

Balancing Consumer Privacy in Publishing: From GDPR to CCPA

Sara DePaul, SIIA's Senior Director of Technology Policy



Accelerating Innovation in
Technology, Data & Media

An Important Disclaimer: This Presentation Is NOT Legal Advice

The information provided in this presentation is not intended to constitute legal advice. Instead, all information and content in this presentation – both written and oral – is for general information purposes only.

If your needs go beyond information and require legal counsel, please contact your organization's in-house or outside counsel. If your organization does not have counsel, I can provide contact information for legal counsel upon request.



Accelerating Innovation in
Technology, Data & Media

What are our goals today?

- Introduction to the EU's General Data Protection Regulation (GDPR), the U.S. Federal Approach to Privacy, and the California Consumer Privacy Act (CCPA)
- Identifying Short-, Medium-, and Long-Term Business Outlook
 - Short-Term: Compliance with CCPA and Advocacy for a Federal Law
 - Medium-Term: Watching GDPR Enforcement Trends and Guidance
 - Long-Term: Preparing for Changes in Transborder Data Flows



Accelerating Innovation in
Technology, Data & Media

But First, What is SIIA?



Accelerating Innovation in
Technology, Data & Media

Divisions of SIIA





SIIA Public Policy



SIIA

Accelerating Innovation in
Technology, Data & Media

Goal 1: A Quick Introduction to Three Privacy Regimes that Impact Marketing Activities



GDPR



U.S. Federal Law



California
Consumer Privacy
Act



SIIA

Accelerating Innovation in
Technology, Data & Media

What is GDPR?

Omnibus, standardized European data protection law with extraterritorial application

Seven Principles: (1) lawfulness, fairness, and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage limitation, (6) integrity and confidentiality, and (7) accountability

Restricts automated decision making and profiling

Confers data subject rights

Distinguishes between data controllers and data processors

Penalties as high as 4% of global turnover



Accelerating Innovation in
Technology, Data & Media

Any other important European laws?

YES, the *ePrivacy Directive*, and the proposed ePrivacy Regulation

- The ePrivacy Regulation will supplant the ePrivacy Directive, and help conform the standards governing commercial electronic privacy to the GDPR
- Its scope will cover all business providing online communications services, including electronic direct marketing:
 - To require consent before marketers can send email or text messages
 - Cookies will be tracked within settings each user can control to do away with pop-up requests for consent
 - To require the same data security as required in a brick and mortar



Accelerating Innovation in
Technology, Data & Media

Privacy on the Federal Level

FTC Act: 1933 provision that prohibits deceptive and unfair practices

Fair Credit Reporting Act: protects information collected by consumer reporting agencies

Gramm-Leach-Bliley Act (and Safeguards and Privacy Rules): sets standards for financial institutions to protect financial privacy

CAN-SPAM Act: sets opt-out and other standards for commercial

TSR: regulates telemarketing, including opt-out (DNC lists) and opt-in for robocalls

COPPA: regulates children's privacy, requiring parental opt-in

FACTA (Pre-Screen Opt-Out Rule): authorizes and requires notices for consumers' to opt out of receiving prescreened credit offers

HIPAA: regulates the disclosure of health data



Accelerating Innovation in
Technology, Data & Media

What is the CCPA?

California privacy law that regulates the collection and sale of a consumer's personal information to third parties and service providers. It applies to for-profit entities with some exceptions and it applies extraterritorially

Broad definition of personal information

Opt-out regime (except for consumers under 16)

Consumer rights: Notice, Access, Control, Deletion, and Portability

Enforced by the California Attorney General, with civil penalties from \$2,500 to \$7,500 per violation with no cap

Private right of action for data security incidents

Implements on January 1, 2020; Enforcement Date is July 1, 2020



SIIA

Accelerating Innovation in
Technology, Data & Media

Goal 2: Identify Short-, Medium-, and Long-Term Business Marketing Outlooks Based on GDPR and CCPA

Short-Term: ramp up for compliance with the CCPA and support Congress passing a comprehensive federal privacy law

Medium-Term: watch for relevant GDPR enforcement and guidance for tweaks to your compliance plan

Long-Term: pay attention to international trends regarding privacy, including policy and legal updates for cross-border data flows



Accelerating Innovation in
Technology, Data & Media

Short-Term Goal: CCPA Compliance

Note: the presumption here is that if GDPR applies to your organization that you've already undertaken a compliance program. If not, that should be your immediate goal.

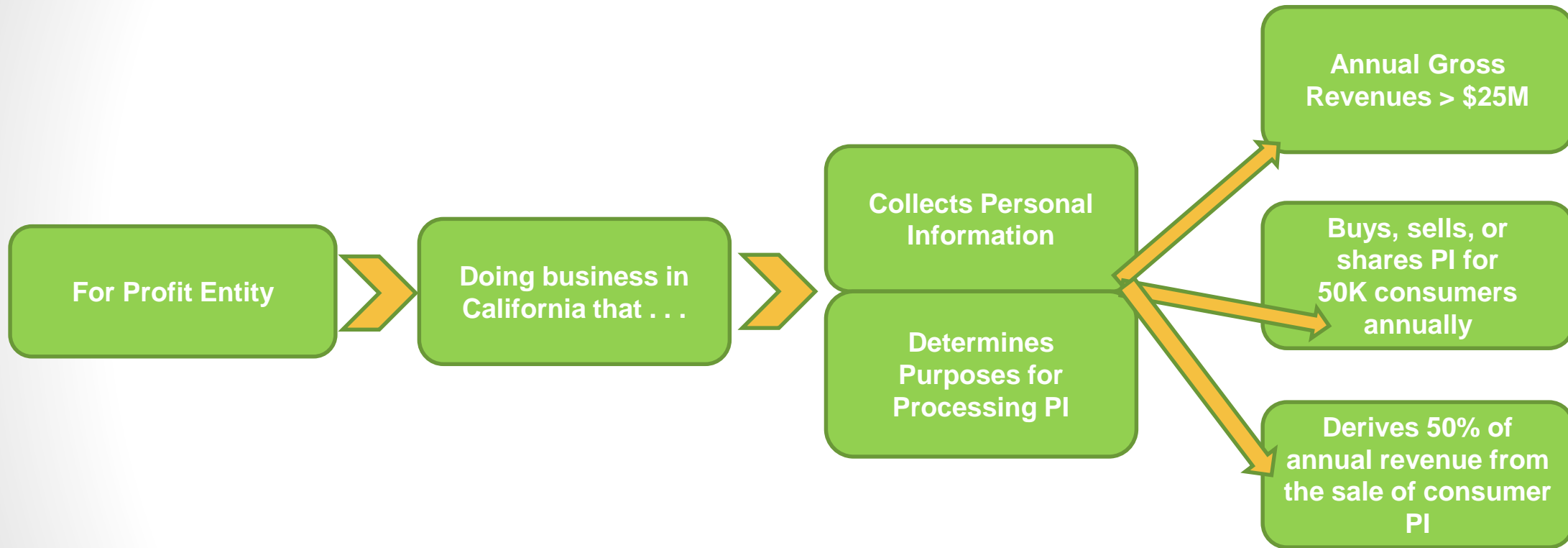
Questions:

- Does CCPA apply to you?
- If it does, what types of personal information are covered by it?
- If it does, what does consent for marketing look like under CCPA?
- What other important restrictions may apply?



