

# The Best Medicine: Respecting Privacy With Health-Related Data



**Dan Frechtling**  
CEO  
503-757-9965  
dan@boltive.com



**Jennifer Garone**  
Privacy & Security Leader  
617-721-0200  
garonepbd1@gmail.com

**KennOne Productions**



**Kirk Nahra**  
Co-Chair, Cybersecurity and  
Privacy Practice  
202-663-6128  
Kirk.Nahra@wilmerhale.com



# Agenda

1. Overview of regulatory and legal developments in 2023

2. Operational challenges of privacy compliance with health regulations

3. Empirical data on companies' online data sharing practices

4. Implications for companies collecting and using health-related data





## *Health Care Privacy in the National Debate*

- HIPAA Rules have set the benchmark for the health care industry for almost two decades
- Have created a standard for the health care industry and consumers that has worked (mostly) well for both the industry and consumers
- Increasing challenges with the existing structure given a variety of changes in both the traditional health care industry and in the broader health information ecosystem
- While HIPAA still works well where it applies (although this may be a controversial statement), there are increasing situations where it doesn't fit or doesn't apply at all



## *Health Care Privacy Framework*

- HIPAA at the forefront
- State “HIPAA-Like” Laws (e.g. CA, TX)
- State Overall Privacy Laws (e.g., CA, Colo, VA)
- State laws on sensitive conditions
- “Non-HIPAA” health data – Washington “My Health My Data” law
- Medical Research principles (US and global)
- Other federal laws (Part 2 substance abuse rules, ADA, etc)
- International principles and standards



## *Health Information (conceptually)*

- Is there something “different” about it?
- 1. HIV/Mental Health/Substance Abuse Information
- 2. Your name and address as a patient
- 3. Foot surgery records (even for this compare my tennis injury to LeBron James seeking a new contract after a major injury)
- 4. Search history of medical information
- 5. Location data “near” a health care facility
- 6. Voting Records/Purchasing Habits/Television Watching (used to evaluate medical issues)



## *HIPAA*

- **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct (1996)
- Focused on portability of health insurance
- Then focused on “administrative simplification”
- Only then got to privacy and security, with almost no detail or meaningful thought
- Critical issue - HIPAA has never been an overall health care privacy rule; it applies to certain defined entities for certain information in certain settings



## *What's Hot in HIPAA Today?*

- Access to records (more than 25 cases)
- Pixel/Tracker issues (guidance, investigations, practical impact)
- Social service organizations
- Opioid Usage
- Dobbs issues



## *The biggest “next generation” issue*

- What is “outside” of HIPAA is growing
- Web sites gather and distribute healthcare information without the involvement of a covered entity.
- Personal health records
- Community/patient support groups
- Significant expansion of mobile applications directed to healthcare data or offered in connection with health information
- Wearables
- All (or at least most) of the health information tech companies have (and now location data)





## *The FTC and health care*

- A number of important cases – breaking new ground on use of health data issues (and data that doesn't really seem like health data but can be in some situations – e.g., location data)
- They are trying to change behavior without new law or regulations
- They are also changing regulations – after guidance and after enforcement cases
- Using a law on health data breaches to define appropriate behavior



## *How is your health information protected under CCPA?*

1. HIPAA protected information (generally exempted from CCPA)
2. CMIA covered companies/information (generally exempted from CCPA)
3. Common Rule/Clinical research (generally exempted from CCPA)
4. CCPA – probably covers your health information if it isn't exempted
5. BUT CCPA doesn't cover non-profits
6. And CCPA doesn't generally cover employers and employee information (note that it will post 7/1/2023)



## *What to watch for in health privacy*

- FTC/State AGs – looking at “non-HIPAA” health data, perhaps HIPAA data, and making lots of other data into health data
- How the pixel/tracker cases evolve
- Other states passing “Washington State” like laws
- Dobbs activity
- State “comprehensive” privacy law implications
- Will there be any movement on a national law and how will health privacy be addressed?

# Agenda

1. Overview of regulatory and legal developments in 2023

2. Operational challenges of privacy compliance with health regulations

3. Empirical data on companies' online data sharing practices

4. Implications for companies collecting and using health-related data



# Operational Challenges

- Jurisdictions
- Which law and when
- Exceptions?
- Implications
  - GeoFencing
  - What is health data?
  - Cookies



# Agenda

1. Overview of regulatory and legal developments in 2023
2. Operational challenges of privacy compliance with health regulations
3. Empirical data on companies' online data sharing practices
4. Implications for companies collecting and using health-related data



# Agenda

**How Do Pixels And Cookies Share Sensitive Health Data?**

Are Websites Gaining Consent Before Collecting Sensitive Health Data?

