March 23, 2022

CPRA Workshop

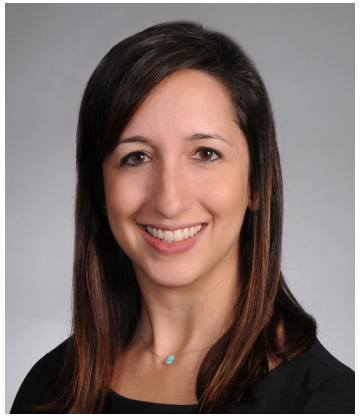
Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Adam Connolly

Partner, Cooley LLP
cyber/data/privacy
San Francisco



Miriam Farhi

Partner & Firmwide Co-Chair, Privacy & Security
Perkins Coie LLP

Drew Liebert

Former Chief Counsel
California Assembly
Judiciary Committee

Quick Overview of This Afternoon's Discussion

Part I: Quick CCPA-CPRA Legislative Overview / The New California Privacy Protection Agency / Rulemaking Status

Part II: Some Nuts and Bolts Of CPRA Compliance / Background / Expansion of Consumer Rights / Major Expansion of Business Obligations

Part III: Lingering CCPA Compliance Gaps / Contracting / Children / "Sale", "Share", "Limit", Oh my! / Sensitive Personal Information … and More

Part IV: Concluding Thoughts About California's Current Privacy Regulation Framework / Q & A

CPRA Workshop

2:00-4:30 PM

Privacy+ Security Forum

Legislative Overview

Privacy+ Security Forum

Original CCPA of 2018

- In response to growing concerns by McTaggart and privacy orgs, and vacuum of federal leadership, CCPA started as a statewide initiative measure for Nov. 2018 ballot.
- Goal was to empower consumers to reasonably discover what info businesses were collecting so they could tell businesses to stop selling or sharing their personal information.
- In response to the pending initiative, later withdrawn, Legislature quickly passed CCPA, signed by Gov. Jerry Brown. New law phased in, kicked off in Jan. 2020.

CCPA's New Consumer Rights

- Inspired in part by GDPR, CCPA sought to create broad new consumer rights over PI, including enhanced notice, access and disclosure rights.
- Also sought to create a right to deletion of inaccurate consumer information.
- Also intended to create right to restrict sale of information.
- Finally sought to deter discrimination against those who exercised these rights.

Enforcement Approach / AG Opinions and Regs

- CCPA provided two forms of enforcement (A) limited private enforcement re data breaches, and (B) broader public enforcement by state AG.
- AG tasked with developing regs to implement law, and draft legal opinions.
- August 2020: OAL approved initial set of AG regs. Process is ongoing, now moving to major new regs work under the new CPRA.

The New CPRA of 2020

- In response to broad concerns about CCPA, McTaggart & Hertzberg hit ballot again 2 years later with another initiative, Prop 24, to “fine tune” CCPA deficiencies.
- California Privacy Rights Act (CPRA) resoundingly passed on Nov. 3, 2020.
- Seeks to “clean up” CCPA inconsistencies (*stay tuned*); moves California’s privacy approach closer to GDPR; and expands consumer rights and creates new business obligations (*stay tuned*).
- Created whole new enforcement agency, California Privacy Protection Agency.

The New Privacy Protection Agency

- CPRA created new California Privacy Protection Agency (CPPA) to implement and enforce the law.
- New privacy agency first state agency of kind in nation governed by 5-member board.
- Chair is Jennifer Urban, a law professor and privacy expert at UC Berkeley Law School.
- New executive director is Ashkan Soltani, a privacy expert who worked at FTC.
- Relatively small budget ($10M) and small staff given the enormous tasks at hand.

Status of the New Required Regs for CPRA

- Agency's first task is to turn new CPRA into detailed regs, including how data is used for targeted ads and how algorithms use PI to make automated decisions.
- Must also determine how businesses must adhere to privacy preferences online users set in their browsers.
- "Listening tour": Agency workshops to be held across California to take public input.
- Executive Director Soltani: ***"We're building the car while we drive it."***

Nuts & Bolts of CPRA Compliance

Privacy+ Security Forum

What's New?

Privacy+ Security Forum

The Good News

- Cleans up certain inconsistencies/ambiguities created under the CCPA
- Heightens threshold requirements for a "business"
- Clarifies liability between businesses and their service providers and contractors
- Extends CCPA exemption for B2B and employee obligations to 2023
- Updates definitions, including for "personal information" and "service provider"

The Not-So-Good News (More Work)

- Moves law closer to the GDPR (data retention, data minimization/purpose limitation, security requirements)
- Expands consumer rights and creates new business obligations related to correction, "sharing" and sensitive PI
- Additional downstream contractual restrictions
- Expanded data breach liability
- Strengthens opt-in rights and enhances penalties vis-a-vis children's data
- Creates new enforcement agency, the California Privacy Protection Agency

What's New?

