



**REDCL**  **VER**  
ADVISORS

**Demystifying Privacy Regulations:  
What every digital marketer should  
know.**

***April 2021***



## Legal Disclaimer

Red Clover Advisors is not a law firm. The materials in this document are for informational purposes only and not for the purpose of providing legal advice.



# How We Got Here





Three in ten US users deploy ad-blocking software that can prevent companies from tracking online activity

39%

of consumers are likely to walk away from a company that requires them to provide highly personal data to conduct business with them  
*(Akamai)*

Consumers want to see data security/privacy made a core corporate value, no third-party sales of their data the option to choose how their data is used and clarity about how they can set privacy settings

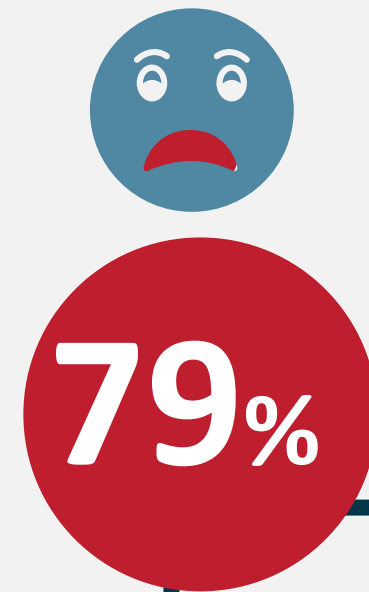
39%

37%

36%

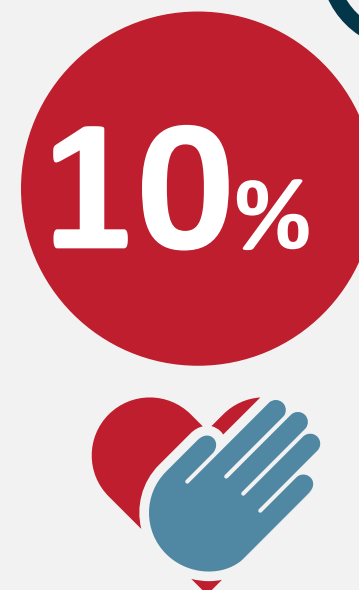


Roughly eight-in-ten adults (79%) said they were at least somewhat **concerned** about how companies were using the **data collected** about them



In 2019, 52% of Americans said they had decided not to use a product or service because they were worried about how **much personal information** would be collected about them

of consumer respondents said that they **trust consumer-packaged-goods** or media and entertainment companies



# Privacy Law 101





# PERSONAL DATA

## EXAMPLES



# Examples of online identifiers

Any moniker used for online presence—social media, e-mail, instant messenger

ID number

IP addresses















“Cookies”

Geolocation

Others





Sensitive Data - Comparison		(must Opt-in)		(must Opt-in)
		GDPR	CPRA	VCDPA
	Racial / ethnic origin	◆	◆	◆
	Political opinions	◆	◆	◆
	Religious / philosophical beliefs	◆	◆	◆
	Trade union membership	◆		◆
	Health data	◆		◆
	Genetic data	◆	◆	◆
	Biometric data	◆	◆	◆
	Sex life / sexual orientation	◆	◆	◆
	Past or spent criminal convictions	◆	◆	
	Mail, email and text message content		◆	
	Precise geolocation data		◆	◆
	Personal data collected from a known child			◆
	Social Security, driver's license, state identification card, or passport number.		◆	
	Account login, financial account, debit card, or credit card number		◆	

## What is the GDPR?



The **General Data Protection Regulation** regulates the way that data is handled across sectors within the **European Union** and **European Economic Area (EEA)**.



The **GDPR** provides those living in the EU with the right to **protect** their own personal data and privacy.



### Scope:

The **GDPR includes** all data controllers and processors located in the EU and all data processing that is in the context of the EU. The GDPR protects **all EU data subjects' data** even if it is processed outside of the EU, it also applies to all goods or services sold within the EU, and if an organization is monitoring a data subject's behavior.



# ePrivacy Regulation



**Draft under review** as of 2/4/2021 by the Council of the EU and the European Parliament



**Create stronger rules** that apply to all people and businesses in the EU. Everyone gets the same level of protection of their electronic communications. Businesses will only have to follow one set of rules.