Are Websites Sharing Health Data With Third Parties After Consumers Opt Out?

# What Are Differences Between Pixels And Cookies?

```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '1885084354934839');
  fbq('track', 'PageView');
</script>
<noscript></noscript>
<!-- End Facebook Pixel Code -->
```

Name	Value	Domain	Path	Expires / Max-Age
S	billing-ui-v3=sJABbfGho2iISkAnJdqz0HQ...	.google.com	/	Session
OTZ	7201252_84_88_104280_84_446940	www.google.com	/	2023-10-10T20:52:22.000Z
NID	511=mKWGeMmONdqERJ34S6wi96f6ueL...	.google.com	/	2024-03-16T21:51:29.099Z
usprivacy	1NYN	www.google.com	/	2024-09-07T00:29:27.222Z

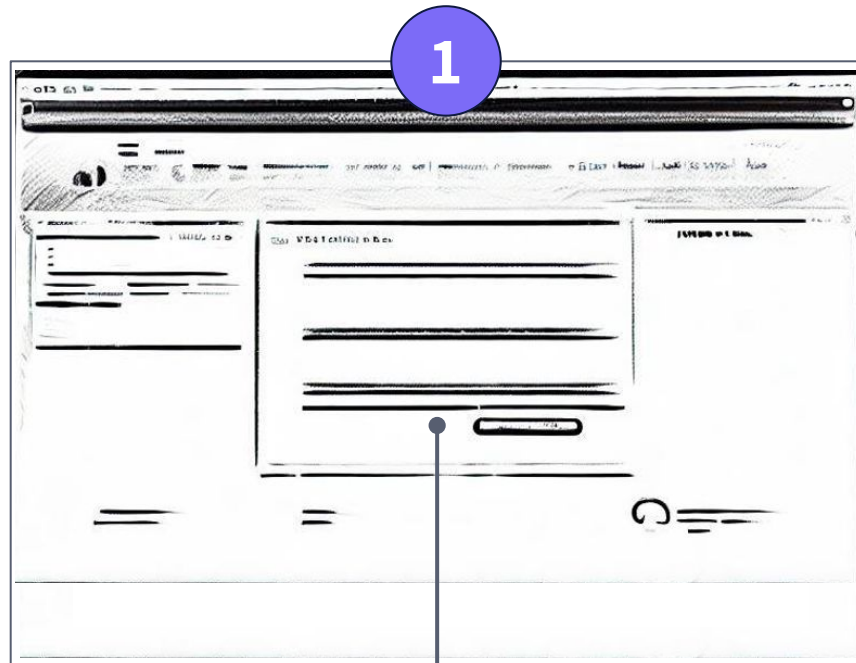
**Cookies** record user info in a unique identifier text file to a browser, so users have the choice to block or clear them

**Pixels** are 1X1 or 0X0 images within websites, ads and emails that send user info directly to third party servers. They can't be easily cleared.

**Tags** are pieces of javascript in webpage code. One type of tag is a **pixel**. Another type sets **cookies**. Another type may be creative being served.

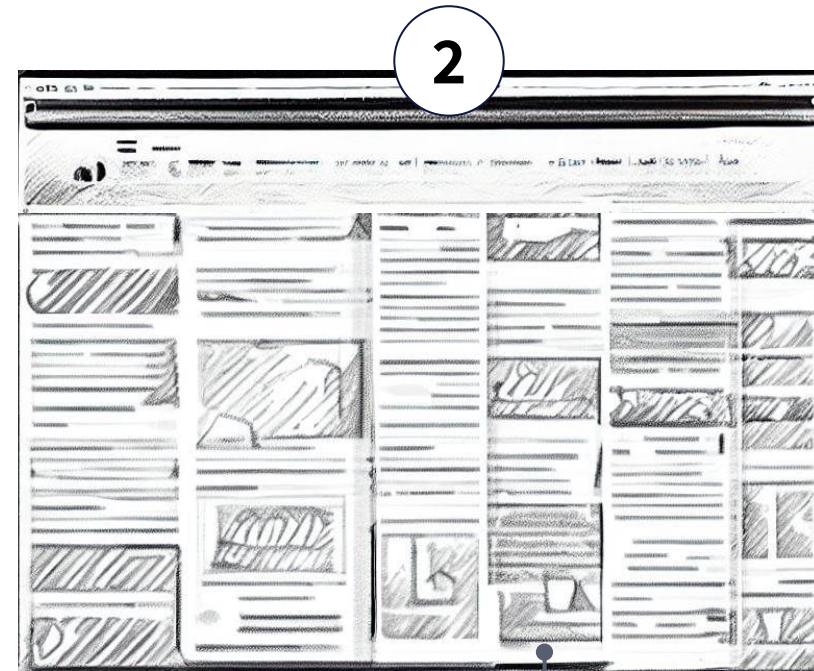


# How Do Pixels And Cookies Appear On Web Pages AND In Ads?



```
https://image2.pubmaltic.com/AdServer/Pag?code=88  
0y0nblc0CfM2jz2R1R7eYm0mudwM0r7yM0A-4p1p9ybackCo  
uk1e-8X 3y076j62 1154 4721 2122 4762146128b06 00544  
uacB-7964409632
```