Accelerating Innovation in
Technology, Data & Media

Does CCPA apply to your organization?



What is personal information under CCPA?

- *Information that identifies, relates to, describes, is capable of being associated with, **or could reasonably be linked, directly or indirectly, with a particular consumer or household.** Personal information includes, but is not limited to, the following:*
 - *Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*
 - *Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.*
 - *Biometric information; audio and video.*
 - *Browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement and geolocation information*
 - *Professional or employment-related information.*
 - *Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.*



Accelerating Innovation in
Technology, Data & Media

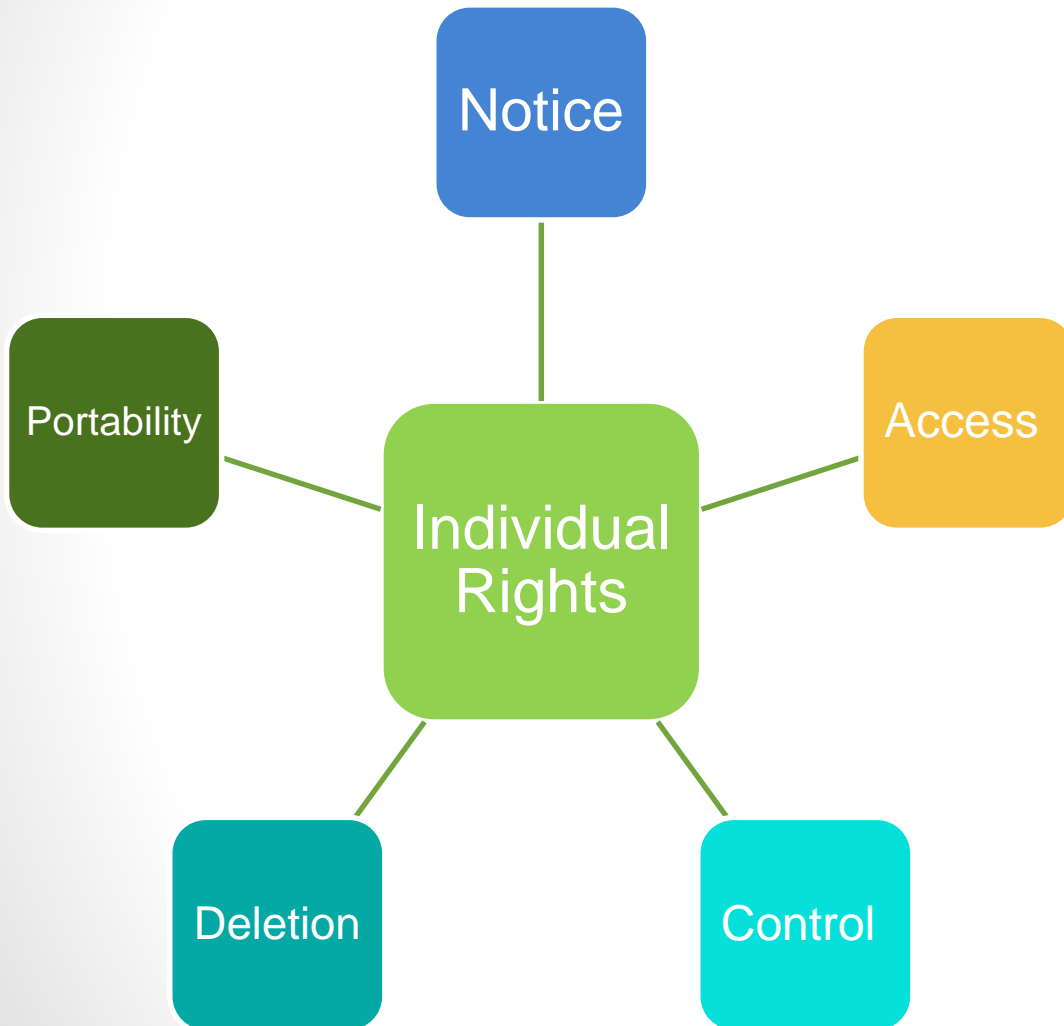
In other words

Practically EVERYTHING, even down to a household level



Accelerating Innovation in
Technology, Data & Media

What is the intention of the CCPA?



To further privacy “by giving consumers an effective way to ***control their personal information***”
(emphasis added)

What does this mean for consent?

First, for direct marketing, consumers have a right to know what you are collecting about them, how the information will be used, and whether that information will be sold to a third party. They also have a right to delete the information.

Second, consumers have the right to control who has access to their information through an opt-out right to the resale of their personal information.

Conclusion: CCPA incentivizes that you build trust with the consumers and that you engage in direct marketing through first-party data collection



Accelerating Innovation in
Technology, Data & Media

What should you watch for?

Possible Amendments: to fix unclear definitions, bring the CCPA into alignment with the First Amendment regarding public domain information, and fix poor policy choices in drafting (*i.e.* extension to employees and the prohibition on loyalty programs)

AG Rulemaking: the process began on January 8, 2019 and is expected to focus on:

1. Identifying the categories of personal information subject to the CCPA;
2. Defining 'unique identifiers' under the CCPA'
3. Exceptions to CCPA where it is necessary to comply with federal or state law;
4. Submitting and complying with consumer requests'
5. Uniform opt-out logo or button to promote consumer awareness of CCPA rights
6. Notices and information to consumers; and
7. Verifying consumer requests.



Accelerating Innovation in
Technology, Data & Media

Short-Term Goal: Federal Advocacy

- Numerous Senate, industry, and civil society proposals
- Gang of Six: Wicker, Cantwell, Blumenthal, Schatz, Thune, and Wyden
- Rep Schakowsky has stated intention to write a House Bill




The Economist Topics ▾ Current edition More ▾

The Cambridge Analytica bill

Congress is trying to create a federal privacy law

The fourth attempt in 45 years turns on how federal law will supersede state laws



Print edition | United States >
Feb 28th 2019 | SAN FRANCISCO

Twitter Facebook LinkedIn Email Print

CONGRESS FIRST tried to pass a privacy law in 1974. Lawmakers succeeded, but lobbying from financial services companies ensured that it applied only to the government, not private firms. Impetus to regulate privacy in the private sector waxed and waned over the next 30 years, building with the first tech bubble, then evaporating in the horror of the 2001 attacks. In 2012, Barack Obama tried again and failed.

