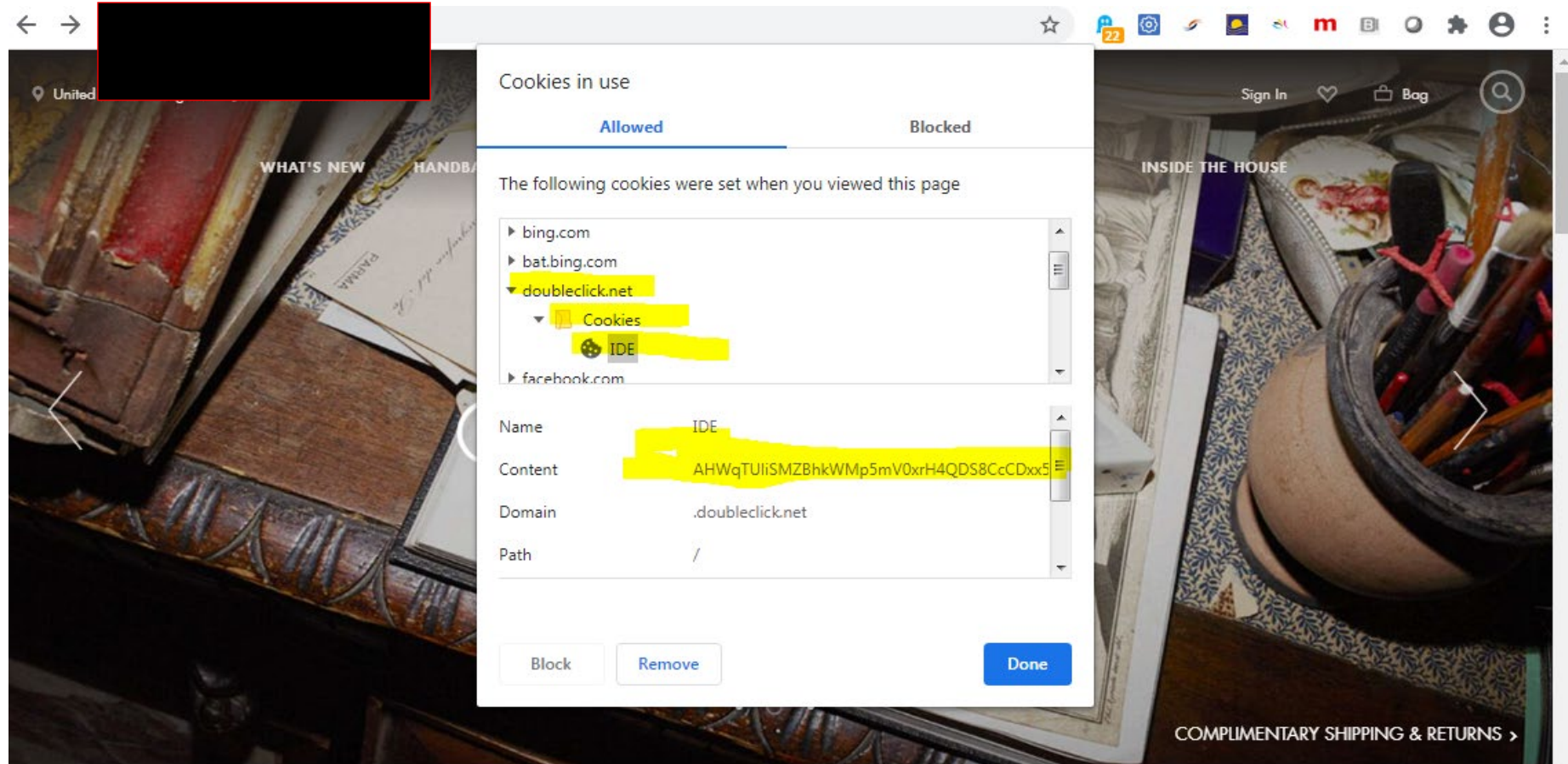
What the consumer does not see:



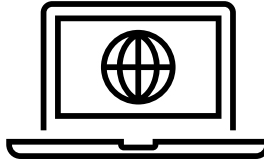
3. Implications for browser-based targeting technologies?