On Web Pages



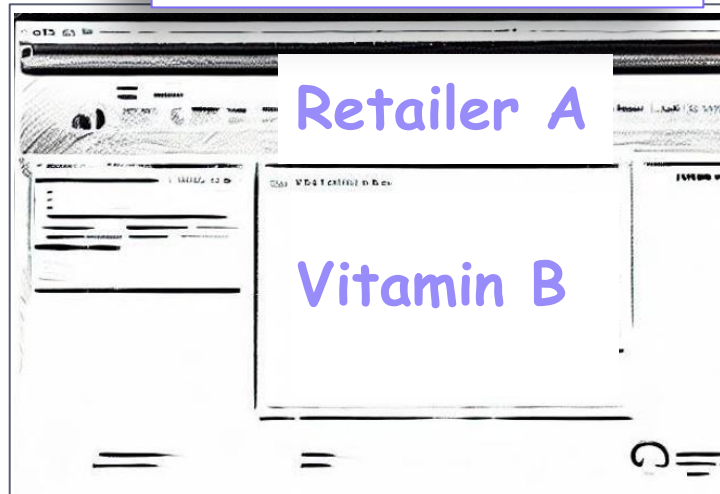
```
https://image2.pubmaltic.com/AdServer/Pag?code=88  
0y0nblc0CfM2jz2R1R7eYm0mudwM0r7yM0A-4p1p9ybackCo  
uk1e-8X 3y076j62 1154 4721 2122 4762146128b06 00544  
uacB-7964409632
```

In Ads

# How Do Web Pages Share User Data?

```

```



**Retailer marks prospect for Vitamin B ads**

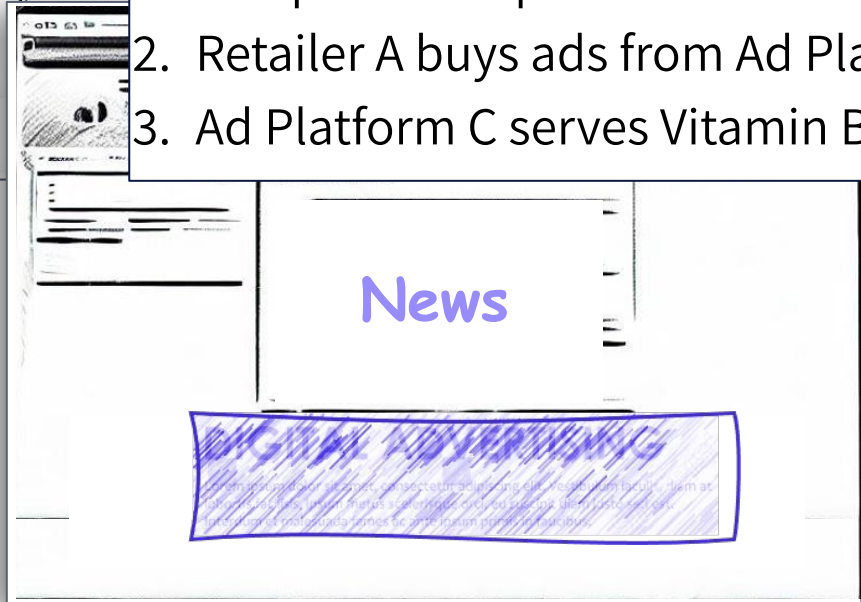
1. Retailer A placed Ad Platform C's pixel\*
2. Platform C's pixel drops cookie
3. User can be tracked, data can be shared