Almost half a century after their first effort, politicians are having a fourth go, triggered by the Cambridge Analytica scandal. Some have already offered their own bills, and work is now under way to knit all those into a bipartisan offering. Ranking Republicans and Democrats held two hearings on Capitol Hill this week with the explicit goal of informing the federal privacy bill. The discussion was familiar to privacy wonks—how transparent data collection should be, what limits there should be on it, how to avoid burdensome regulation—but the environment in which it took place suggests it might be fourth time lucky.

What are the hot policy issues?

Public Domain Information

- Exemption
- First Amendment

Preemption

- How to draft it?
- How to get Dem support?

Enforcement

- Strengthen the FTC?
- Role of the States?
- Need to avoid private right of action

Consumer Protection

- What is the basis of the law?
- Abandon the FIPPs?
- Interoperability



SIIA

Accelerating Innovation in
Technology, Data & Media

Medium-Term Goal: GDPR updates on lawful processing



Relevant bases for marketing are **legitimate interest** and **consent**

For **sensitive data**: you must identify a lawful basis under Art. 6 AND a separate condition under Article 9



SIIA

Accelerating Innovation in
Technology, Data & Media

How to decide?

Legitimate Interest

Consent

Risk-based

Balancing your legitimate interests against individual's privacy

Clear, Affirmative Act

Freely given

Specific, informed, and unambiguous

- **Legitimate Interest:** No enforcement actions have addressed legitimate interest to date, but it will most likely meet standards when it falls within the reasonable expectation of the consumer (such as in direct marketing or contextual advertising)
- **Consent:** remember the standard is affirmative act (i.e. opt-in) and that withdrawing has to be as easy as it was to give consent. Required for electronic marketing
 - CNIL fined Google \$50M
 - Expected actions on forced consent
 - Watch for Apple investigation
 - No contact with the data subjects? Then don't forget the individual rights – Polish DPA fined a marketing company for scraping public record data



SIIA

Accelerating Innovation in
Technology, Data & Media

Medium-Term Goal: GDPR Updates on Storage Limitation

Article 5(3) requires that personal data be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*

What does this mean?

- No specific time limits for erasing or anonymizing personal data
- Factors to consider: (1) do you need to keep a record of the relationship with the data subject once the relationship ends and (2) do you need to keep information to defend future legal claims or otherwise meet legal requirements
- Danish DPA: **fined Taxa 4x35 €180,000** for failing to delete records on 9 million taxi rides after they were no longer needed (company attempted to comply with Art. 5 by anonymizing data after two years, but in practice it only removed customer names, keeping all other data, including phone numbers and ride histories, for five years for purposes of business analytics)



Accelerating Innovation in
Technology, Data & Media

Long-Term Goal: Watching out for International Trends and Updates

New or Amended Laws Aligned with GDPR

Brazil

Serbia

Jersey

Anticipated Amended Laws to Align with GDPR

Bosnia and Herzegovina

Ukraine

North Macedonia

Montenegro

Monaco

Malaysia

Switzerland

Amended Laws

Uruguay

Israel

Peru

Chile (constitutional amendment)

Anticipated New Laws

India

Indonesia

Honduras

Kenya

Zimbabwe

British Virgin Islands

New Zealand

Two Big International Factors to Watch

Canada

- Recently announced a Digital Charter that could lead to amendments to PIPEDA
- OPC currently has an open consultation on the Digital Charter and whether to add a consent requirement to transborder data flow

India

- New government elected
- What will happen with the draft Indian Privacy Law?



SIIA

Accelerating Innovation in
Technology, Data & Media

Questions?
sdepaul@siia.net



Accelerating Innovation in
Technology, Data & Media

CRAIN



Data Regulatory Compliance

2019 AABP - Audience Development Track

Bonnie Roche, CCIO
Crain Communications Inc

June 29, 2019

Being Compliant – What Does It Mean to Me?

- Changes to how we collect, process, use and share data means diligence to **revising and enforcing Data Management & Protection Policies**. Impacts:
 - All channels
 - Future & past data collected (list rental, opt-in, non-PII data)
 - Vendors that support brand business and store or process customer data (considered Processors)
 - Establishing **Data Governance Team** and **Data Protection Lead**
- Updates to **Privacy Policy**
- Updates site for **Data Consent Management** (allow customers to manage cookies and data collection)
- Updates to **HR Policies** about internal use for **Employee Data**

Checklist

At risk processes:

- ✓ Opt-in Process
- ✓ Past Data Mgmt Process
- ✓ Lead Generation Process
- ✓ Collect Forms
- ✓ Contracts
- ✓ Consent Manger
- ✓ Privacy Policy
- ✓ Vendor compliance Notification
- ✓ 3rd Party List Management