**Expand privacy rules** to new players who provide electronic communication, such as Facebook, Skype, and WhatsApp) so they provide the same level of confidentiality as traditional telecoms operators.

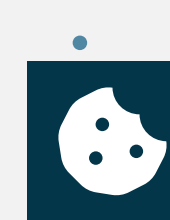


**Guarantee privacy** for content and metadata of communications. For instance, the file size of an email will be just as private as the email content itself. Metadata must be anonymized or deleted if users did not give consent, unless the data is needed for billing.

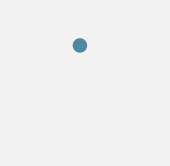
- Examples can include the telephone numbers called and the websites visited, including the geographical location of the caller or website user; and the time, date, and duration when an individual made a call or visited a website.
- Also includes provisions on when disclosures must be made to end users about metadata processing, the circumstances under which metadata may be stored, and the length of time metadata can be stored.



**Protect against spam.** Unsolicited electronic communications by emails, SMS, and automated calling machines are banned. People will either be protected by default or have the opportunity to use do-not-call lists. Marketing callers must display their phone number or use a special prefix.



**Simplify rules on cookies** by permitting browsers to create user-friendly ways to accept or refuse cookies and clarifying that no consent is needed for non-privacy-intrusive cookies that improve the internet experience, such as cookies that track your shopping cart or remember your username.



**Improve enforcement of the confidentiality** by granting more power to data protection authorities, who are already in charge under the General Data Protection Regulation.





## What is the CCPA?



The **California Consumer Privacy Act** is the first comprehensive data privacy law to go into effect in the United States and its creation has catalyzed other states to begin the process of passing their own **data privacy laws**.



### Scope:

The CCPA covers a smaller region and includes any for-profit company that is operating and conducting business in the state of California or any business that collects information from California residents.



## What is the CPRA?



The **California Privacy Rights Act** is a new state-wide data privacy bill that takes effect on January 1, 2023 that was passed into law on November 3rd, 2020. It amends various parts of the existing CCPA, is broader in scope, and establishes the **California Privacy Protection Agency**.



### CPPA:

The California Privacy Protection Agency will be governed by a five member board and will have investigative, enforcement, and rulemaking powers.



## Selling

“any arrangement involving an exchange of value ("consideration") between the business and a third party or another company for the personal information. These include the act of disclosing or making available personal information for monetary or other valuable consideration.”

## Sharing (introduced via CPRA)

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





## What is the VCDPA?



The **Virginia Consumer Data Privacy Act** is a new state-wide data privacy bill that takes effect on January 1, 2023 that was signed into law on March 3, 2021.



### Enforcement:

Only the **Attorney General of Virginia** will have the authority to sue businesses who aren't in compliance.