**User becomes a prospect**

1. User visits Retailer A site
2. User browses Vitamin B
3. User qualifies for tracking

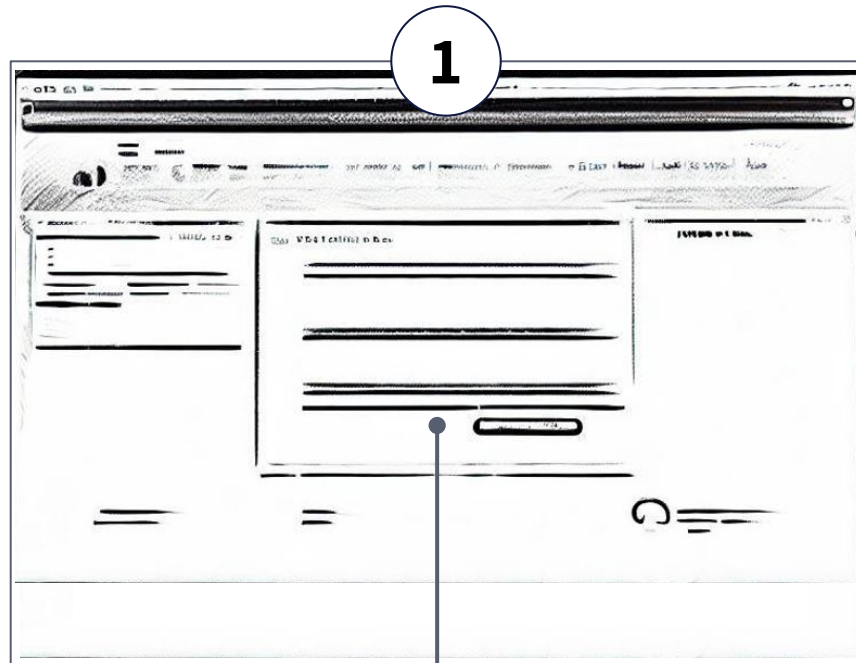
**User visits another site**

1. Site provides space to Ad Platform C
2. Retailer A buys ads from Ad Platform C
3. Ad Platform C serves Vitamin B ad to User



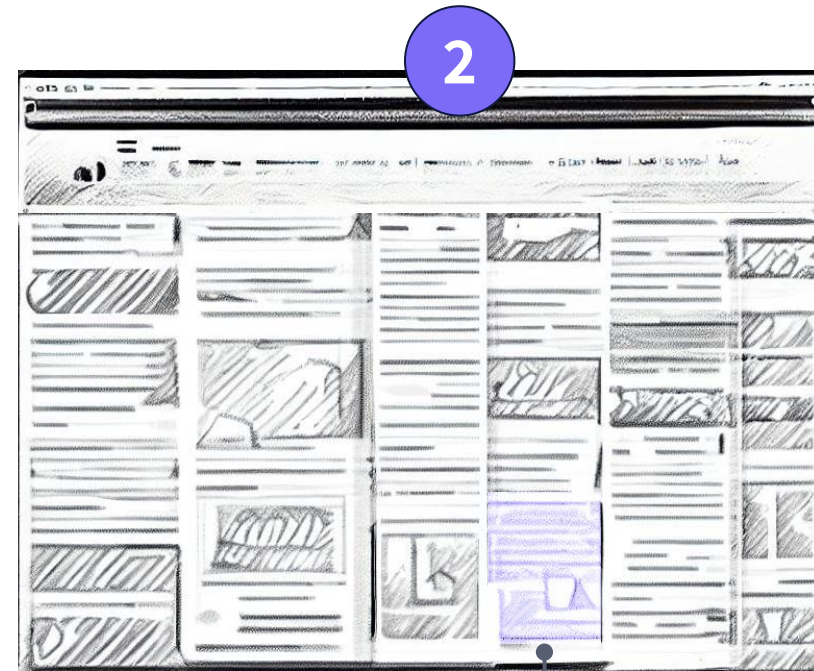
\*Or "tag"

# How Do Pixels And Cookies Appear On Web Pages AND In Ads?



```
https://image2.pubmatic.com/AdServer/Pag?code=88  
0y0nblc0Cf622jz2R107ym0mudwM07ym0A-4p199yb-ack0o  
0x1e-8X 3y076j62 1154 4742 2522 4742w622b06 0054z  
uacB-7964409632
```