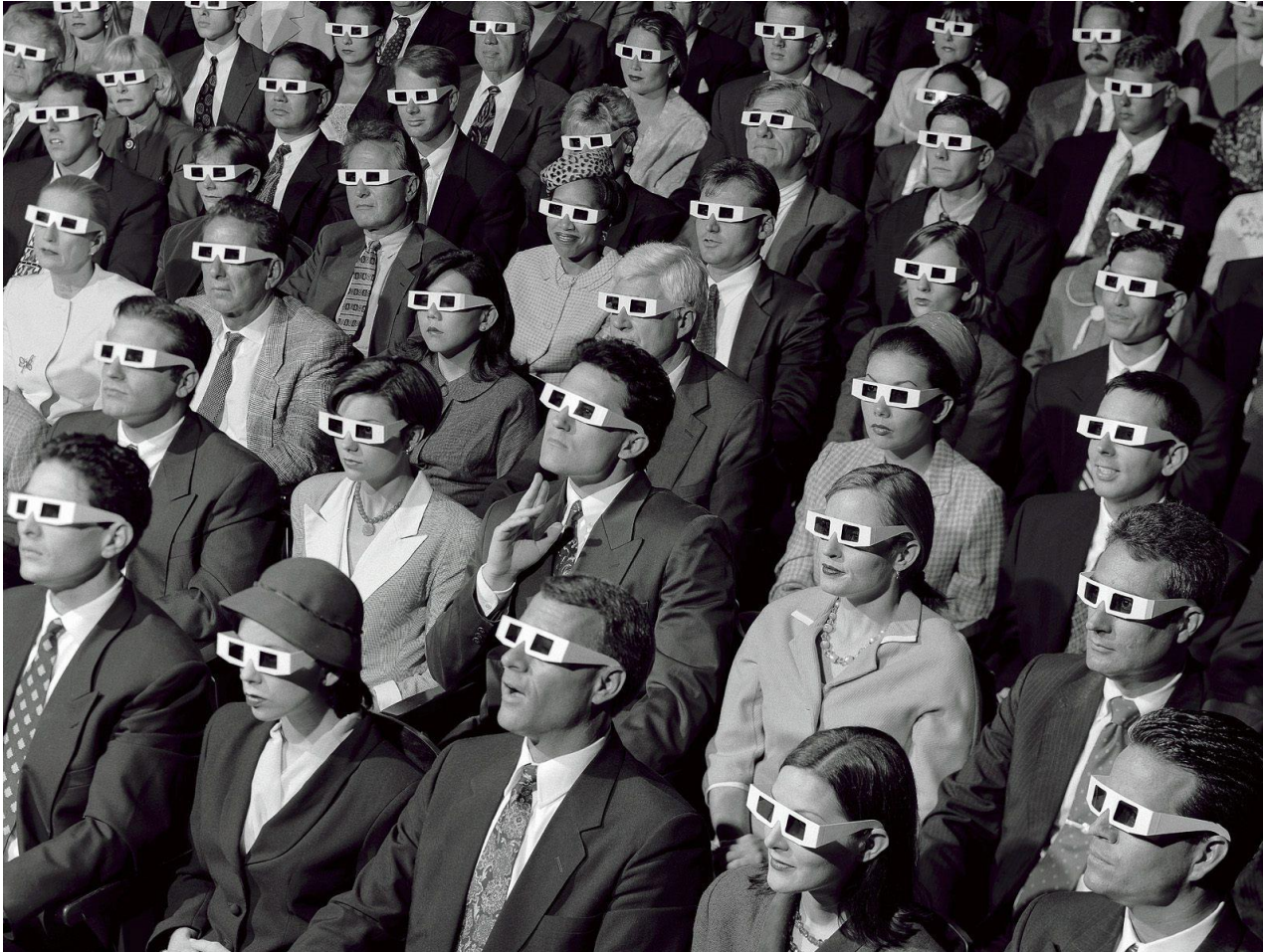
Other Documentation & Process

- ✓ Ability to track consent and messaging associated with each campaign
- ✓ Create Data Breach Policy and Processes
- ✓ Create Right to Be Forgotten Process
- ✓ Create Standard Response for inquiries from clients or vendors
- ✓ Qualify vendors for Compliance

This could be serious

- So What?
 - Be in the know about the **data permission rules**. Don't need to be an expert, but know where to find them.
 - Create a data governance team and make them accessible to answer any questions.

Audience Impact Inevitable



- Newsletter List Sizes
- Digital Access List Sizes
- Higher Engagement

Stay in the Know

It isn't yet clear which, if any, legislation could secure enough support to become law. But the comments from Mr. McCarthy and others indicated that there was significant bipartisan support for establishing stronger privacy guidelines.

House GOP Leader Backs a Data-Privacy Law

By KRISTINA PETERSON AND LINDSAY WISE



WASHINGTON—House Minority Leader Kevin McCarthy backed the idea of national legislation to safeguard consumers' data privacy, adding a prominent GOP voice to the bipartisan support in Congress for tackling how technology companies amass and use that information.

Lawmakers from both parties in the House and Senate have been working on many bills aimed at strengthening individuals' ability to control their data collected by the biggest technology companies, including Alphabet Inc.'s Google, Facebook Inc. and Apple Inc.

It isn't yet clear which, if any, legislation could secure enough support to become law. But the comments from Mr. McCarthy and others indicated that there was significant bipartisan support for establishing stronger privacy guidelines.

"There needs to be a national-level regulation, not state-by-state on what we're going to do about privacy," Mr. McCarthy, a California Republican, said in an interview Thursday with *The Wall Street Journal*. "We should know what data you keep on us. We should be able to take our data and be able to delete our data."

Mr. McCarthy said he plans to introduce legislation that would ensure that people know what data companies are tracking and allow them to transfer or delete that data.

A data-privacy law passed last year in California helped spur action from both Mr. McCarthy and Sen. Wicker (R., Miss.) and Sen. Marsha Blackburn (R., Miss.) in the House to continue to use online sites. Passage of the California law helped spur the formation in the U.S. Senate of a group last year that is drafting what its members hope will be landmark data-privacy legislation.

Composed of members of the Commerce Committee, the working group are expected to meet Friday to discuss the draft legislation. Mr. Wicker hopes to introduce a bill before the Senate's August recess, a goal primarily driven by a desire to get the bill passed before the California law takes effect in January, according to a GOP aide familiar with the discussions.

Richard Blumenthal of Connecticut, the top Democrat on the Commerce Committee's consumer protection panel, said there was "very powerful support for privacy legislation across party lines because of the discussions."

Technology companies have warmed to a national privacy law as the implementation of the California law would be less stringent and provide a sole set of guidelines. Supporters of big tech companies have warned against regulation that could threaten competition.

Some Democrats have called for taking more forceful action to limit the power of the biggest technology companies. Sen. Elizabeth Warren (D., Mass.), who is running for president, called in March for breaking up some companies, including Amazon.com Inc., Google and Facebook, saying they have too much power over the economy, and urged regulation of Google and Facebook as utilities.

Mr. McCarthy said he disagreed with the idea of breaking up big tech companies.

Some lawmakers were skeptical that Congress would be able to agree on an approach to privacy guidelines. "I hope that we'll pass something, but you know, we'll see," said Sen. Josh Hawley (R., Mo.), a freshman lawmaker who has introduced two bipartisan privacy bills of his own since taking office in January.

Technology companies have warmed to a national privacy law as the implementation of the California law would be less stringent and provide a sole set of guidelines. Supporters of big tech companies have warned against regulation that could threaten competition.

Some Democrats have called for taking more forceful action to limit the power of the biggest technology companies. Sen. Elizabeth Warren (D., Mass.), who is running for president, called in March for breaking up some companies, including Amazon.com Inc., Google and Facebook, saying they have too much power over the economy, and urged regulation of Google and Facebook as utilities.

Mr. McCarthy said he disagreed with the idea of breaking up big tech companies.

Rep. Kevin McCarthy favors national regulation of consumer data over a state-by-state approach.

Bipartisan support for federal regulation has grown since rules in California passed.

group includes the panel's chairman, Roger Wicker (R., Miss.) and Sen. Marsha Blackburn (R., Miss.) of Washington, the committee's top Democrat.