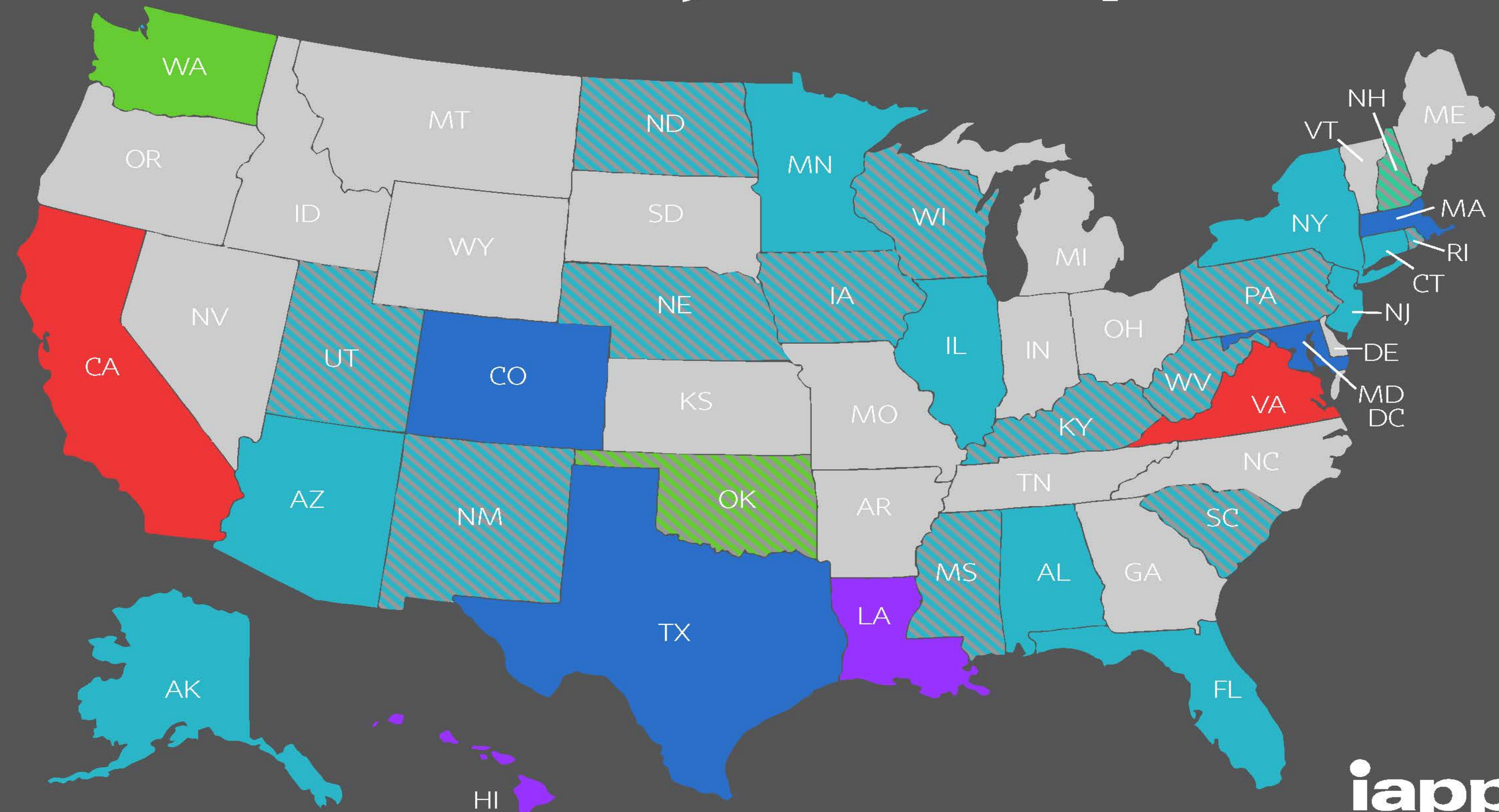
# State Comprehensive-Privacy Law Comparison



- Task Force Substituted for Comprehensive Bill
- Bill Died in Committee or Postponed
- None

## Statute/Bill in Legislative Process:

- Introduced
- In Committee
- Cross Chamber
- Cross Committee
- Passed
- Signed



Last updated: 4/12/2021

iapp





What happens  
when you  
don't comply!



