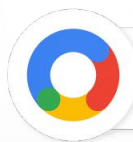


Embracing Data Privacy in Digital Marketing

Nashville AMA

January 10, 2024

InfoTrust is a privacy-centric digital analytics solutions company that empowers marketers to make confident, data-driven decisions.



Google Marketing Platform
Sales Partner



Google Cloud
Partner



LUCAS LONG

*Head of Global Privacy Strategy,
InfoTrust*

Cincinnati | Chicago | Dubai | Barcelona | Cebu City | Manila



The information we'll cover today is not intended to be legal advice or counsel and is not represented as such by InfoTrust.

We do not make any warranties or statements regarding the legal acceptability of the information presented in this webinar. Action performed as a result of the information provided are of your/your company's own choosing.

Please obtain legal advice from legal counsel whenever taking action related to the law.



Current State

What changes, what stays the same

Key Privacy Considerations

Requirements of privacy laws in the United States

How to Approach the Compliance Environment

Core principles and solutions available

Key Takeaways

If nothing else, focus on these items

Answers to Your Questions


Fire away!

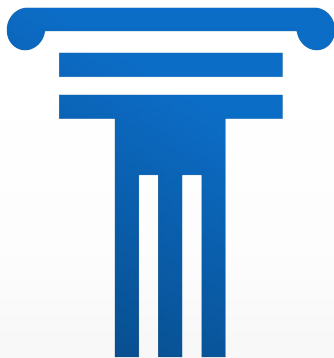
91% of internet users aged 16-74 say they are more likely to shop with brands that provide offers and recommendations that are relevant to them

Meanwhile...

- 68% of internet users feel skeptical about the way companies use their data in marketing
- Ad blocker usage estimated between 30-40% across the US and EU
- Internal InfoTrust analysis estimates between 30-40% of users decline cookie consent on EU retail websites when presented in a compliant way
- Apple ATT opt-in rates as low as 25%

How to accomplish core use cases in a privacy-centric way?

- Audience definition/creation
 - On-site personalization
 - Media campaign optimization
 - User experience optimization
 - Site interaction reporting
 - Content evaluation
- 