CRAIN

Implement Consent Management Platform - TrustArc

Consent Manager Platform Overview

Preference Manager

- TrustArc currently powers the AdChoices on Crain sites that offer or will offer first party ad targeting
- Enables a customer to opt-out from receiving ads from certain providers

Consent Manager

- TrustArc's Consent Manager product provides additional functionality allowing a customer to manage the data collected when on a site or from various 3rd providers
- Provides comprehensive reporting and audit trail to support GDPR compliance

CRAIN Your Advertising Choices

How does it work?

Advertisers may collect data about your online browsing activity and use it to show you targeted ads (a process known as "behavioral advertising").

You can prevent the companies listed below from showing you targeted ads by submitting opt-outs. Opting-out will only prevent targeted ads so you may continue to see generic (non-targeted ads) from these companies after you opt-out.

You may opt in to behaviorally targeted ads anytime by deleting your browser's cookies.

[Industry Resources - US](#)
[Industry Resources - Canada](#)
[Industry Resources - EU](#)

Multiple opt-outs Select All

Company	Company Type	Status	Opt-out
151Media	Demand Side Platform (DSP)		<input type="checkbox"/>
33Across	Ad Platform	no cookie	<input type="checkbox"/>
(24)7.ai Inc (Formerly Engageclick)	Ad Platform		<input type="checkbox"/> Learn More
Acuity Ads	Demand Side Platform (DSP)	no cookie	<input type="checkbox"/>

[Submit Opt-outs](#)

Your Choices Regarding Cookies on this Site

Please choose whether this site may use Functional and/or Advertising cookies, as described below:

- REQUIRED COOKIES**
These cookies are required to enable core site functionality.
- FUNCTIONAL COOKIES**
These cookies allow us to analyze site usage so we can measure and improve performance.
- ADVERTISING COOKIES**
These cookies are used by advertising companies to serve ads that are relevant to your interests.

Functionality Allowed

- Provide secure log-in
- Remember how far you are through an order
- Remember your log-in details
- Remember what is in your shopping cart
- Make sure the website looks consistent
- Allow you to share pages with social networks
- Allow you to post comments
- Serve ads relevant to your interests

[CANCEL](#) [SUBMIT PREFERENCES](#) [ADVANCED SETTINGS](#)

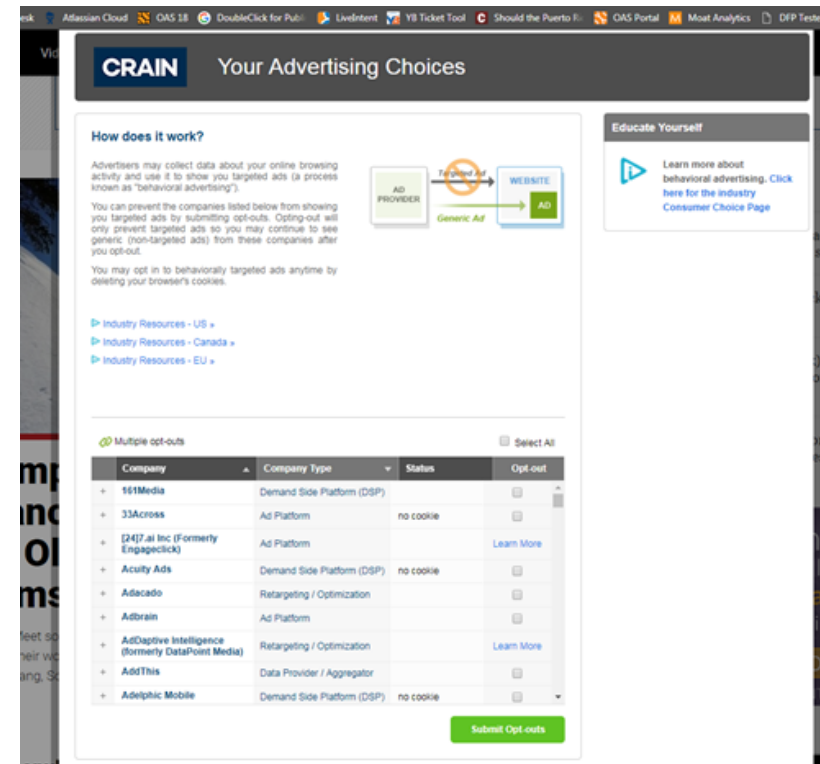
Privacy Policy | Powered by TRUSTe

Preference Manager: US/CA

For **US/Canada sites**, we utilize the Preference Manager which is part of the Consent Management Platform. This product allows users the ability to opt out of specific vendor cookies.



Users will see an “AdChoices” link typically in the footer of the site. Once you click on the “AdChoices” link, you will see the screen to opt-out of each vendor:



CRAIN Your Advertising Choices

How does it work?

Advertisers may collect data about your online browsing activity and use it to show you targeted ads (a process known as “behavioral advertising”).

You can prevent the companies listed below from showing you targeted ads by submitting opt-outs. Opting-out will only prevent targeted ads so you may continue to see generic (non-targeted ads) from these companies after you opt-out.

You may opt in to behaviorally targeted ads anytime by deleting your browser's cookies.

[Industry Resources - US](#)
[Industry Resources - Canada](#)
[Industry Resources - EU](#)