What the consumer does not see:

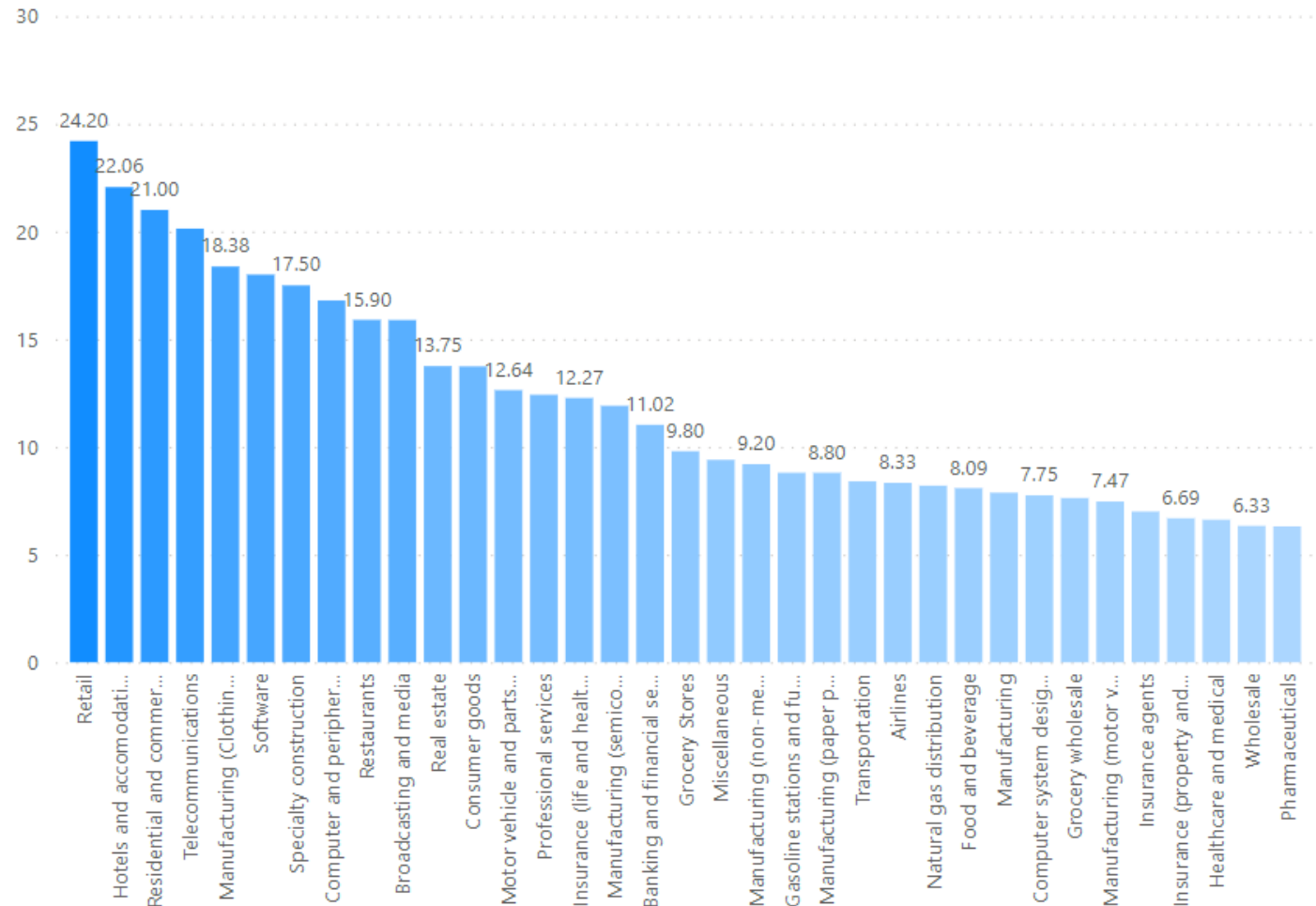


3. Implications for browser-based targeting technologies?

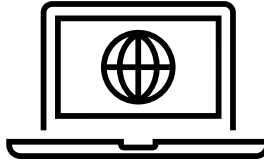


Quantity of Browser-Based AdTech deployed by industry:

- Study conducted by Greenberg Traurig on 560 companies approximating Fortune 500
- Quantity reflects the number of third party AdTech providers that were utilized on public-facing websites of each company.
- Testing was conducted from a California IP address.