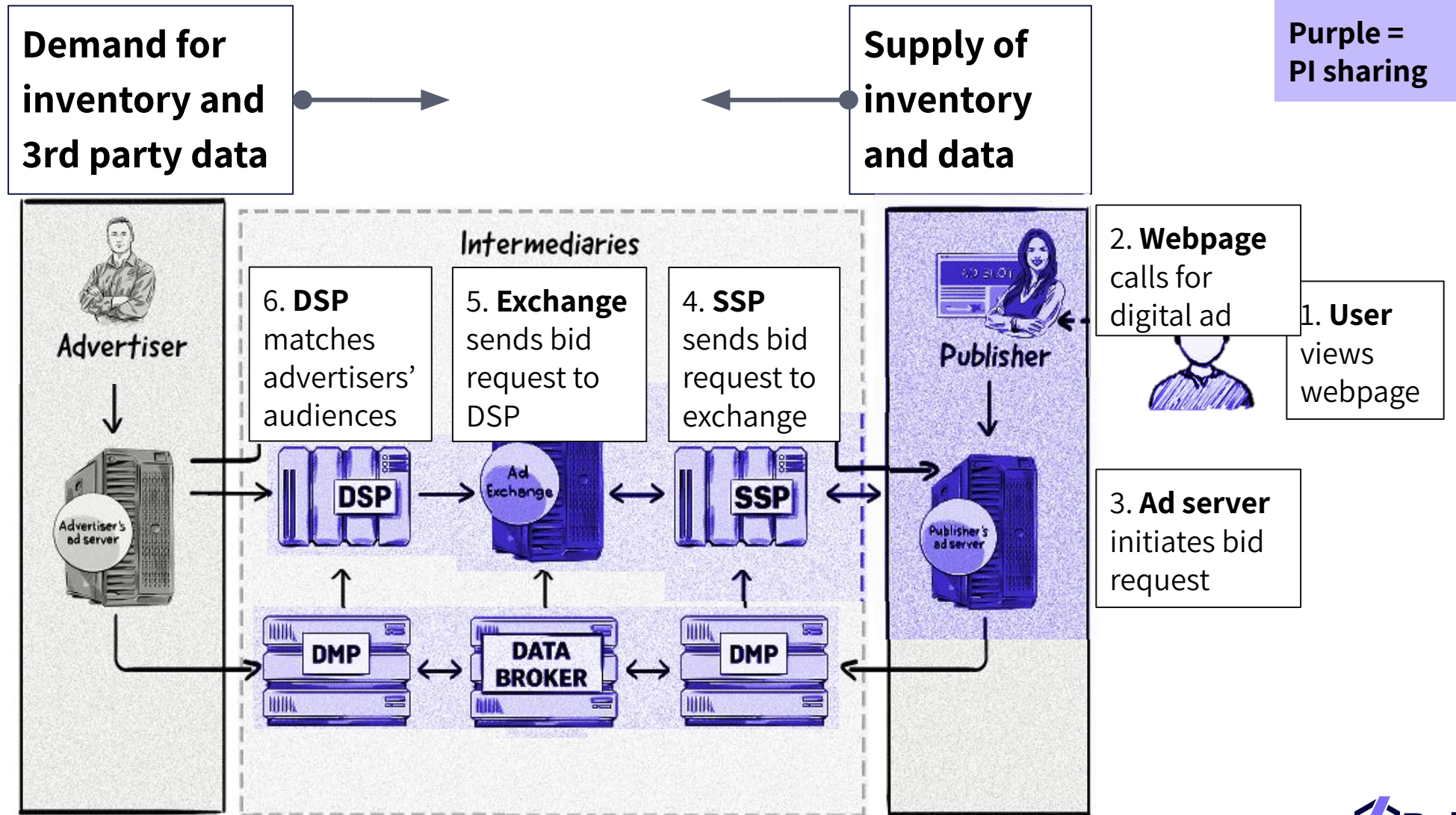
**On Web Pages**



```
https://image2.pubmatic.com/AdServer/Pag?code=88  
0y0nblc0Cf622jz2R107ym0mudwM07ym0A-4p199yb-ack0o  
0x1e-8X 3y076j62 1154 4742 2522 4742w622b06 0054z  
uacB-7964409632
```