The Question Marks

The CPRA delegates 22 issues for additional rulemaking, including:

- the use of automated decision-making technology (including profiling);
- cybersecurity audits and risk assessments for high-risk processing;
- recordkeeping requirements; and
- requirements and technical specifications for an opt-out preference signal.

Key Terms & Dates

Privacy+ Security Forum

Who?

- Business
- Consumer

What?

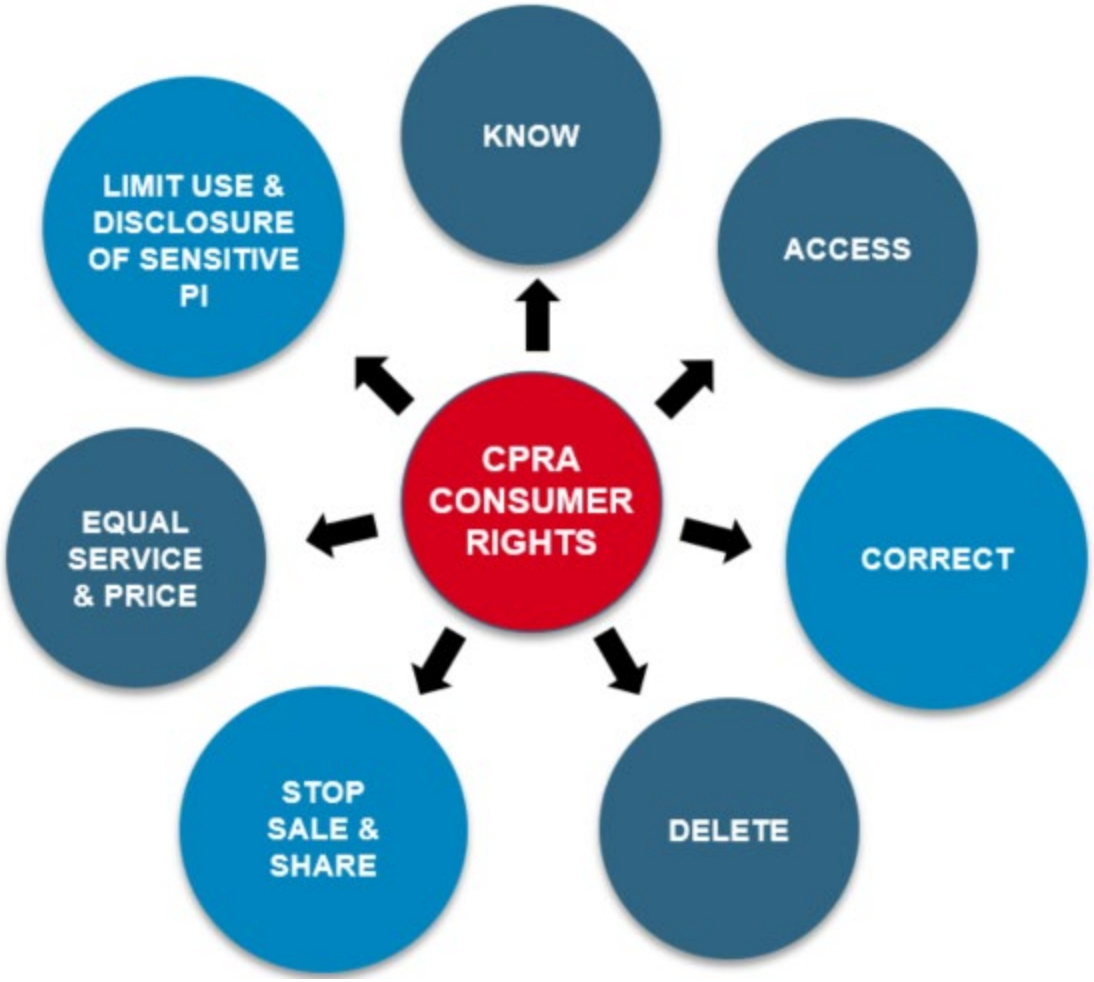
- Personal information
- Sensitive personal information

When?

- End of 2022: CPPA expected to adopt final regs
- Jan. 1, 2023: CPRA becomes fully operative
- July 1, 2023: CPPA can begin enforcing CPRA and regs

Expansion of Consumer Rights

Privacy+ Security Forum



Expansion of Business Obligations

Privacy+ Security Forum

- Data minimization
- Data retention
- Purpose limitation
- Contract requirements: service providers, contractors & third parties
- Auditing and risk assessment requirements
- Security
- Employee training

Key Issues & Compliance Challenges

Privacy+ Security Forum

Lingering CCPA Compliance Gaps

Privacy+ Security Forum

Have you updated your CCPA work since Jan 1, 2020?