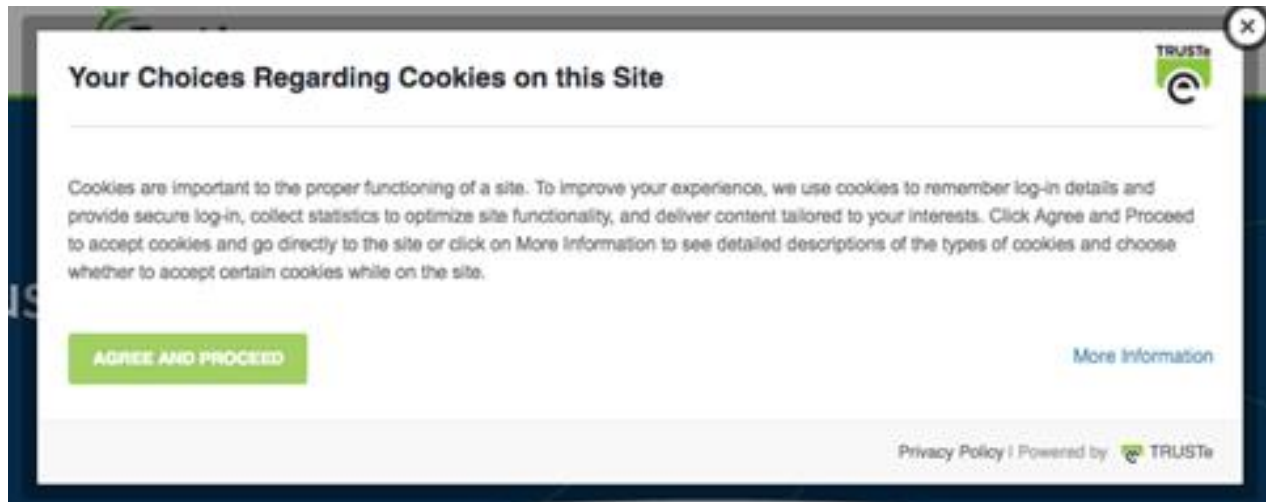
Multiple opt-outs Select All

Company	Company Type	Status	Opt-out
+ 161Media	Demand Side Platform (DSP)		<input type="checkbox"/>
+ 33Across	Ad Platform	no cookie	<input type="checkbox"/>
+ [24]7.ai Inc (Formerly Engageclick)	Ad Platform		<input type="checkbox"/> Learn More
+ Acuity Ads	Demand Side Platform (DSP)	no cookie	<input type="checkbox"/>
+ Adacado	Retargeting / Optimization		<input type="checkbox"/>
+ Adbrain	Ad Platform		<input type="checkbox"/>
+ Adaptive Intelligence (formerly DataPoint Media)	Retargeting / Optimization		<input type="checkbox"/> Learn More
+ AddThis	Data Provider / Aggregator		<input type="checkbox"/>
+ Adelphic Mobile	Demand Side Platform (DSP)	no cookie	<input type="checkbox"/>

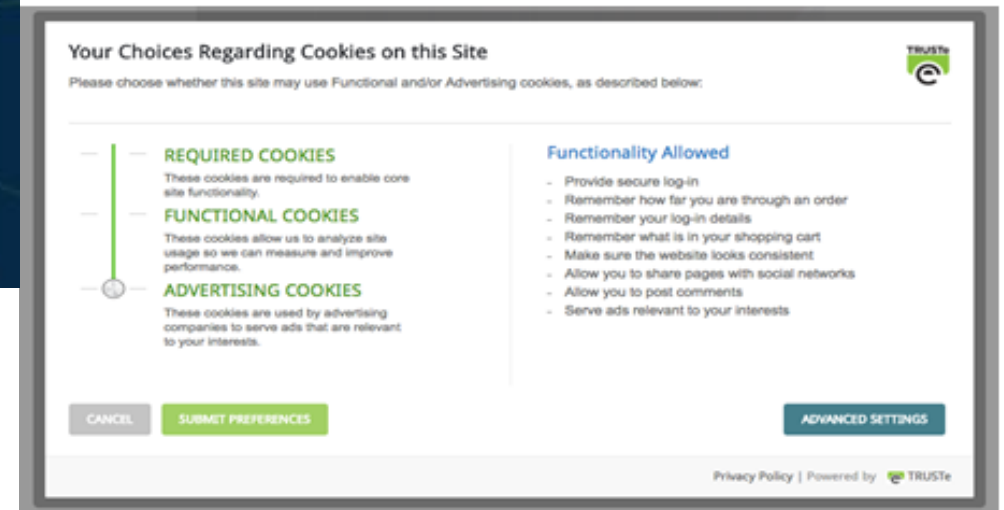
[Submit Opt-outs](#)

Consent Manager: EU (Expressed Consent)

Expressed Consent – Users will see an explicit pop-up on the page. Users cannot interact with the page until consent is provided.



When user clicks on “More Information” the consent manager will pop up and they will be given the option to opt-in of Required, Functional, and Advertising cookies.

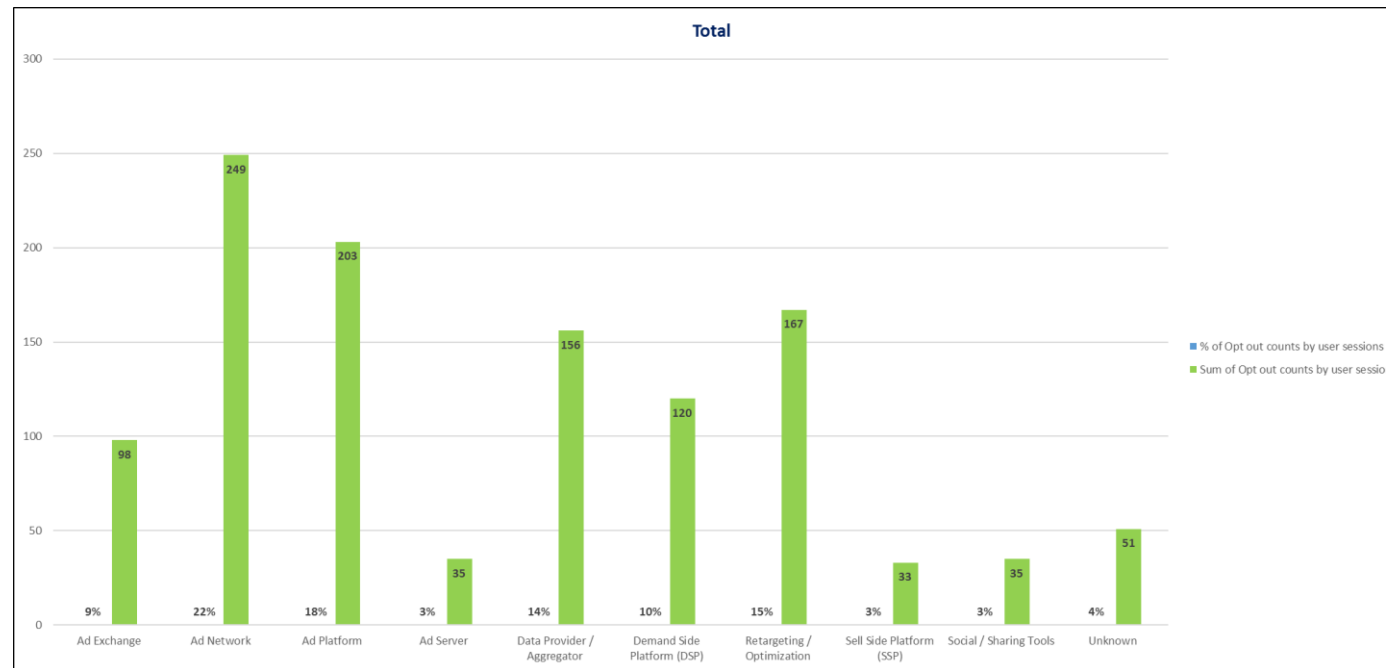


Once the user has given consent, they won't see the pop-up again for another 13 months. However, users have an option to change their preferences anytime by clicking on the “Cookie Preferences” button at the bottom of the page.