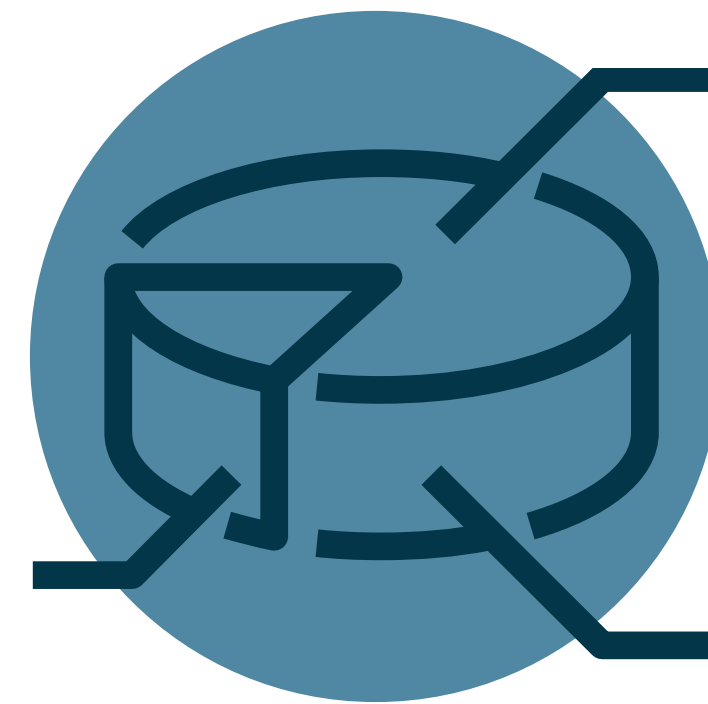


# What does this mean for me?

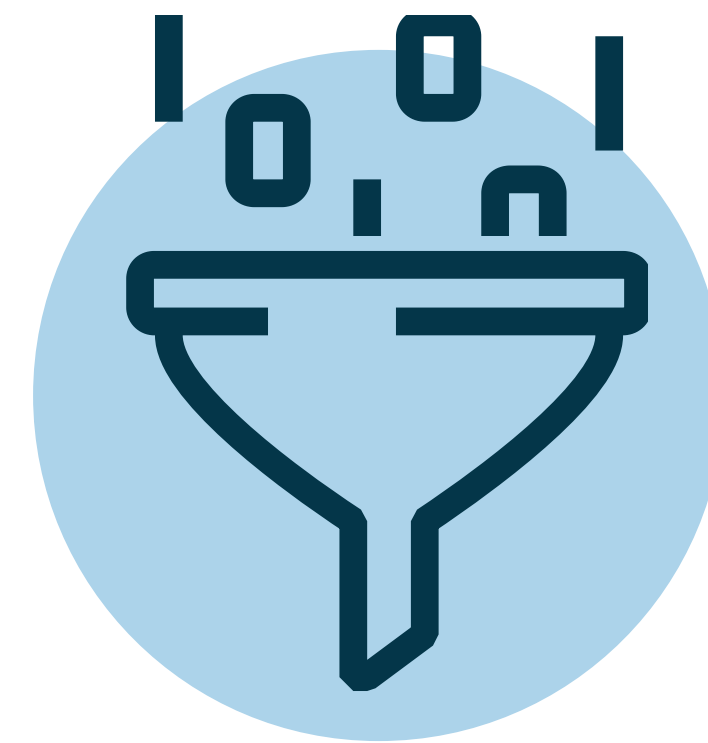




**What data do  
you have?**



**How do you  
use data?**



**Where is it  
stored?**



**Who do you  
share it  
with?**





# The GDPR is primarily against:

- The building of profiles around personal data without the person's knowledge or consent
- Using this data in automated decision making
- Unsafe storage and leakage of PII



“Pseudonymised” data is PII if the pseudonym can be linked to an individual

- Biggest change is it's now illegal to share IP addresses and do user matching (cookies/mobile IDs) with ad partners for EU traffic.
- Even frequency capping and interest targeting for direct-sold campaigns could be impacted. And without user matching, the value of one's traffic drops significantly, negatively impacting everyone in the ad tech chain.
- Brands can continue to do cookie matching, frequency targeting, programmatic ads, etc, as long as the user consents to it.
- If using a 3rd-party to show ads (aka using an ad network/exchange), may need to mention all those involved.





## Opt-In Requirements Must Haves

- NO pre-ticked boxes
- Be specific
- Not a condition of service
  - Opt-in for marketing emails should not be tied to purchasing the service (*must be freely given*)
- Must be easy to withdraw
- Link to privacy notice
- *Note: unsubscribe does not fulfill the individual right to deletion*



- In the EU: cookie banners should be explicit OPT IN and the cookie should fire after the user hits accept
- Cookie banners should not block the site or be a condition of using the site
- Consider the cookie banner and mobile experience (don't block the site)
- The language should explain what cookies do (advertising, analytics, user experience)
- There should be a separate cookie notice
- In the US: cookie banners do NOT need to be explicit opt in
- In the US: under CCPA, cookies can be considered a sale of data