- **August 14, 2020**. Final regs take effect
- **March 15, 2021.** Amendments to regs effective
- **Jan 2021.** AG guidance (via Tweet) re Global Privacy Control
- **July 2021.** AG enforcement case examples published.
- **January 28, 2022.** AG press release re CCPA's financial incentive requirements
- **March 10, 2022**. AG advisory opinion that 'right to know' includes inferences

Common gaps

- Not collecting opt-in consent to "sell" PI of Californians under age 16
- Saying interest-based advertising does not trigger a "sale" of PI
- Referring users to "self-serve" tools (DAA/NAI/browser settings) instead of processing opt-out requests
- Privacy policies lacking required detail
- Missing/broken DNSMPI links
- Not giving notice of financial incentive
- Not honoring Global Privacy Control signals
- Not following the regs' detailed rules for processing privacy requests
- Internal teams not yet trained on CCPA

CPRA Contracting

Specific language required in contracts with

- Service providers
- Contractors
- Third parties if you are “selling” to or “sharing” with them

Contracts must

- Contain requisite data use restrictions if counterpart is service provider or contractor
- Specify that the PI is sold or disclosed by the business only for limited and specified purposes
- Obligate the receiving party to comply with applicable CPRA obligations, including to provide the same level of privacy protection as is required by the CPRA
- Grant the business rights to take reasonable and appropriate steps to help to ensure that the receiving party uses the PI transferred in a manner consistent with the business’s CPRA obligations
- Require the receiving party to notify the business if it determines that it can no longer meet its obligations under the CPRA
- Give business the right to take reasonable and appropriate steps to stop and remediate unauthorized use of PI

CPRA Contracting

Privacy+ Security Forum

- How do we future-proof contracts we're drafting now?
- How do we retrofit existing contracts?
- How do we get vendors/partners to sign these when we have no leverage?

Children

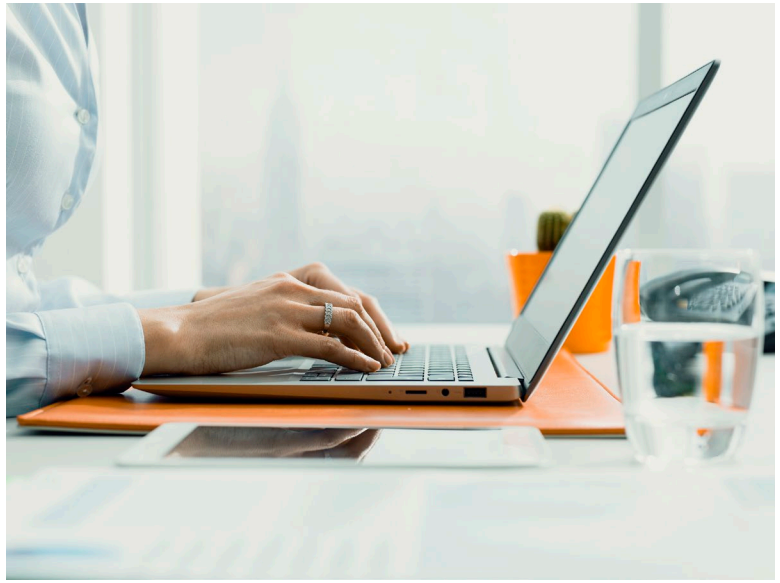
- Requirement to get opt-in consent to “sell” (and starting 1/1/2023, to “share”) PI of children under 16 was a sea-change of the COPPA status-quo
- Enforcement action expected to focus on children and CPRA increases fines to $7,500 per violation involving children
- Noncompliance widespread
- Technical implementation is complex; privacy tech solutions have not caught up
- COPPA savings clause helps with under 13 but not with 13-15

“Sell”, “share”, “limit”, oh my!

Privacy+ Security Forum

Website footers today

Do not sell my personal information



Website footers starting 1/1/2023

Do not sell or share my personal information
Limit the use of my sensitive personal information

OR

“A single, clearly labeled link…if that link easily allows a consumer to opt out of the sale or sharing…and to limit the use or disclosure of the consumer’s sensitive personal information.”

OR

None of the above if the business honors requests transmitted by platforms/technology/mechanisms to be specified in CPPA regs

Global Privacy Control

Privacy+ Security Forum

globalprivacycontrol.org

Manufacturer and Retailer Stopped Selling Personal Information
Industry: Consumer Electronics
Issue: Sales of Personal Information

A business that sells electronics maintained third-party online trackers on its retail website that shared data with advertisers about consumers' online shopping. The business neither imposed a service provider contractual relationship on these third parties, nor processed consumers' requests to opt-out that were submitted via a user-enabled global privacy control, e.g., a browser extension that signaled the GPC. After being notified of alleged noncompliance, the company worked with its privacy vendor to effectuate consumer opt-out requests and avoid sharing personal information with third parties under conditions that amounted to a sale in violation of the CCPA.

Sensitive personal information

Privacy+ Security Forum

What is in scope?

- social security, driver's license, state identification card, or passport number.
- account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- precise geolocation.
- racial or ethnic origin, religious or philosophical beliefs, or union membership.
- contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
- genetic data.
- biometric information processed for the purpose of uniquely identifying a consumer.
- PI collected and analyzed concerning a consumer's health.
- PI collected and analyzed concerning a consumer's sex life or sexual orientation.