Preference Manager: Reporting

- Within the Preference Manager, we are able to get the total numbers of opt-out selections per vendor and vendor type.
- The opt-out numbers represents the number of user sessions which involved a user opting out. This does not exactly correlate to unique users as a user could have opt out of more than one vendor in one session.



Consent Manager: Reporting

- We are able to report on # of users who have seen the expressed interstitial (pop-up)
- Data is further broken down by % of users who opted in to each cookie category (required, functional, and advertising)

Metrics Definitions	
Expressed Consent	
New Views	Number of new users who opened/viewed Consent Manager
Returns	Number of previously seen TrustArc cookie users
Clicks	Number of clicks to open/re-open the Consent Manager. Note: for Expressed this metric ONLY correlates to returning users
Agree	Number of users who selected "Agree and Proceed"
More Info	Number of users who selected "More Info/Set Preferences"
Ask Me Later	Number of users who selected "Ask Me later". Note: Only for those sites that have implemented this button
Close	Number of users who clicked "X" or close button. Note: Only available for expressed to returning users
Advertising	Number of users who clicked "More Info" and then selected "Advertising" Category
Functional	Number of users who clicked "More Info" and then selected "Functional" category
Required	Number of users who clicked "More Info" and then selected "Required" category
# of people who saw the interstitial	Sum of New Views + Sum of Clicks
% of "Agree & Proceed"	Sum of Agree & Proceed / (Sum of New Views + Sum of Clicks)
% of "Ask Me Later"	Sum of Ask Me Later / (Sum of New Views + Sum of Clicks)
% of "More Information"	Sum of More Info / (Sum of New Views + Sum of Clicks)
% of Advertising Opt-in's	Sum of Advertising / (Sum of New Views + Sum of Clicks)
% of Functional Opt-in's	Sum of Functional / (Sum of New Views + Sum of Clicks)
% of Required Opt-in's	Sum of Required / (Sum of New Views + Sum of Clicks)
% of "Close"	Sum of Close / (Sum of New Views + Sum of Clicks)
Adjusted Bounce Rate	$((\text{Sum of Clicks} + \text{Sum of New Views}) - (\text{Sum of Agree \& Proceed, Ask Me Later, Advertising, Functional, Required, Close})) / (\text{Sum of New Views} + \text{Sum of Clicks})$

Consent Manager: GDPR Compliance

- Consent manager also provides a report of all opt-in selections to comply with GDPR requirements
- Report is broken out by day along with a user's partial ip address, cookie category, vendor name, consent location (website), and country

Found 569779 results. Showing 1 - 25.

Date	Script in Use	Country	Behavior	Category	OS Type	Browser Type	Partial IP	Company	Domains	Consent Location
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	161Media	ads.creative-serving.com, creative-serving.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	33Across	cdn.tynt.com, de.tynt.com, sc.tynt.com, tynt.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	Acuityads Inc.	acuityplatform.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	AddToAny	addtoany.com, static.addtoany.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	Adelphic LLC	ipredictive.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	Adform A/S	adform.net	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	AdGear Technologies, Inc.	cm.adgpx.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	ADDITION technologies AG	adfarm1.adition.com	adage.com
06/13/2019 00:00:04 EST	crain.com	GB	implied	Advertising Cookies	iOS 12.3.1	Mobile Safari UI/WKWebView 12.3.1	xx.xx.242.121	Admedo Ltd	pool.admedo.com	adage.com

Document Process

The screenshot displays the CRAINIUM website interface. At the top left is the CRAINIUM logo. To its right is a navigation menu with links for INSIDE CRAIN, CORPORATE DEPARTMENTS, BRANDS, RESOURCE CENTERS, and DIRECTORY. Below this is a green banner with the breadcrumb path "Resource Centers > Compliance Policies > Compliance Files >" and a dropdown arrow. The main heading of the banner is "GENERAL DATA PROTECTION (GDPR) POLICIES". Below the banner is a secondary navigation menu with links for HOME, CRAINIUM HELP, HELP DESK, PRESSRUN LEARNING FORUM, DRUPAL 8/CMS, and COMPLIANCE POLICIES. Underneath the navigation is a "Download This Folder" button with a folder icon. To the right of this button are two icons: a list view icon and a grid view icon. Below these elements is a table with a "Title" header and one row containing the document "GDPR Data Breach Response Policy.docx" with a document icon and a dropdown arrow.

CRAINIUM INSIDE CRAIN ▾ CORPORATE DEPARTMENTS ▾ BRANDS ▾ RESOURCE CENTERS ▾ DIRECTORY

Resource Centers > Compliance Policies > Compliance Files > ▾

GENERAL DATA PROTECTION (GDPR) POLICIES

HOME CRAINIUM HELP ▾ HELP DESK PRESSRUN LEARNING FORUM DRUPAL 8/CMS COMPLIANCE POLICIES

Download This Folder

Title ▲
GDPR Data Breach Response Policy.docx ▾

Update Consent Language

- Develop suggested content and placement related to GDPR compliant language on forms. Work with your legal council to ensure language meets compliance laws in all countries that you do business.
- Language must be near the conversion action (aka - button or opt-in box)
- Language & un-checked vs. pre-checked options can be altered depending on country – GDPR, Canada, US, Rest of World if the system being used can do this. Remember that each iteration must be documented for any compliance complaints, so the more variations of this, the more tracking will need to be done.

The screenshot shows a form titled "A Future in Digital Health: Transforming Healthcare for Patients and Providers" from Modern Healthcare. The form is for requesting a white paper. It includes fields for First Name, Last Name, Organization Name, Facility/Organization Type, Title, Email Address, Country, State, and a dropdown menu for State (currently showing Alabama). Below the form is a "Download" button. To the right of the form is an "About" section with text describing the white paper's focus on digital transformation in healthcare. At the bottom right is the SAP Health logo.

Modern Healthcare

PERSPECTIVES special advertising content

A Future in Digital Health: Transforming Healthcare for Patients and Providers

Fill out the form for **instant access** to the white paper:

First Name:

Last Name:

Organization Name:

Facility/Organization Type:

Title:

Email Address:

Country:

State:

Alabama

By clicking below, you consent to receive emails from us related to this content, and for us to share your contact information with the content sponsor who may contact you, by email or otherwise, about their related products and services. You may unsubscribe or change your email preferences through links in emails you receive. For more information, see Modern Healthcare's Privacy Policy.

Download

SAP Health

More About GDPR



EU Countries

Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France

Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands

Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom

Personal Data

DATA SUBJECT = any information relating to **an identified** or **identifiable** natural person.