**In Ads**

# How Do Pixels, Cookies And The Ad Ecosystem Sell/Share Data?



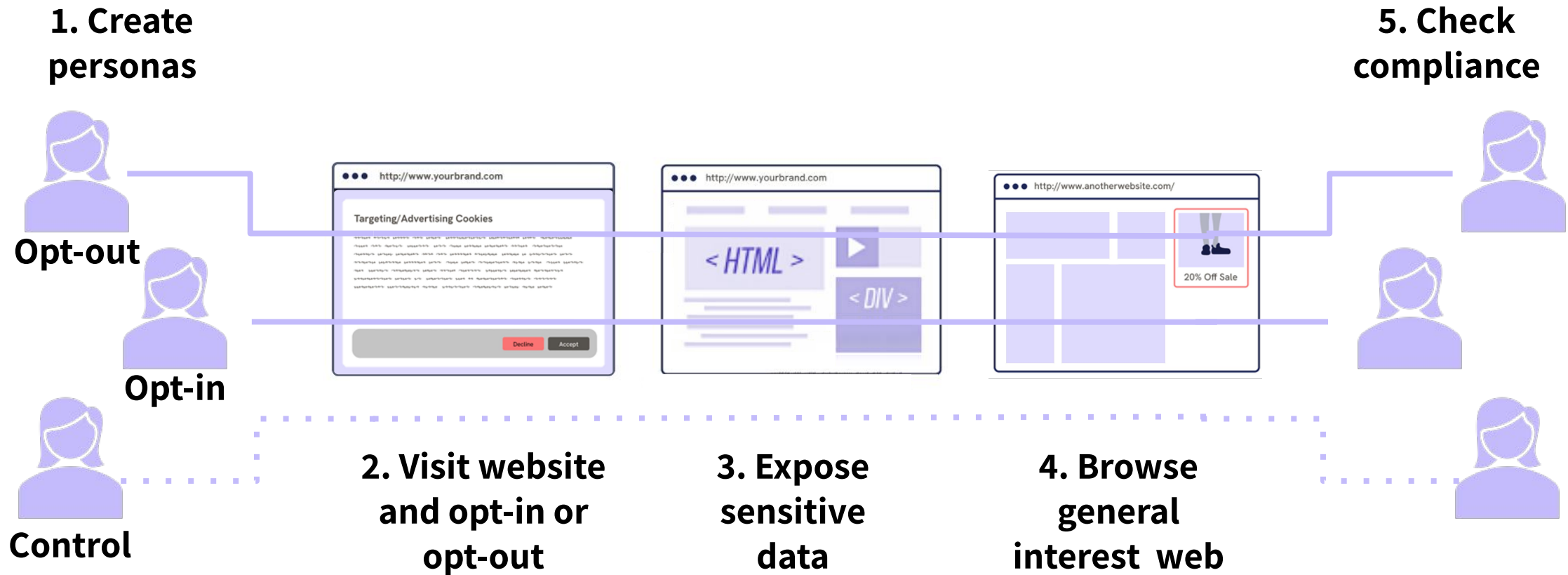
# Agenda

How Do Pixels And Cookies Share Sensitive Health Data?

**Are Websites Gaining Consent Before Collecting Sensitive Health Data?**

Are Websites Sharing Health Data With Third Parties After Consumers Opt Out?

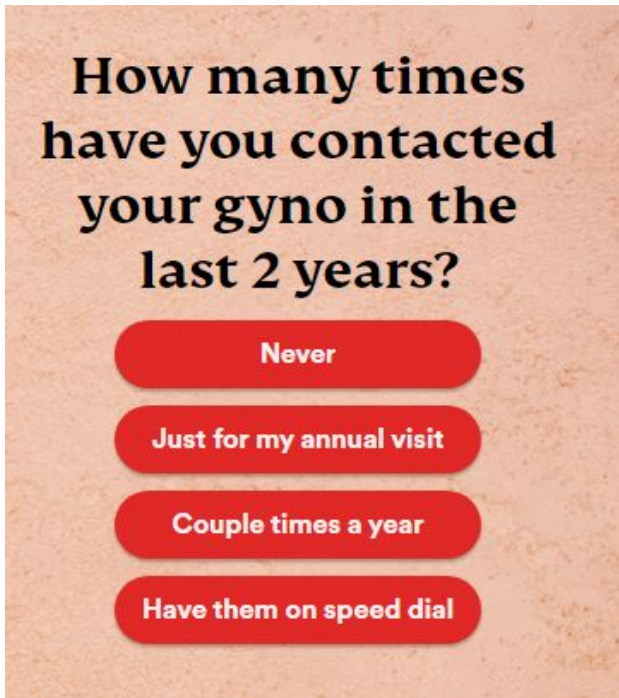
# Methodology Employs Simulated Customer Journeys



# Some Websites Collect Sensitive Health Data Without Explicit Notice

**Women's wellness products** maker presented quiz questions that collect data likely considered "sensitive" in CA

**Drug company** collected data likely considered "sensitive" in states including CA and VA, as it identified a specific medical condition and medical history.



**Commentary:** Neither site is clear how they use sensitive data. One site discloses collection of sensitive data, one doesn't.

# Some Websites Collect Such Data With Consent, But Without Clear Purpose

**Seller of personalized vitamins required opt-in before quiz, but did not disclose how data would be used.** Extensive quiz enabled a personalized vitamin formulation. But it didn't specify how data would be used unless users read entire privacy notice.

**Privacy policy acknowledged it shared data, including health quiz responses, to third-party marketers.** A CA-specific policy explained identifying health information is not disclosed. But “health data” is undefined. Even after opting out, the CA persona saw retargeted ads based on the items viewed.