What about publicly available PI?

- Not in scope.

What about the usage exemption?

- SPI collected or processed "without the purpose of inferring characteristics about a consumer" is exempt from "limit use" requests but exemption to be further defined in CPPA regs
- Does not apply to other CPRA requirements (e.g., privacy notices, risk assessments, audits)

Discussion

Privacy+ Security Forum

Why Is Privacy Important?
Some Reasons by Privacy Expert Dan Solove

Privacy+ Security Forum

It Limits Abuse of Power: Personal data can be used as a tool to exercise control over us.

It Encourages Respect for Individuals: If a person has a reasonable desire to keep something private, it is disrespectful to ignore that person's wishes.

It Helps Protect Reputations: Although we can't have complete control over our reputations, we must have some ability to protect them from being unfairly harmed.

It Enhances Trust in Others: In relationships, whether personal, professional, governmental, or commercial, we depend upon trusting the other party. Breaches of confidentiality on the Internet are breaches of that trust.

It Protects Freedom of Thought, Speech and Democracy: Privacy is key to freedom of thought and speech. We are witnessing in real time how government spying on individual privacy can quickly stamp out democratic institutions.

What Are Consumers' Top Three Internet Privacy Priorities According to Recent Surveys? Pew 11/2019

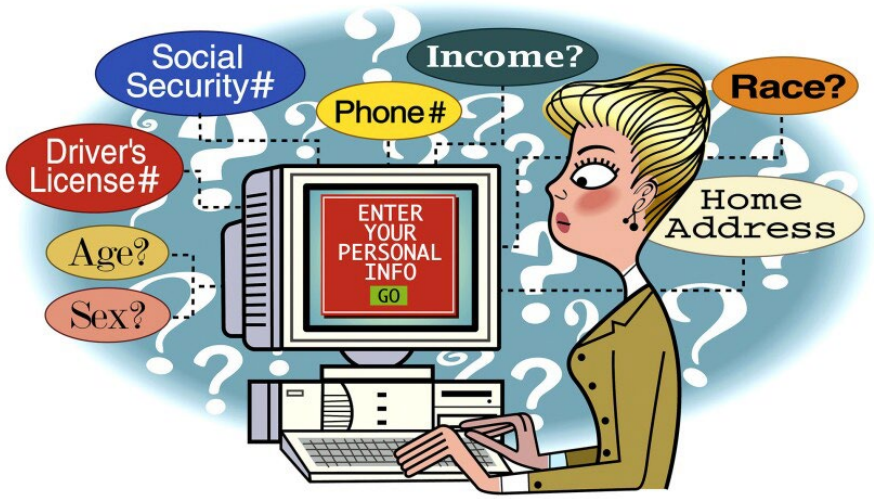
Privacy+ Security Forum

To Reasonably Prevent Other People and Orgs From Tracking Their Private Lives

To Reasonably Control Which of Their Personal Information Is Protected

To Reasonably Prevent Their PI From Being Sold Or Shared

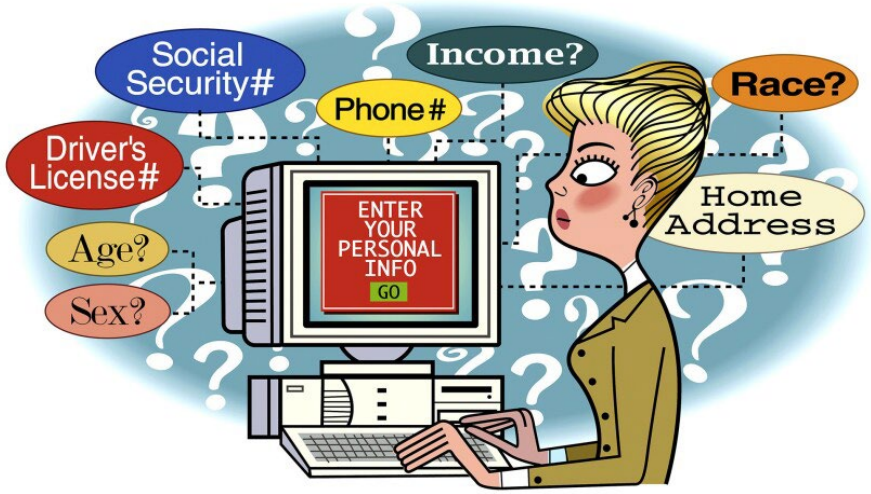
How Well Do Americans Think Businesses Are Complying With Their PI Wishes? Pew 11/2019



- ***Pew:*** Fully ¾ of Americans report feeling that all or most of what they do online, or while using their cellphone, is being tracked by advertisers.
- ***Pew:*** A whopping 81% of Americans feel as if they have little control over data collected about them by companies and government.
- ***Pew:*** 80% of Americans lack confidence that companies will honor their PI preferences or admit when they make mistakes with or misuse their data.