Article 4. (1)

IDENTIFIABLE NATURAL PERSON = one who can be **identified**, **directly or indirectly**, in particular by reference to an identifier such as:

IDENTIFICATION NUMBER		LOCATION DATA	
NAME		ONLINE IDENTIFIER	
FACTORS SPECIFIC TO THE DATA SUBJECT'S:			
PHYSIOLOGICAL	PHYSICAL	GENETIC	SOCIAL IDENTITY
CULTURAL	MENTAL	ECONOMIC	HASHED ID



NEW PII DEFINITION

PREVIOUS POSITION

In place since 1996 Directive

- Name
- Contact details
- Job role
- Lifestyle
- Demographics

NEW POSITION

Expanded GDPR definition

- ID number
- Biometric data
- Economic data



Certain online identifiers

- IP address
- **Cookies**



MAC Address	00.90.d1.01.6b.9e
IP Address	172.20.161.0
Subnet Mask	255.255.255.0
Default Gateway	172.20.161.1

EXPANSION: Any data which enables a **living** individual to be identified directly or indirectly such and any online **identifiers that can be linked to an individual**

When Can I Use Customer Data?

Crain focus =

- Consent
- Legitimate Interest
- Performance of Contract



MEMBER STATES SHALL PROVIDE THAT PERSONAL DATA MAY BE PROCESSED ONLY IF:

- (a) The data subject has **unambiguously** given his consent; *or*
- (b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; *or*
- (c) Processing is necessary for **compliance with a legal obligation** to which the data controller is subject; *or*
- (d) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; *or*
- (e) Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed, **except where such interests are overridden by the interests for fundamental rights and freedoms** of the data subject which **require protection**.

Some EU countries viewed legitimate interests as an open door to justifying data processing which does not fit in one of the other legal grounds, but GDPR requires harmonization that will supersede this lesser standard.

Clear Consent

1995 Data Protection Directive Article 4. (h)

Any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

General Data Protection Regulation Article 4. (11)

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

What Does Clear Consent Mean?

LEGAL BASIS: CONSENT

- 1 Requires clear affirmative action to signify agreement
- 2 Consent may be withdrawn at any time
- 3 Consent for processing sensitive personal data must be explicit
- 4 Must be able to Demonstrate that 'Compliant' consent was given:

A Data Subject's consent to processing of their PII data must be:



So...



Freely? No!



Not Clear!



Affirmative?



Too Generic!

How To get Consent?

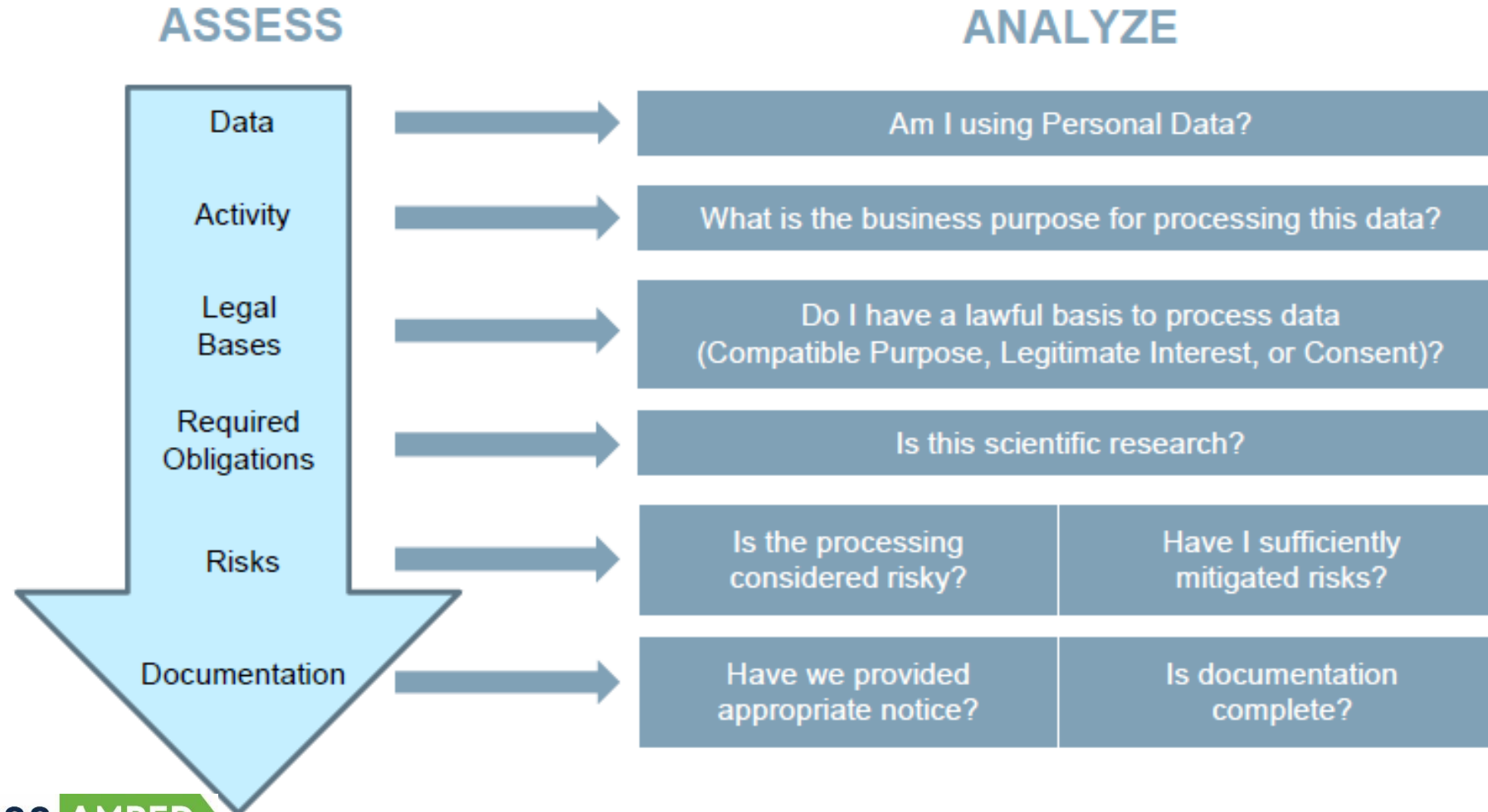
- **PRE-TICKED** boxes or **INACTIVITY** should not constitute consent.
- When the processing has **MULTIPLE** purposes, consent **should be given for all** of them.
- If the data subject's consent is to be given following a request by electronic means, the request must be **clear, concise**, and not **unnecessarily disruptive**, to the use of the service for which it is provided.



Legitimate Interest

- See the [ICO Overview](#) for a full listing of the
 - ...[M]ost appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
 - If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
 - There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
 - identify a legitimate interest;
 - show that the processing is necessary to achieve it; and
 - balance it against the individual's interests, rights and freedoms.
 - You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

Assessment Criteria to Use



Data Subject Rights