To continue, please read the statement below

In completing this quiz, you will be asked to provide personal information, including certain health information. [redacted] processes your personal information in order to provide you with a recommendation for a personalized [redacted] pack in accordance with our privacy statement, available here: [Privacy statement](#).

By clicking “I agree” and completing the quiz, you consent to us processing your health information for the purposes of creating a recommendation for a personalized [redacted] vitamins pack in accordance with our privacy statement. You can withdraw your consent at any time, as indicated in our privacy statement. If you do not want us to process this information, please do not proceed with the quiz.





Do you use any of the following forms of birth control?

<input type="checkbox"/> Birth control pill Estrogen, progestin, or both	<input type="checkbox"/> Other hormonal birth control Patch, ring, or IUD
---	--

PRENATAL

Which of these best describes you?

 <input type="radio"/> I'm looking to become pregnant	 <input type="radio"/> I'm currently pregnant	 <input type="radio"/> I'm looking for postnatal support
---	---	--

**Commentary:** Most consumers won't know if their health answers are used for inferences. Those who read the privacy notice may not understand health inferences are used for ads.



# Agenda

How Do Pixels And Cookies Share Sensitive Health Data?

Are Websites Gaining Consent Before Collecting Sensitive Health Data?

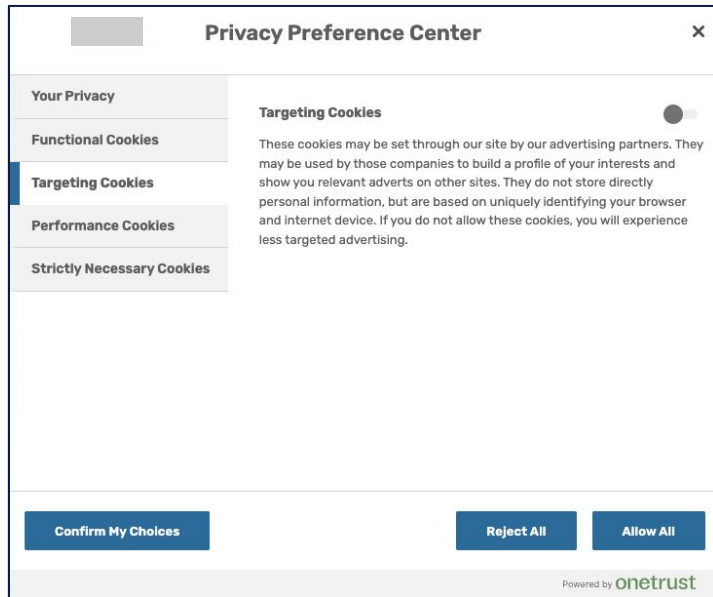
**Are Websites Sharing Health Data With Third Parties After Consumers Opt Out?**

# Companies Default To Sharing Health Data Nearly 100% Of The Time

**Websites we examined use pixels and cookies** to share health-related data with third-parties, despite new legislation that gives consumers control around the collection and sharing of sensitive data

## Treatment center still set IBA cookies after opt-out.

For CA, 7 first-party IBA cookies tracked visitors across social media such as Facebook and Google. For VA, 9 such cookies tracked visitors.



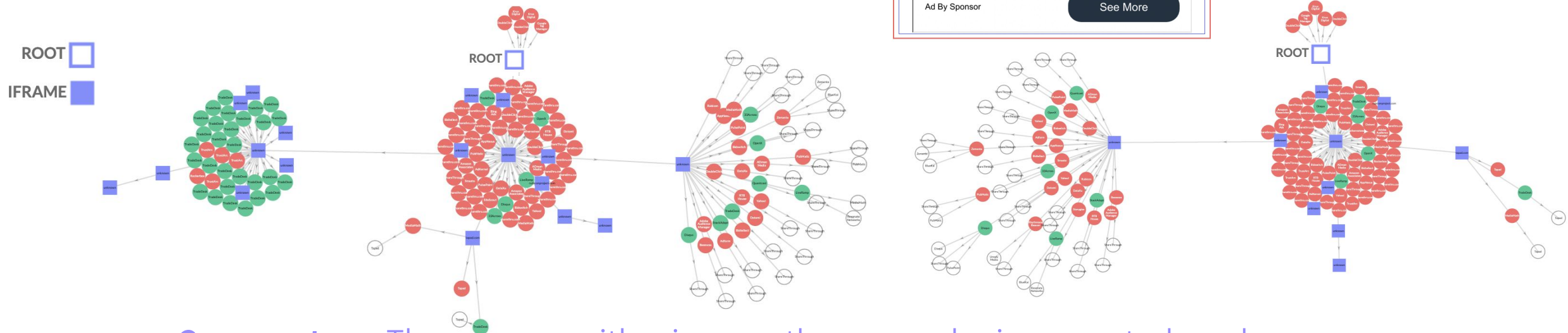
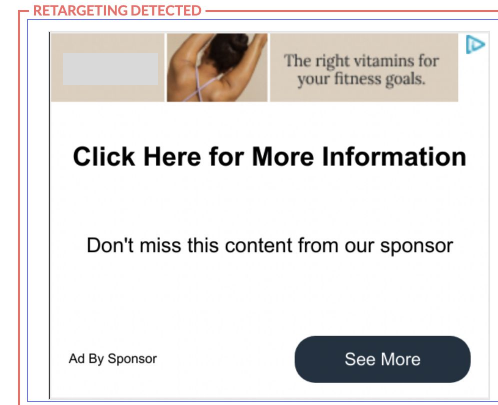
## Overall, opt-out personas only see small reduction in IBA cookies.