# What's the deal with cookie banners?

Cross Device Tracking







# What are my options?

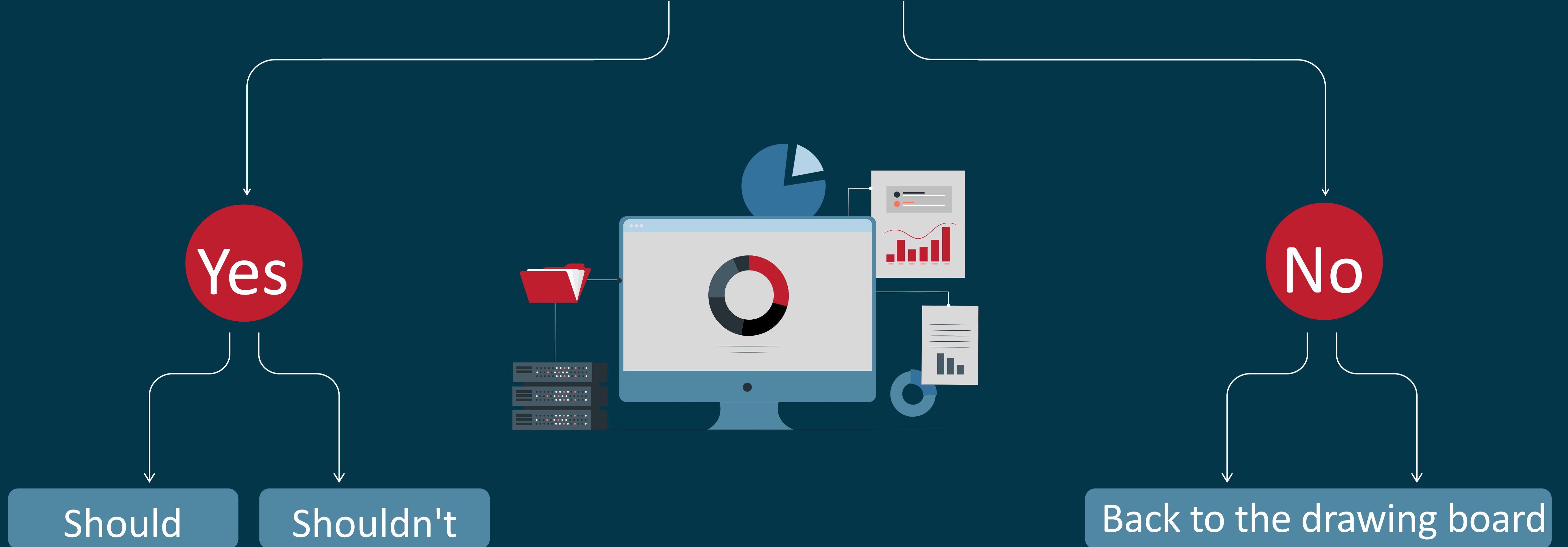


# Marketing responsibly





# Can I use this data?



# Privacy in Marketing Messaging



Privacy as a feature of a product and service



Privacy portal



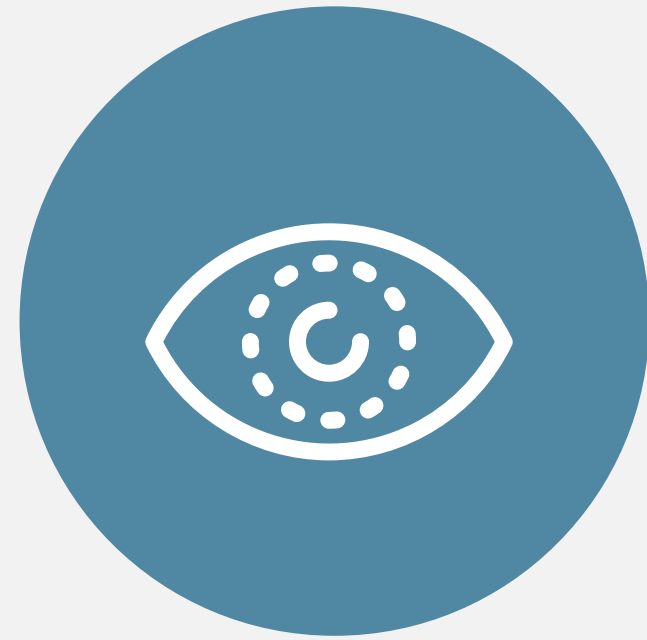
Consider objections to someone providing data or opting in