Respect User
Privacy



First-Party Ownership
of First-Party Data



Decisions and Actions
from Insights

**Comprehensive State Privacy
Laws**

**State Laws for Specific
Activities**

Federal Laws

Healthcare Specific Laws

California

Virginia

Colorado

Connecticut

Utah

Tennessee

- Effective July 1, 2024

Oregon

- Effective July 1, 2024

Texas

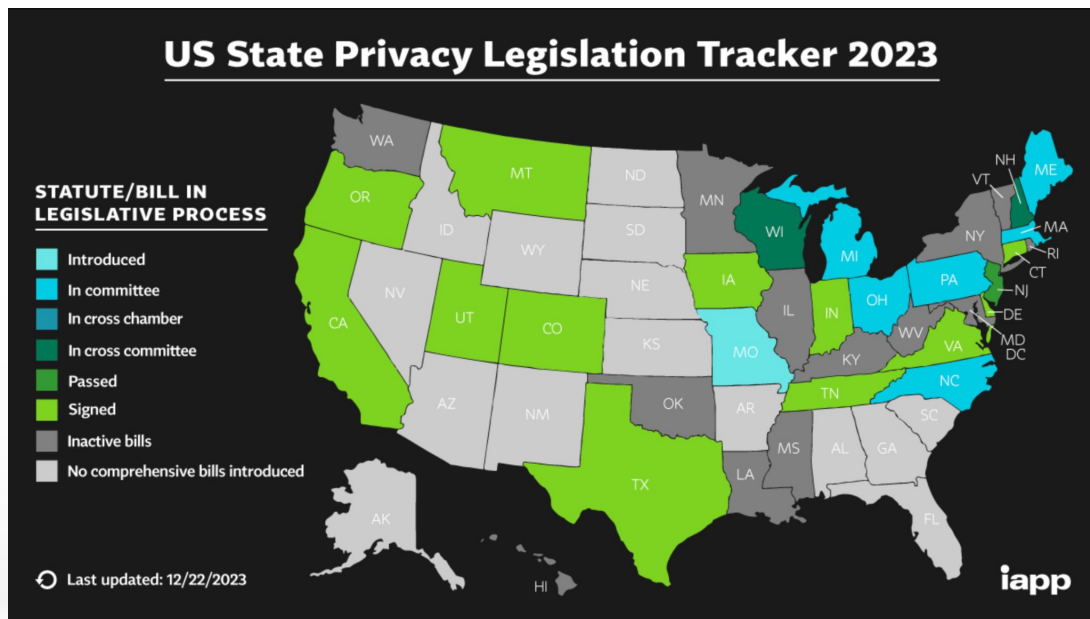
- Effective July 31, 2024

Montana

- Effective October 1, 2024

Iowa, Delaware, Indiana

- Effective 2025+



Applicability

U.S. state privacy laws set minimum thresholds for businesses to be in scope

This part applies to persons who conduct business in the state of Tennessee or produce products or services that are targeted to residents of the state and that:

- During a calendar year, control or process personal information of at least one hundred thousand (100,000) consumers; or
- Control or process personal information of at least twenty-five thousand (25,000) consumers and derive more than fifty percent (50%) of gross revenue from the sale of personal information.

Common exceptions

- HIPPA covered entities - covered by HIPPA
- Non-profit organizations

Consumer expectations – Some statistics to ponder...

66% of customers say they will stop buying from companies that misuse their data (Adobe & Advanis)

49% in the Americas said they would choose to switch from their preferred brand to their second choice brand after a positive privacy experience with their second-choice brand (Google research)

81% of people said they preferred to buy from brands that are honest about what data they collect and why (Google research)

Personal Information

Limits and requirements for activities involving “personal information”

Information that identifies, relates to, or describes a particular consumer or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer

Some stated examples:

- Identifiers such as a real name, alias, unique identifier, online identifier, internet protocol address, email address, account name, social security number, driver 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;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;



Digital Advertising



Email Marketing



Web Analytics



Experience
Personalization

Consumer Rights

Laws grant consumers specific rights as it relates to their personal information

1. **Transparency / Disclosure**
 - a. What is collected, to whom it is disclosed, how/why it is used, what is the impact on the consumer, consumers' rights
2. **Access**
3. **Correct inaccuracies**
4. **Delete personal information**
5. **Opt-out of the 'sale' of personal information**
 - a. Most states also include opt-out of 'sharing' for certain use cases

Controller Obligations

Companies that collect and process personal information have specific requirements

1. **Data minimization**
2. **Technical and operational protections for personal information**
3. **Do not unlawfully discriminate**
4. **Only process sensitive data with consent**
5. **Transparency & disclosure**
6. **Data Protection Assessments**

Processing Activities (w/ Personal Information)

- Targeted advertising
- “Sale” of personal information
- Profiling, where foreseeable risk of:
 - Unfair or disparate impact on consumers
 - Financial, physical, or reputational injury
 - Intrusion upon the solitude or private affairs where the intrusion would be offensive
 - Other substantial injury
- Processing of sensitive data
- Activities that present a heightened risk of harm

Obligations

- Identify and weigh benefits against potential risks to the rights of consumers
- Identify and implement safeguards to mitigate risks
- Factoring in use of deidentified data and relationship expectations of consumers

General Requirements

- Attorney General can request DPA be made available
- DPAs are confidential and not open to public inspection
- Applies to processing activities created or generated on or after July 1, 2024 and are not retroactive

HIPPA

- Health information for “Covered Entities”

COPPA

- Children’s information

VPPA

- Video Privacy Protection Act

FTC Act

- Unlawful and deceptive business practices

Wiretapping Laws

- Federal law but actions primarily for specific state laws (CIPA big one)
- Recording & disclosure of chat and keystroke data

HIPPA

Federal law for protection of health information

Applies to HIPPA-Covered Entities

Focus on Personal Health Information / Individually Identifiable Health Information

- Relates to health condition, provision of health care, or payment of the provision of health care AND
 - Identifies the individual OR
 - Reasonable basis to believe it can be used to identify the individual