	IBA Cookies Set For CA No Opt-Out Persona	IBA Cookies Set For CA Opt-Out Persona
Pharma maker	59	No website opt-out
Treatment center	29	No opt-out
Men's Health Clinic	46	No opt-out
Women's Health Retailer	22	18
Telehealth provider	32	No website opt-out
Vitamin maker	20	8
Health bookseller	0	0
Senior health retailer	6	No opt-out
Fertility marketplace	22	No website opt-out
Treatment center	7	7

**Commentary:** IBA tags and cookies are present on 9 of the 10 sites examined. Most visitors are at risk of having health-related data used for marketing purposes.

# Some Companies Share Health Data Through Retargeted Ads

A vitamin and supplements maker served re-targeted ads to users that opted out. The manufacturer **seemingly** continued to share personal information with third parties after the user opt-out, apparently in contravention of applicable state privacy laws.



**Commentary:** The company either incorrectly managed privacy controls and allowed some back-end sharing, or ignored user requests

# Agenda

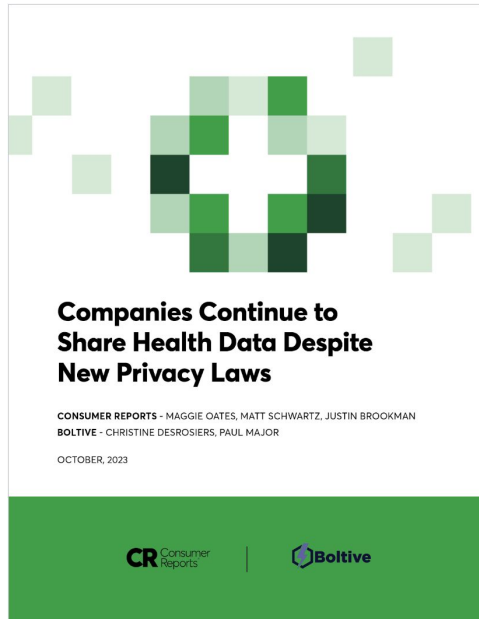
1. Overview of regulatory and legal developments in 2023
2. Operational challenges of privacy compliance with health regulations
3. Empirical data on companies' online data sharing practices
4. Implications for companies collecting and using health-related data



# What Should You Do? We Recommend Three Reviews (Repeat Periodically)

	<b>Assessments</b>		
	<b>Data</b>	<b>Legal</b>	<b>Trade-off</b>
<b>A. Data elements</b>	Which of your “generic” data elements are now possibly health-related?	Have you evaluated how relevant regulatory agencies are analyzing data elements you collect? Have you appropriately disclosed your practices to relevant individuals?	What is business value vs. legal risk of collecting your data elements?
<b>B. Third parties</b>	What third parties do you share health data with?	Do you have appropriate agreements in place with any third parties? Have you provided appropriate rights to individuals about sharing with these parties?	What is business value vs. legal risk of partnering with third parties?
<b>C. Sharing</b>	What data are you sharing with these third parties and how are they using data they receive?	Do you have the right controls in place to ensure that only appropriate data is shared (and for appropriate purposes)?	What is business value vs. legal risk of sharing particular data with particular third parties?
<b>Specifically ....</b>	Are you including trackers (pixels, cookies, SDKs) in B, C? Does your current DSR process include this expanded scope of data?		Are you including trackers in B, C? Are there less intrusive methods to achieve the business value of A, B, C? What are your processes for approving data elements and auditing third parties?

# Sign up To Receive The Research Paper (Free For Attendees)



## Key contributors to this study

- Maggie Oates, Consumer Reports
- Matt Schwartz, Consumer Reports
- Christine Desrosiers, Boltive
- Paul Major, Boltive