3. Implications for browser-based targeting technologies?



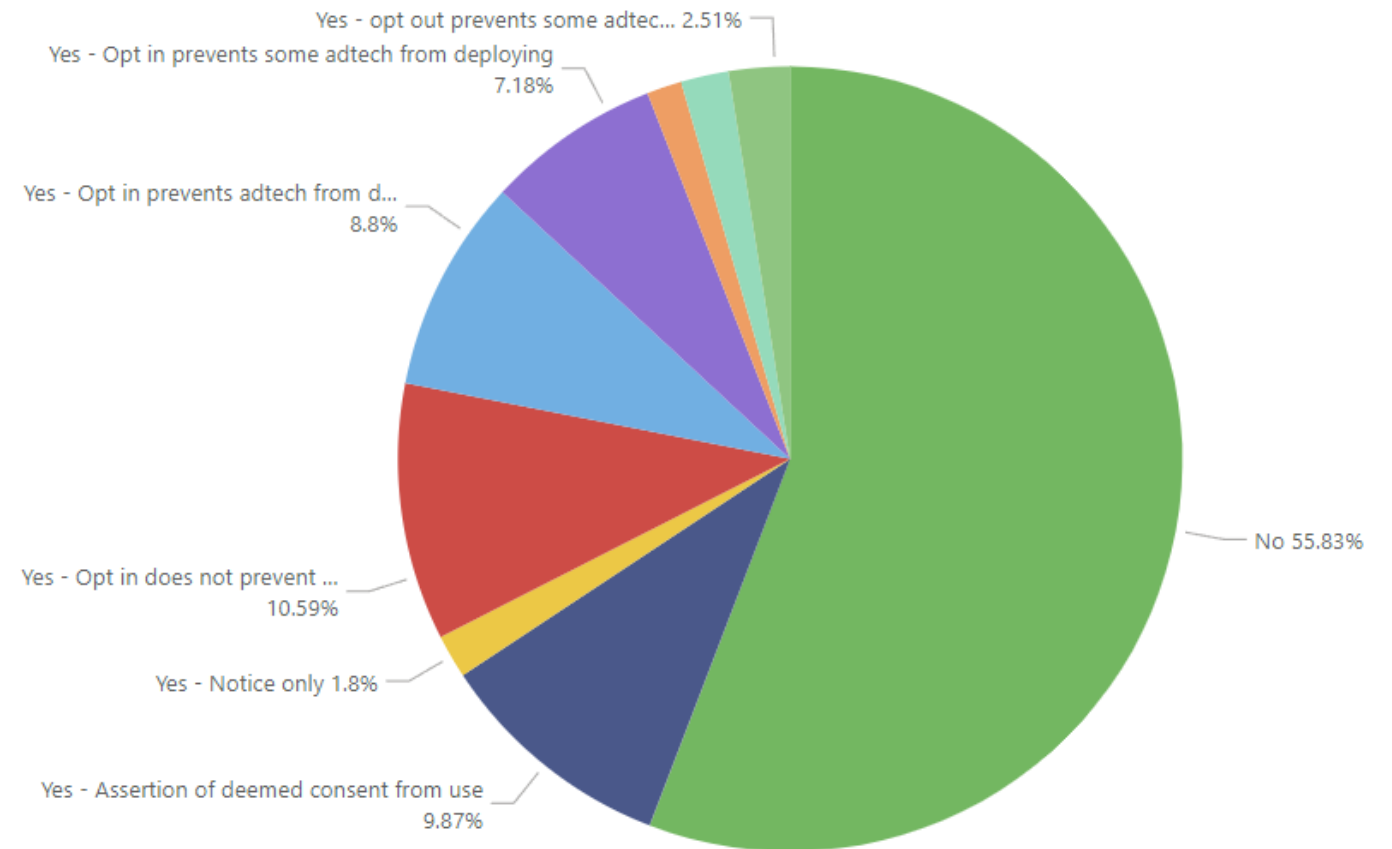
Is browser-based advertising “targeted advertising” or “sharing” under the modern state privacy statutes?

Elements of Targeted Advertising (VA/CO/CT/UT)	Examples of Factors that Might Impact Whether Browser-Side Technologies Would be Considered Targeted Advertising
Ads are displayed to a consumer	<p>Factors:</p> <ul style="list-style-type: none"> • Most browser-side technologies involve displaying ads to consumers. • That said, some browser-based technologies which are utilized for analytics or attribution may not involve the display of ads.
Selection based on activities over time	<p>Factors</p> <ul style="list-style-type: none"> • This element would likely be met in the case of traditional “retargeting” campaigns wherein browser-based tracking technology is used to create a consumer profile that is in turn used to help select ads.
Selection based on activities across nonaffiliated website or online applications	<p>Factors:</p> <ul style="list-style-type: none"> • This element would likely be met in the case of traditional “retargeting” campaigns wherein a profile is created based upon a consumers visits across nonaffiliated websites.
Selection based upon prediction of consumer’s preferences or interests	<p>Factors:</p> <ul style="list-style-type: none"> • Element is likely met in the context of a traditional “retargeting” campaign as the selection of the ad would be based upon a prediction that the consumer’s preferences or interests match those of the advertiser.