Restrictions on use

Restrictions on disclosure (any sending of data to another entity)

- Transparency
- Business Associate Agreement

Health-Specific Laws

Additional state and federal laws with protections for health data

U.S. State Privacy Laws

- Additional protections for “sensitive data”
- From TN law: “includes: Personal information revealing racial or ethnic origin, religious beliefs, **mental or physical health diagnosis**, sexual orientation, or citizenship or immigration status”
- Higher standard of care
- Unique disclosures
- Requires affirmative consent for processing (collection as well as use)

Health-Specific Laws

- Washington My Health My Data
 - Requires consent or necessary to collect and use “consumer health data” (Any data that identifies a consumer seeking health care services is within scope)

FTC Health Breach Notification Rule

- If in scope, need to have authorization for the disclosure of a personal health record. If no authorization, would constitute a breach and the organization can be liable for unlawful disclosure.

FTC Act

- FTC willing to litigate privacy misrepresentations as “deceptive practices”



Financial

Tennessee

Up to \$15,000 for each violation

Each provision and each consumer affected is a separate violation

Private Rights of Action

VPPA, Wiretapping laws, etc.



Financial

Tennessee

Up to \$15,000 for each violation

Each provision and each consumer affected is a separate violation

Private Rights of Action

VPPA, wiretapping laws, etc.



Relief

Court order to stop an activity or impose specific requirements

BetterHelp (FTC Settlement) - Banned from disclosing health information

Consent Orders - Annual disclosure of privacy controls + bi-annual audits



Financial

Tennessee

Up to \$15,000 for each violation

Each provision and each consumer affected is a separate violation

Private Rights of Action

VPPA, Wiretapping laws, etc.



Consumer Expectations

Google research: “After a positive privacy experience with their second-choice brand, **49% of people** said they would switch from their preferred brand to the second-choice brand.”



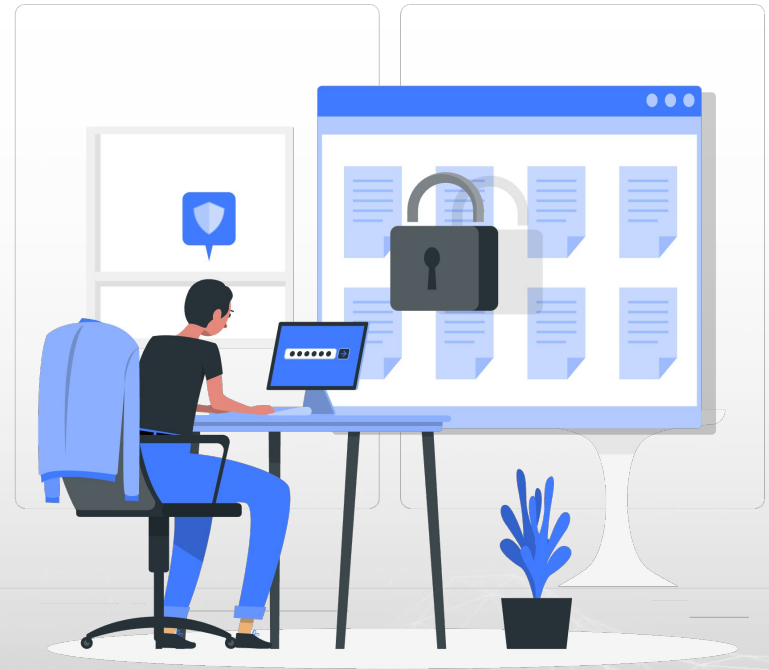
Relief

Court order to stop an activity or impose specific requirements

BetterHelp (FTC Settlement) - Banned from disclosing health information

Consent Orders - Annual disclosure of privacy controls + bi-annual audits

Be Compliance Conscious!