So How Well Do You Think California's Privacy Laws Are Protecting These Top Consumer Expectations?

Privacy+ Security Forum



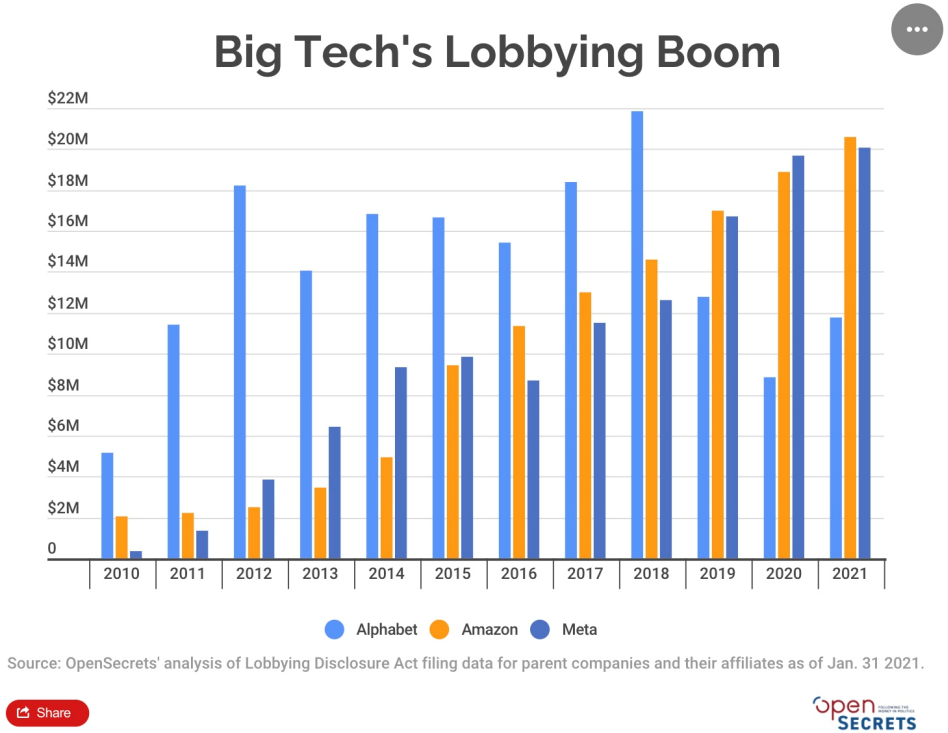
- To Honor Consumers' Typical Preference To Keep All Or Most Of What They Do Online, Or While Using Their Cellphone, From Being Tracked By Advertisers?
- To Give Consumers Confidence That They Have Reasonable Control Over the Data That Companies and Government Collect About Them?
- To Give Consumers Confidence That Companies Will Properly Honor Their PI Preferences And Inform Them When They Make Mistakes With, Or Purposely Misuse, Their Data?

If You Agree CPRA's Current Privacy Approach Appears to Falter in Protecting PI, It's Worth Considering How We Got Here

- California's tech sector has always had the political clout to defeat efforts by policy-makers to require consumers to affirmatively agree to "opt in" before businesses could sell or share their PI.
- State's privacy approaches – both CCPA and CPRA – have been enormously influenced by Silicon Valley – both were intensely negotiated political compromises ultimately found acceptable to the biggest players. Efforts by privacy groups to switch to an "opt in" approach have always been thwarted.
- We don't expect politicians to understand technical complexities of how to regulate nuclear power. Understanding how advertising ecosystem functions is not much easier – so it is no wonder politicians largely rely on the tech sector itself to explain what regulation will not "kill the economic goose that continually lays golden eggs in California."

So Just How Much Do The Big Technology Companies Spend to Influence Privacy and Other Tech Policies?

Privacy+ Security Forum



Internet industry organizations and corporations collectively spent more than $91.4 million on lobbying in 2021, a roughly $11 million increase from the previous year and an all-time high for the industry. The three top-spending platforms accounted for more than half of all internet industry lobbying spending in 2021.