3. Implications for browser-based targeting technologies?

Industry trends in re cookie banners:

- Cookie notices are approaching 50%
- Configuration of cookie notices reflect the fact that there is no “one-size-fits-all” compliance solution.
- Opt-in cookie notices have been on a consistent rise over the past four years, and now account for almost 1/3 of banners.
- The “functionality” of cookie banners (whether opt-in or opt-out) is a persistent issue.



Nov. 2022 | Data of 560 companies reflecting Fortune 500

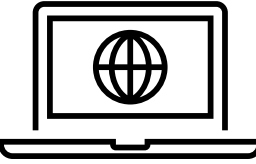
3. Implications for browser-based targeting technologies?



The main issues to consider are:

- You must offer an opt-out capability (or withdrawal of consent if you solicited opt-in).
- As part of your opt-out option you should consider:
 - Processing opt-outs where the consumer broadcasts an electronic preference to opt-out.
 - The degree to which an opt-out preference will be sticky as the user changes browsers and computers (persistence).
 - The degree to which you are able to communicate an opt-out preference to companies to whom you have transmitted information in the past.
- If you solicit “opt-in” (i.e., ask permission before using browser-based technologies like cookies) then you arguably are not subject to many of the more complex opt-out requirements under California law. Specifically,
 - Under California law you arguably don’t have to monitor for electronic signals that indicate a desire to opt-out, don’t have to flow down opt-out requests to third parties (proposed regulation), don’t have to design a system to ensure that the consumers selection persists across browsers, devices, and time.
- If subject to Colorado, Connecticut, or Virginia law you must conduct a written DPIA.

3. Implications for browser-based targeting technologies?



Question:

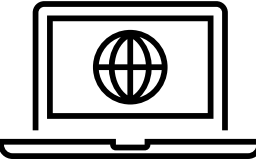
Are cookies and pixels dying??

Answer:

Google Chrome's deprecation of support for third party tracking technologies has felt like a bogeyman.



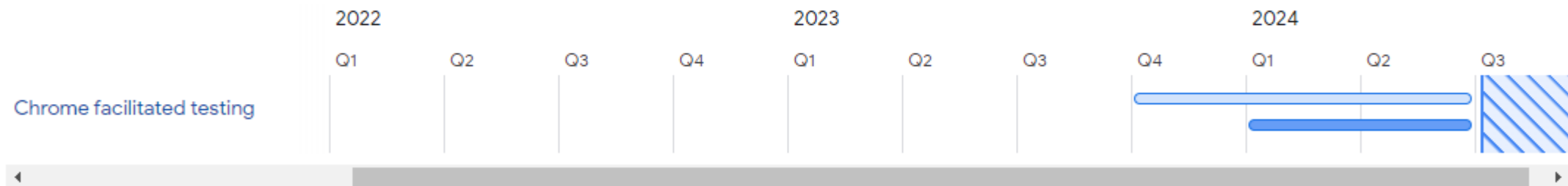
3. Implications for browser-based targeting technologies?



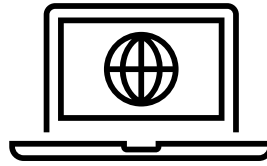
Google's timeline to deprecate tracking tech support (as of Aug. 29, 2023)