Strategy & Design Phase

1. What are we trying to achieve? (purpose and goal)
2. What personal data is necessary to accomplish?
3. What is the benefit to the consumer?
4. What is the benefit to the business?
5. What is the risk to the consumer?
6. Do the benefit(s) outweigh the risk(s)?
 - a. “Non-industry friend test”

For any and all activities

1. What is the activity?
2. What platforms are in use to support the effort?
3. What data is being collected?
4. What of that is personal information?
 - a. What is potentially “sensitive data”?
5. Where is it sent?
6. How is it used?

Strategy & Design Phase

Paid search example

1. What are we trying to achieve? (purpose and goal)

Increase revenue

Improve ROAS

- Bid optimization
- Creative/copy optimization
- Landing page optimization

Increase conversions

- Remarketing (RLSA)

Increase brand awareness

- Tools in Google Ads
- **Note for controller / processor obligations**

Strategy & Design Phase

Paid search example

2. What personal data is necessary to accomplish?

User identifier - Cookie/device ID, persistent User ID

Associated behavior information - transactions, actions on website, demographic information, location data, campaign data

Strategy & Design Phase

Paid search example

3. What is the benefit to the consumer?

Personalized ad experience

- Consumer expectations for personalization

Strategy & Design Phase

Paid search example

4. What is the benefit to the business?

Improved conversions (more \$\$\$)

More efficient ad spend (save \$\$\$)

Strategy & Design Phase

Paid search example

5. What is the risk to the consumer?

Annoyance

No financial impact or offensive intrusion for a reasonable person

Worst case scenario - embarrassing advertising and possible reputational impact

What are we doing to mitigate risk in the worst case scenario?

Transparency

Opt-out ability

Strategy & Design Phase

Paid search example

6. Do the benefit(s) outweigh the risk(s)?

“Non-industry friend test”

In this case - yes

For any and all activities

Paid search example

1. What is the activity?

Remarketing (RLSA)

For any and all activities

Paid search example

2. What platforms are in use to support the effort?

Google Analytics

Google Ads

Customer Data Platform (in our case a “built” solution in GCP
- BigQuery)

For any and all activities

Paid search example

3. What data is being collected and processed?

Google Analytics

- Device ID - Client ID in GA
- Google ID - Ads 3P cookie ID
- User ID (for registered users)
- Associated behavior information

GCP / BigQuery

- Email
- Profiling based upon GA behavior information

Google Ads

- Google ID
- Assigned segment information

For any and all activities

Paid search example

4. What of that is personal information?

Identifiers

Associated behavior information

Associated profile segment

What is potentially “sensitive data”?

None

For any and all activities

Paid search example

5. Where is it sent?

Google Analytics

Google Ads

GCP environment - BigQuery

For any and all activities

Paid search example

6. How is it used?

Targeted advertising

Compliance Requirements

Consumer Rights

- Transparency / Disclosure
- Access
- Correct inaccuracies
- Delete personal information
- Opt-out of the 'sale' of personal information
 - Opt-out of 'sharing' of personal information

Controller Obligations

- Data minimization
- Technical and operational protections for personal information
- Do not unlawfully discriminate
- Only process sensitive data with consent
- Transparency and disclosure
- Data Protection Assessments

Tag Inspector
AN INFOTRUST PRODUCT

Tag auditing and monitoring platform

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Consent Management Platform

 **Ketch**

Consent Management Platform

InfoTrust

Education resources and consulting services

Consumer expectations for privacy

Foundational privacy requirements

Be privacy conscious

Privacy is an expectation, not an obligation.

Privacy practices are not just the realm of compliance but rather a business necessity.

Competitive advantage is available for organizations that do this well.

Consumer expectations for privacy

**Foundational privacy
requirements**

Be privacy conscious

Transparency / Disclosure

Accuracy

Deletion of Personal Information

Access

Opt-out

Data Minimization

**Technical and Operational
Protections**

Consumer expectations for privacy

Foundational privacy requirements

Be privacy conscious

What is the goal?

Is personal information necessary?

Weigh benefit vs risk for the consumer

What activities are being done?

What platforms are used?

What personal information is present?

Where is it sent ?

How is it used?

Questions?

Thank You!

Email: lucas@infotrustllc.com

LinkedIn: [Lucas Long](#)

InfoTrust: [Contact Us](#)

January 10, 2024