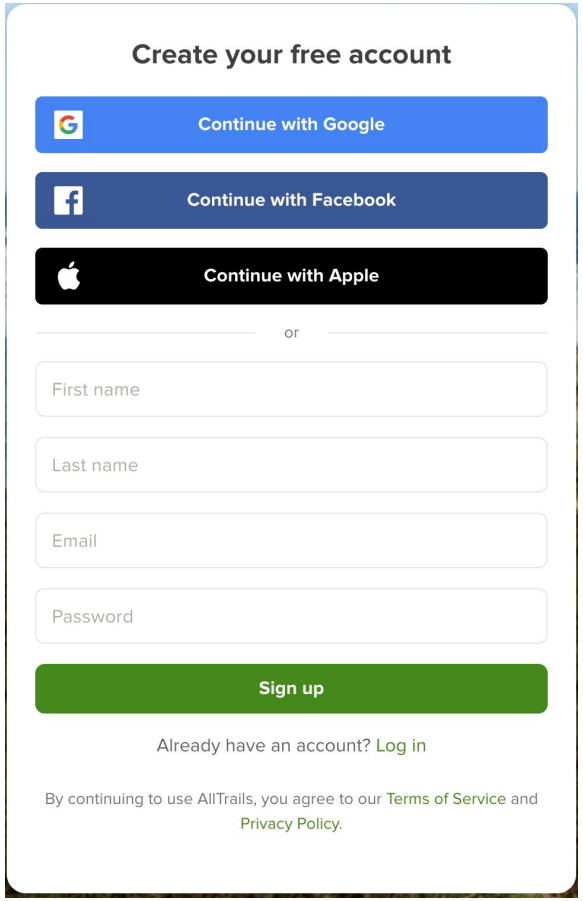
- The fact is that the privacy laws we have on the books today reflect what privacy approaches have been acceptable to California's technology sector.

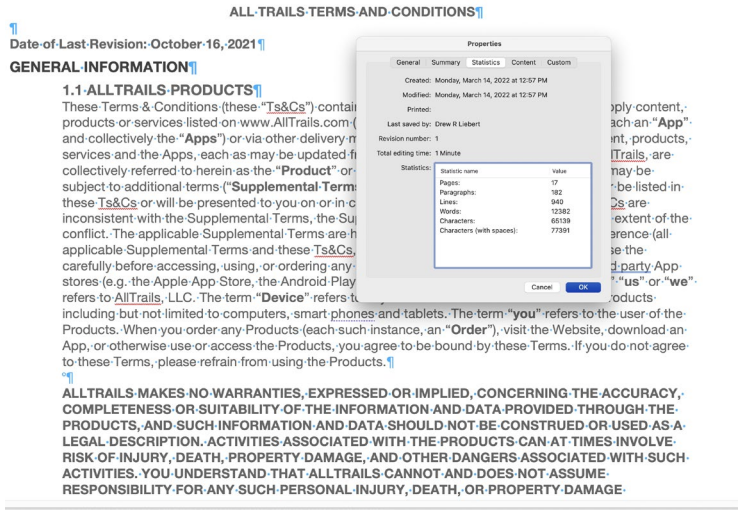
- Facilitating consumer privacy preferences, and consumer understanding of privacy rights, has not been goal of many of state's and nation's largest and most politically powerful technology companies.

T/F: ***Based on the percentage of consumers exercising their privacy preferences, our current privacy approaches appear to be serving the interests of America's technology sector much better than they are serving the privacy objectives of consumers?***

The Cynical "Click & Accept" Illusion

Privacy+ Security Forum





ALL·TRAILS·TERMS·AND·CONDITIONS¶

Date·of·Last·Revision:·October·16,·2021¶

GENERAL·INFORMATION¶

1.1·ALLTRAILS·PRODUCTS¶

These·Terms·&·Conditions·(these·"Ts&Cs")·contai… products·or·services·listed·on·www.AllTrails.com·(… and·collectively·the·"**Apps**")·or·via·other·delivery·m… services·and·the·Apps,·each·as·may·be·updated·f… collectively·referred·to·herein·as·the·"**Product**"·or·… subject·to·additional·terms·("**Supplemental·Terms**… these·Ts&Cs·or·will·be·presented·to·you·on·or·in·c… inconsistent·with·the·Supplemental·Terms,·the·Su… conflict.·The·applicable·Supplemental·Terms·are·h… applicable·Supplemental·Terms·and·these·Ts&Cs,… carefully·before·accessing,·using,·or·ordering·any·… stores·(e.g.·the·Apple·App·Store,·the·Android·Play… refers·to·AllTrails,·LLC.·The·term·"**Device**"·refers·t… including·but·not·limited·to·computers,·smart·phones·and·tablets.·The·term·"**you**"·refers·to·the·user·of·the·Products.·When·you·order·any·Products·(each·such·instance,·an·"**Order**"),·visit·the·Website,·download·an·App,·or·otherwise·use·or·access·the·Products,·you·agree·to·be·bound·by·these·Terms.·If·you·do·not·agree·to·these·Terms,·please·refrain·from·using·the·Products.¶