THIRD-PARTY COOKIES (3PC) AND TESTING

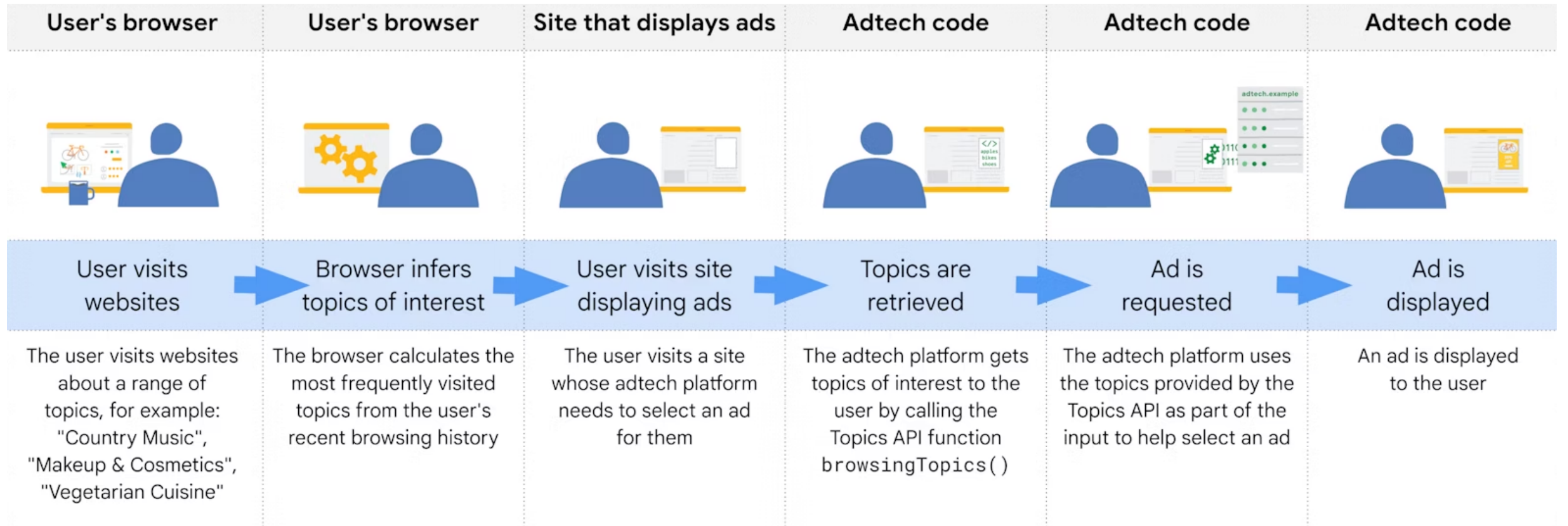
- Opt-in Testing with Labels
- 1% 3PC Deprecation
- ▨ Third-Party Cookie Phase Out



3. Implications for browser-based targeting technologies?



What comes next? **Google Topic API**



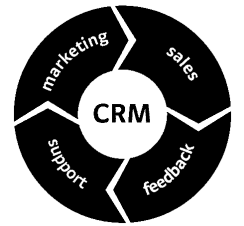
4. Implications for CRM-based targeting technologies?



CRM-Based Technologies:

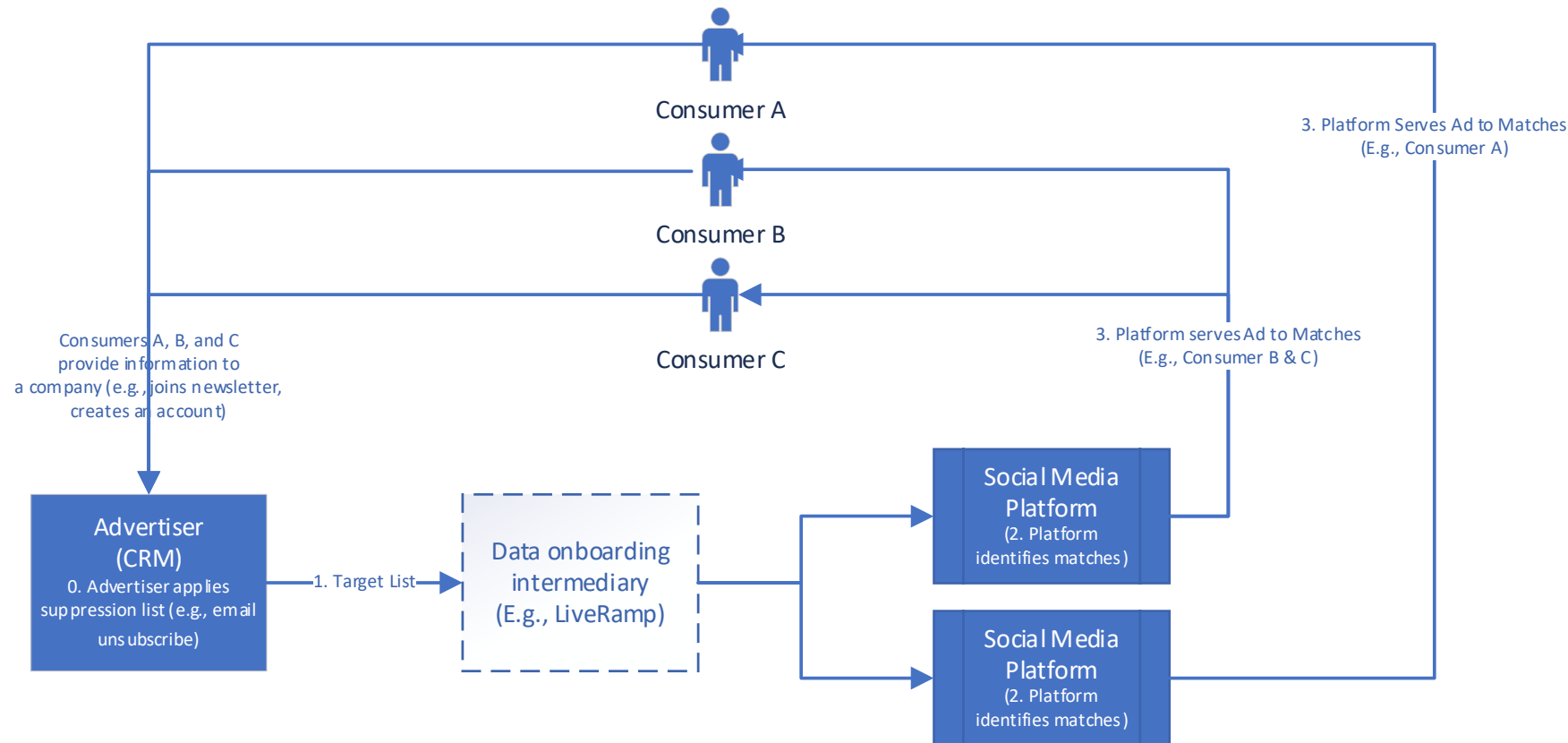
- Leverage the first party data of the advertiser (often kept in customer relationship management (CRM) systems).
- Tend to rely less (if at all) on browser-side tracking.
- Come in a variety of permutations and flavors, and are described by a number of different names, but can generally be grouped under two rubrics:
(1) Custom Audience and (2) Lookalike Audience

4. Implications for CRM-based targeting technologies?



Custom Audience refers to the following:

1. Advertiser transmits a list of consumers to a social media platform (the “Target List”),
2. The social media platform attempts to identify those consumers on the Target List that have a social media account (“matches”), and
3. The social media platform serves the advertiser’s advertisement to each match on the social media platform.



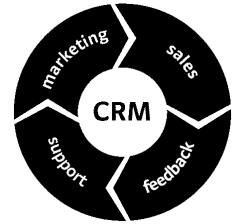
4. Implications for CRM-based targeting technologies?



Is the use of custom audiences “targeted advertising” under the modern state privacy statutes?

Elements of Targeted Advertising under VA/CO/CT/UT	Examples of Factors that Might Impact Whether Custom Audience Would be Considered Targeted Advertising
Ads are displayed to a consumer	✓ Element is likely met.
Selection based on activities over time	Factors: <ul style="list-style-type: none"> • If custom audience only attempts to serve ads to matches, element is likely not met as the selection of the advertisements is arguably not based on consumers activities over time.
Selection based on activities across nonaffiliated website or online applications	Factors: <ul style="list-style-type: none"> • If Advertiser selected Target List based only on data collected in-store, the element may not be met as the selection is arguably not based on activities that occurred across any websites. • If Advertiser selected Target List based only on its own first party data, the element may not be met as the selection is arguably not based on activities that occurred across more than one website.
Selection based upon prediction of consumer’s preferences or interests	Factors: <ul style="list-style-type: none"> • If Advertiser has not predicted a preference/interest of the Target List (e.g., the advertiser intends to serve advertisement to everyone within its CRM system), the element may not be met as the selection is arguably not based on a prediction of the consumer’s preferences or interests.