Explain the benefits of providing data



## Building Trust Through Privacy Notices



Updating and reviewing  
your privacy notice  
creates transparency with  
your customers



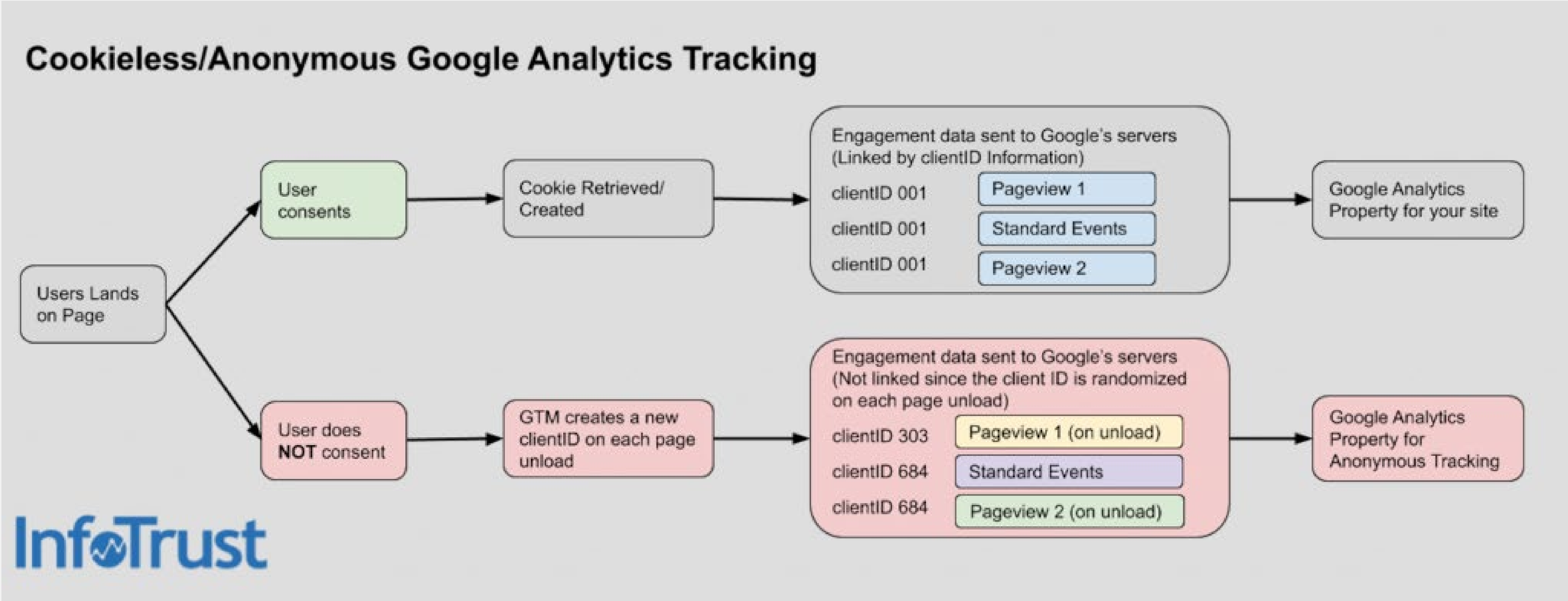
Knowing your data will  
help you create an  
accurate privacy notice  
and manage individual  
rights requests



Implementing the  
right compliance  
requirements can help  
strengthen customer  
relationships







This method will provide insight into an action was taken (pageview, event, or purchase), but provides no information on who took that action, where they came from, or any of their previous actions in that session or previous sessions.



## Move from cookies to identifiers



### Digital Fingerprinting:

by gathering variables like the browser name and version, screen resolution, list of fonts and plugins, and IP address and location, companies can identify unique users with 99% accuracy. Even though ad tech companies have promised the data used for these fingerprints don't contain any PII (personally identifiable information like name, email address, or phone numbers), the fingerprints remain privacy-invasive nonetheless.