¶

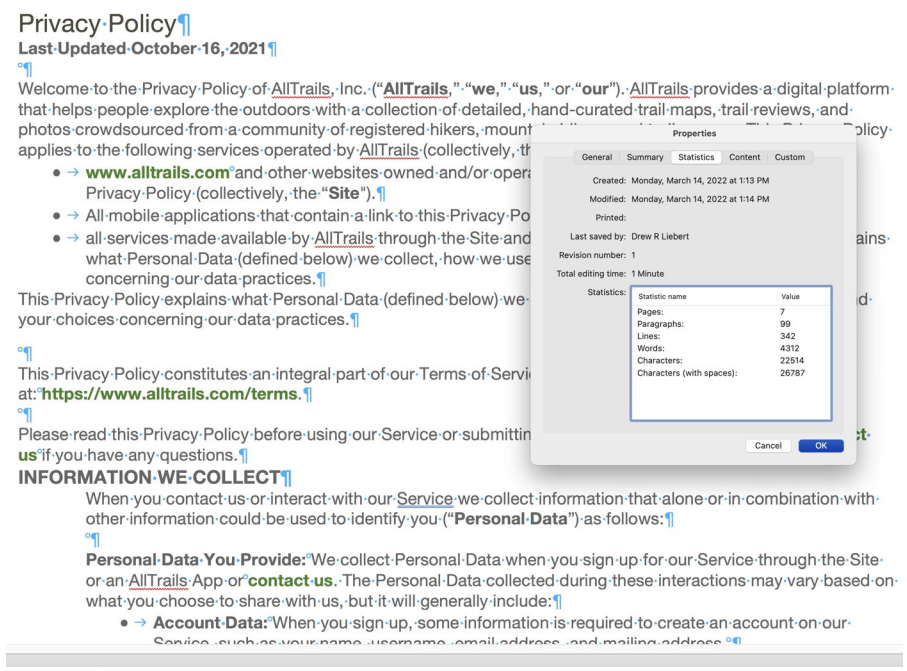
**ALLTRAILS·MAKES·NO·WARRANTIES,·EXPRESSED·OR·IMPLIED,·CONCERNING·THE·ACCURACY,·COMPLETENESS·OR·SUITABILITY·OF·THE·INFORMATION·AND·DATA·PROVIDED·THROUGH·THE·PRODUCTS,·AND·SUCH·INFORMATION·AND·DATA·SHOULD·NOT·BE·CONSTRUED·OR·USED·AS·A·LEGAL·DESCRIPTION.·ACTIVITIES·ASSOCIATED·WITH·THE·PRODUCTS·CAN·AT·TIMES·INVOLVE·RISK·OF·INJURY,·DEATH,·PROPERTY·DAMAGE,·AND·OTHER·DANGERS·ASSOCIATED·WITH·SUCH·ACTIVITIES.·YOU·UNDERSTAND·THAT·ALLTRAILS·CANNOT·AND·DOES·NOT·ASSUME·RESPONSIBILITY·FOR·ANY·SUCH·PERSONAL·INJURY,·DEATH,·OR·PROPERTY·DAMAGE·

- How many words do you think the typical "terms and conditions" policy contains? Over 10,000, with lots of legaleze. (***The typical policy at left is 12,382 words.***)
- According to Pew, what % of American consumers state they always read such policies? A paltry 9%! (***And isn't that likely a big exaggeration?***)

What % of Americans do you think routinely click "accept" in order to get the "free" services they desire without having the slightest idea of what they are agreeing to? Isn't this approach an obviously failed privacy framework? Aren't these classic examples of potentially unconscionable adhesion contracts?

The Similarly Impenetrable Privacy Policy Thicket

Privacy+ Security Forum


Privacy Policy

Last Updated October 16, 2021

Welcome to the Privacy Policy of AllTrails, Inc. ("AllTrails," "we," "us," or "our"). AllTrails provides a digital platform that helps people explore the outdoors with a collection of detailed, hand-curated trail maps, trail reviews, and photos crowdsourced from a community of registered hikers, mount… Policy applies to the following services operated by AllTrails (collectively, th…

- www.alltrails.com and other websites owned and/or opera… Privacy Policy (collectively, the "Site").
- All mobile applications that contain a link to this Privacy Po…
- all services made available by AllTrails through the Site and… ains what Personal Data (defined below) we collect, how we use… concerning our data practices.

This Privacy Policy explains what Personal Data (defined below) we… d your choices concerning our data practices.

This Privacy Policy constitutes an integral part of our Terms of Servi… at: https://www.alltrails.com/terms.

Please read this Privacy Policy before using our Service or submittin… t us if you have any questions.

INFORMATION WE COLLECT

When you contact us or interact with our Service we collect information that alone or in combination with other information could be used to identify you ("Personal Data") as follows:

Personal Data You Provide: We collect Personal Data when you sign up for our Service through the Site or an AllTrails App or contact us. The Personal Data collected during these interactions may vary based on what you choose to share with us, but it will generally include:

- Account Data: When you sign up, some information is required to create an account on our Service, such as your name, username, email address, and mailing address.