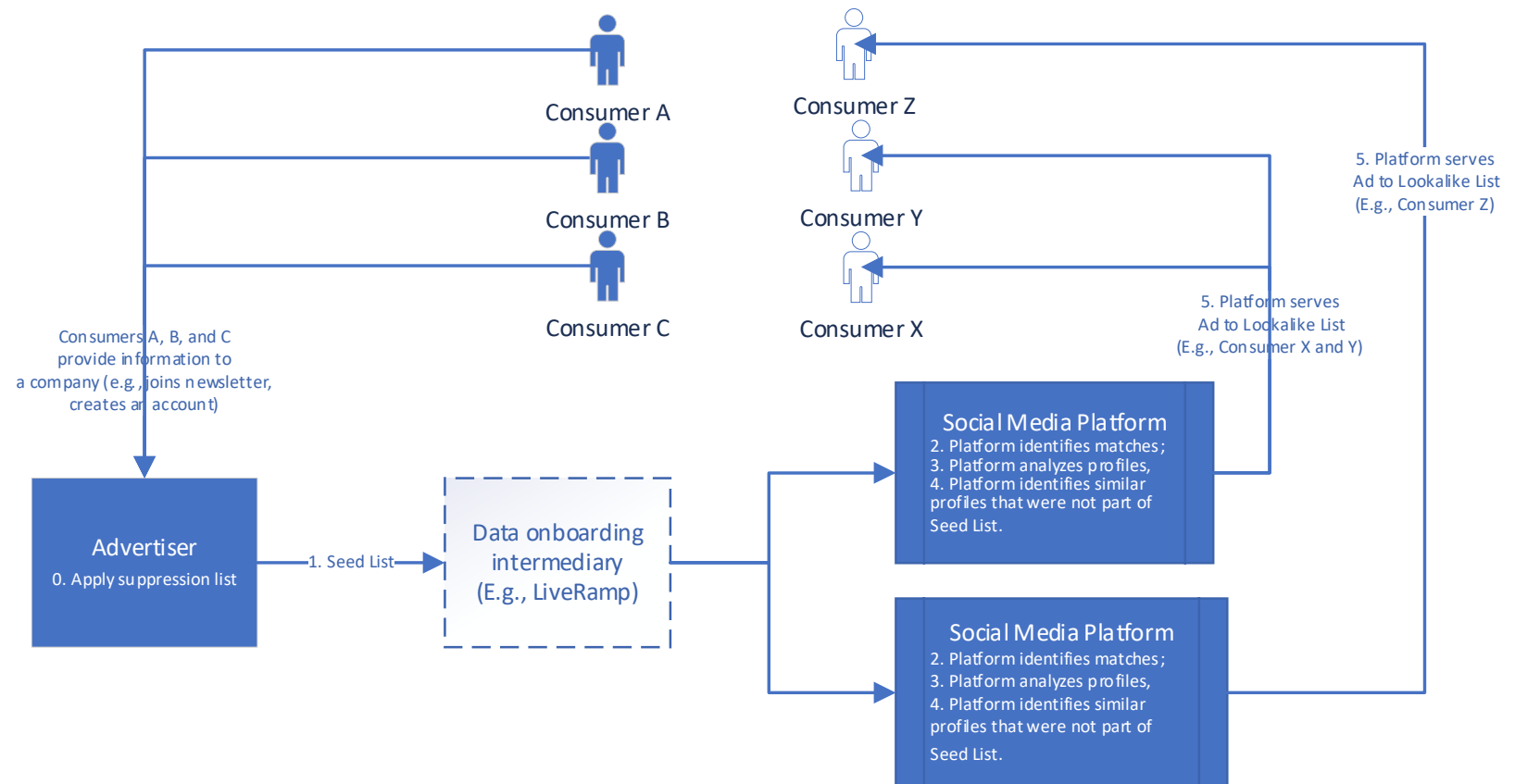
4. Implications for CRM-based targeting technologies?



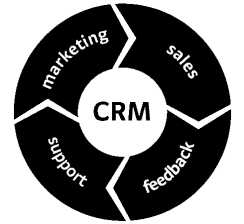
Lookalike Audience refers to the following:

1. Advertiser transmits a list of consumers to a social media platform (the “Seed List”),
2. Social media platform attempts to identify those individuals on the Seed List that have social media accounts (“matches”),
3. Social media platform analyzes the profile data that it holds about the matches,
4. Social media platform attempts to identify other social media platform account holders with similar profiles who were not on the Seed List (“Lookalike List”), and
5. Social media platform serves the advertiser’s advertisements to members of the Lookalike List.

High Level Depiction of Data Usage via Typical Lookalike Audience Campaign



4. Implications for CRM-based targeting technologies?



Is the use of lookalike audiences “targeted advertising” or “sharing” under the modern state privacy statutes?