### Demographic Attributes:

“Researchers from two universities in Europe have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes.” Even if no personally identifiable information is collected, ad tech companies can re-identify users using data from other data sets, collected or purchased.



### Browsing histories:

The dataset consists of two weeks of browsing data from ~52,000 Firefox users. The work replicates the original paper's core findings by identifying 48,919 distinct browsing profiles, of which 99% are unique

Source: <https://www.usenix.org/system/files/soups2020-bird.pdf>  
<https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/>  
<https://www.forbes.com/sites/augustinefou/2020/08/31/no-more-third-party-cookies---good-or-bad-news/?sh=3e9e64555948>



# Privacy – an opportunity to engage with customers



Building long lasting  
relationships built  
on trust



Companies who pay  
attention to privacy  
have a competitive  
edge.





Grab the slides and more

<https://www.redcloveradvisors.com/cbuswaw>







**RED**CL<sup>VER</sup>  
ADVISORS

THANK YOU

✉ [info@redcloveradvisors.com](mailto:info@redcloveradvisors.com)

🌐 [RedCloverAdvisors.com](https://RedCloverAdvisors.com)



# Appendix



## Agency/Advertiser Evolution & Efficacy

- In some studies, contextual targeting has been found to increase purchase intent by up to 63%.
- Rely on less accurate means of targeting or relying on more direct buys
- Reliance on more page level data attributes
- Despite the initial nosedive in programmatic buys pre- and post-GDPR enforcement, companies now have the opportunity to yield cleaner and more reliable data.

There has definitely been a noticeable dip in the efficacy across the ad industry with continued restrictions over the identifiers that have been typically used for personalization. However, there has been an emergence of the use of other methods that have been able to provide comparable results. These include:

- Digital fingerprinting
- Contextual advertising
- Use of other identifiers like IFA
- FLoC – federated learning of cohorts - proposes a new way for businesses to reach people with relevant content and ads by clustering large groups of people with similar interests. This approach effectively hides individuals “in the crowd” and uses on-device processing to keep a person’s web history private on the browser.
- Initial tests are seeing 95% conversion per dollar spent vs cookie-based advertising



# Privacy Tech Changes



## Apple - App tracking Transparency - IDFA will essentially not be available as a persistent identifier for IOS devices

- users will proactively receive prompts from their updated apple devices that require that users give permission for data collection to happen. If no permission is given, Facebook and other publishers can't track site and app activity through their pixels.
- users will be asked permission before apps can use their unique Identifier for Advertisers (IDFA) for third party ad tracking.
- Require privacy "nutrition labels" that give you a better idea of what's going on inside an app before you download it from the iOS App Store or Mac App Store. The labels will list what information an app collects, and present that visually on the app page, much like looking at the backs of labels in a grocery store.



## Chrome update - disabling third party tracking cookies

- Google Privacy Sandbox: working on tools that allow advertisers to target groups of users instead of directly targeting individuals

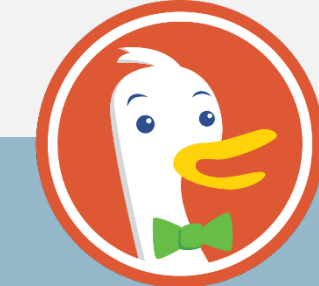
Google announced on 3/3/2020, that it plans to stop using or investing in tracking technologies that uniquely identify web users as they move from site to site across the internet in 2022.

- Google will not build alternative tracking technologies, or use those being developed by other entities, to replace third-party cookies for its own ad-buying tools.
- This could also further extend into the Android mobile environment.



## Firefox - Total Cookie Protection - will prevent cross-site tracking by siloing third-party cookies per website

- prevent websites from being able to 'tag' your browser, thereby eliminating the most pervasive cross-site tracking technique



## Global Privacy control - next generation "do not track" on your browser.

- It is a proposed specification designed to allow Internet users to notify businesses of their privacy preferences, such as whether or not they want their personal information to be sold or shared. It consists of a setting or extension in the user's browser or mobile device and acts as a mechanism that websites can use to indicate they support the specification.
- Currently live on Brave, Mozilla, DuckDuckGo