Properties

General | Summary | Statistics | Content | Custom

Created: Monday, March 14, 2022 at 1:13 PM
Modified: Monday, March 14, 2022 at 1:14 PM
Printed:
Last saved by: Drew R Liebert
Revision number: 1
Total editing time: 1 Minute
Statistics:

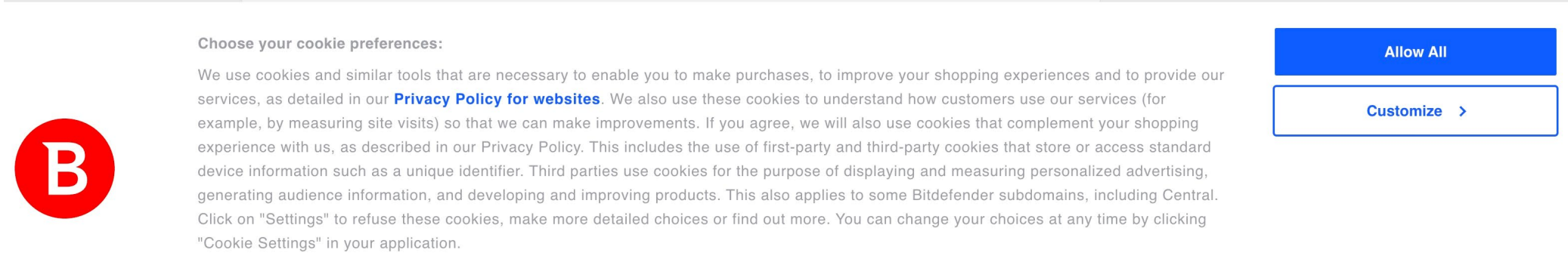
Statistic name	Value
Pages:	7
Paragraphs:	99
Lines:	342
Words:	4312
Characters:	22514
Characters (with spaces):	26787

Cancel OK

- Just like with "Terms & Conditions" policies, under our current privacy framework consumers are expected to agree to firm's "privacy policy" treatises that are typically oxymorons – policies stating precisely the opposite about how the business may often *use* rather than protect the consumer's PI. ***(The "privacy" policy to the left is atypically short – coming in at well over 4000 words.)***
- We all know these policies usually contain legal and technical terms that even many lawyers don't understand, let alone consumers. At least partially because of this, according to Pew, less than ¼ of Americans ever read privacy policies before they "accept" the services. And almost 2/3 of this already tiny number admit they understand "very little or nothing" after they actually try to read the privacy policies. ***(Isn't it likely higher than that?)***

“Want A Cookie?” The Latest Privacy Fallacy

Privacy+ Security Forum

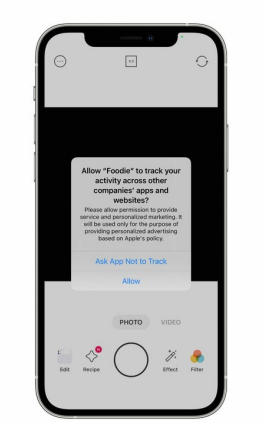


Not to pile on, but what percentage of consumers do you believe fully, or even partially, understand what they are agreeing to, often many times each day, when they now routinely click the “Allow All” button in order to accept a service’s “cookies”? (*Bet it’s less than 10% at best, don’t you agree?)*

Aren’t consumers too often being asked to agree to a fundamentally secretive and deceptive digital ecosystem they don’t understand, one that is fundamentally premised on a lack of lucidity and transparency?

Will Apple's Recent Approach to "Opt-In" Help to Transform the Privacy Ecosystem?

Privacy+ Security Forum



- As you know, last year Apple shook up many in the digital world with its IOS update that contains a powerful new consumer privacy control called "App Tracking Transparency." Indeed, just use of the term "transparency" appeared pathbreaking.
- With this new and relatively easily accessible privacy preferences tool, app developers can no longer presumptively host tools to track user data from within an app to broadly identify user information to better target consumers with ads, and sell those ad opportunities to other companies and businesses.
- Against FaceBook's cries, this privacy development strikes at the heart of the current secretive digital ad ecosystem that has kept consumers in the dark about whether their PI is being sold or shared. It is a potentially user-friendly "opt in" approach that might have a major impact on more effectively and reasonably protecting consumers' privacy wishes.

Is the Key Question Now Whether It's Simply Too Late to Effectively Protect Our Privacy on the Internet?

Privacy+ Security Forum

- The CCPA said a key goal was "putting consumers back in charge of their own data." (*Californians for Consumer Privacy,* https://www.caprivacy.org.)
- As Prof. Solove has noted, the current privacy approaches – which are premised on *consumers* having the burden to take extensive affirmative actions to protect their privacy preferences – "put too much of the onus on individuals to fight a war that they cannot win…People lack the expertise to make meaningful choices about their data… Effective privacy protection involves not just facilitating individual control but also bringing the collection, processing, and transfer of personal data under control." -- "*The Limitations of Privacy Rights*," Daniel J. Solove, Feb. 2022.

Some Final Big Picture Questions: Is it too late to put the "data genie" back in the bottle? Can the CCPA/CPRA "opt out" framework, which fundamentally rely on consumers confronting overwhelming hurdles to manage their privacy preferences ever really meet consumer expectations to be able to reasonably, and easily, protect their PI?

Closing Remarks

Privacy+ Security Forum

Q&A

Privacy+ Security Forum