Elements of Targeted Advertising under VA/CO/CT/UT	Examples of Factors that Might Impact Whether Lookalike Audience Would be Considered Targeted Advertising
Ads are displayed to a consumer	<p>Factors:</p> <ul style="list-style-type: none"> Although Ads are displayed to consumers, it is uncertain whether a court would find that this element is met where the “consumer” that receives the ad in the Lookalike List is not a consumer that is known to the advertiser.
Selection based on activities over time	<p>✓ Element is likely met as the selection of the ad would be based upon consumers activities over time (which contribute to the consumer’s profile with the social media platform).</p>
Selection based on activities across nonaffiliated website or online applications	<p>Factors:</p> <ul style="list-style-type: none"> If the Social Media Platform does not collect information about the members of the Lookalike List from external sources (or does not use such information, even if collected, for selecting advertisements) this element may not be met, as the selection of the Lookalike List members would only be based upon the Lookalike List members’ activities within a single website or online application.
Selection based upon prediction of consumer’s preferences or interests	<p>✓ Element is likely met as the selection of the ad would be based upon a prediction that the consumer’s preferences or interests match those of the members of the Seed List.</p>

4. Implications for CRM-based targeting technologies?



Assuming that your use of either custom or lookalike audiences are “targeted advertising” or “sharing” under the modern state privacy statutes then consider:

- Does your company have an opt-out mechanism that someone could use so that they are not part of your custom audience campaigns.
- Does your opt-out mechanism sync with the opt-out mechanisms that you have for other forms of targeted advertising (i.e., browser-based targeted advertising)?
- Colorado, Connecticut, and Virginia require the creation of a written DPIA (if a company is subject to those statutes).

5. Industry trends

Plaintiffs bar

- Plaintiffs' firms have filed hundreds of class actions across the country focused on companies' use of AdTech.
- Plaintiffs are not able to use modern privacy statutes (no private right of action) so they are consistently testing new theories under other laws including wiretapping, Video Privacy Protection Act, and deception.

Cyber insurance

- Given the quantity of litigation filings, most cyber insurance companies have attempted to write exclusions into their policies to avoid tracking and AdTech related data privacy litigation.

Regulators

- Many regulators are focused on AdTech, and the use of potentially deceptive opt-out and opt-in structures or so called “dark patterns”
- FTC brought its first case (*FTC v. GoodRx*) in Feb. 2023 against a company that utilized AdTech (browser and possibly CRM). That case will likely spawn AG and plaintiff’s bar to follow in trend.

Technology

- Technology and AdTech providers are constantly changing and adapting their products.
- Consistent speculation over the past four years that some technologies that are the focus of AdTech (e.g., third party cookies) may be deprecated.

6. Practical suggestions for compliance

1. In-house counsel need to “go deep” with marketing departments to understand what they are doing with regard to AdTech.
 - Don’t be intimidated by industry terms and lingo. There is no universal translator!! Ask marketing to explain exactly that they are doing.
 - Approach the question from both the browser-side and the CRM-side. Marketing and digital advertising departments are often siloed and may not be thinking about both applications.
 - Explore the level of understanding that marketing departments have regarding their use of the technology, technological changes, and legal requirements.
 - Explore their two to three year roadmap (i.e., what are they planning on doing next).
2. Don’t look for black-and-white compliance solutions.
 - There are dozens of approaches to compliance; each has their pros- and cons-
 - Compliance approaches continue to change in risk as the laws adapt and regulators change positions.
 - Be prepared to discuss with the business the degree of acceptable risk.

6. Practical suggestions for compliance

3. Monitor legal and technological developments

- Be prepared for a monthly conversation regarding the twists and turns of litigation, regulatory action, and legislative action. There is no one-and-done when it comes to AdTech.
- Subscribe to Greenberg Traurig's privacy updates: <https://www.gtlaw-dataprivacydish.com/subscribe/>

4. Discuss with business whether the goal should be chasing minimum legal requirements (i.e., opt-out systems) or best practices (opt-in).

- “Minimum legal requirements” evolve extremely fast which causes near constant operational costs.

Presenters

David A. Zetoony

Shareholder; Co-Chair, U.S. Data, Privacy and Cybersecurity Practice

DENVER | T: +1 303.685.7425

David.Zetoony@gtlaw.com | [LinkedIn](#) | [Detailed Biography](#)

David Zetoony focuses on helping businesses navigate data privacy and cyber security laws from a practical standpoint. David has helped hundreds of companies establish and maintain ongoing privacy and security programs, and he has defended corporate privacy and security practices in investigations initiated by the Federal Trade Commission, and other data privacy and security regulatory agencies around the world, as well as in class action litigation.

