



Privacy Disclosure Risks from Web 2.0/3.0 Technologies

Legal and Best Practice Requirements Considering FTC,
OCR/HIPAA, CCPA and Other State Laws

Presented by:
Igor Gorlach, Nicholas
Maietta, Sydney Teng, and
Aaron Massey

Friday, May 12, 2023



Introductions



Igor Gorlach
Partner (HOU)
King & Spalding
igorlach@kslaw.com



Nicholas Maietta
Associate (D.C.)
King & Spalding
nmaietta@kslaw.com



Sydney Teng
Associate (CLT)
King & Spalding
steng@kslaw.com



Aaron Massey
Senior Policy Analyst
Future of Privacy Forum
amassey@fpf.org

Web 1.0 – The Consumer Web

Content delivery network

Static

No social media interaction



Web 2.0 – The Social Web

User-driven
communities

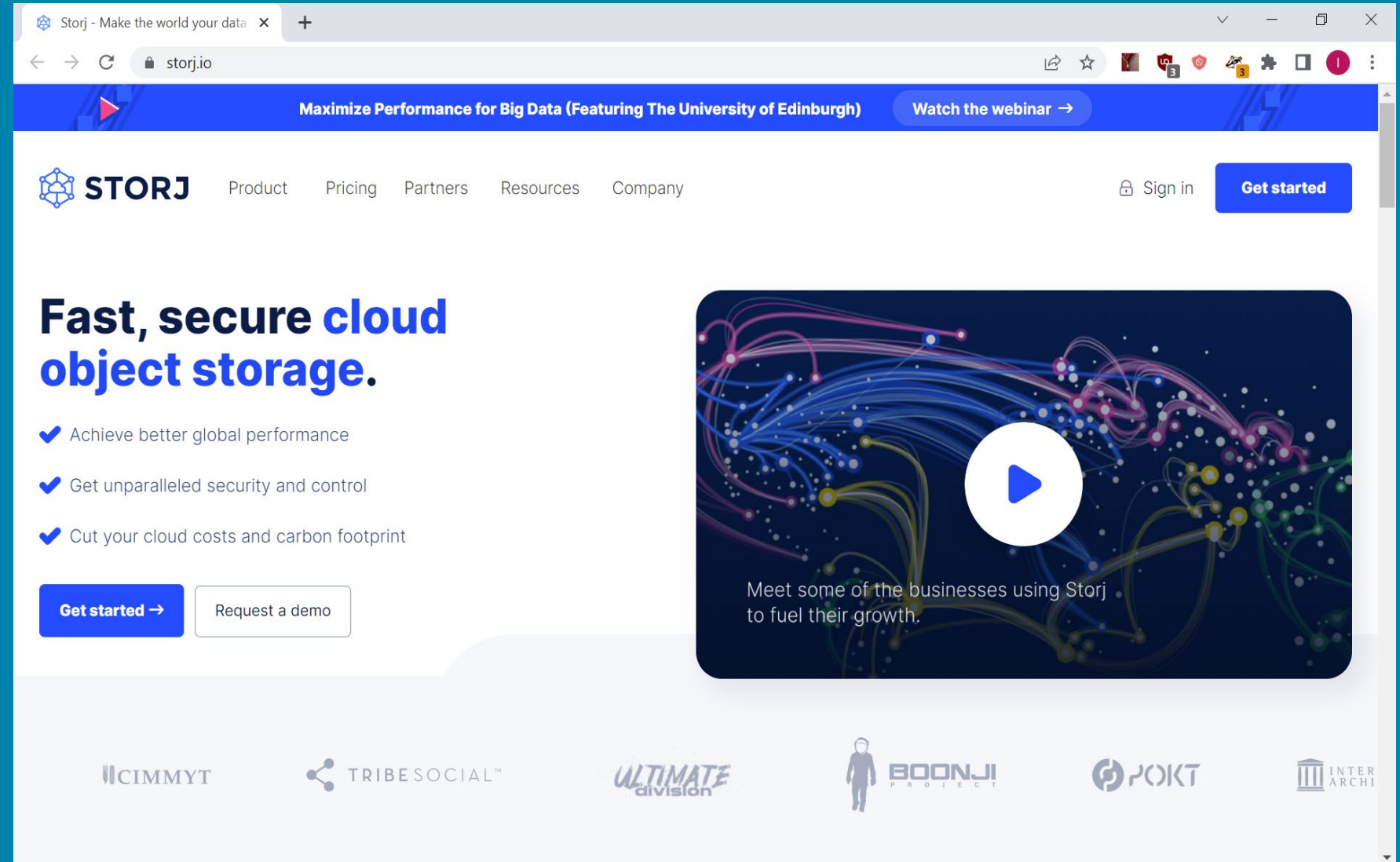
Read-write
interactions
dominate content



Web 3.0 – The Decentralized, Semantic Web

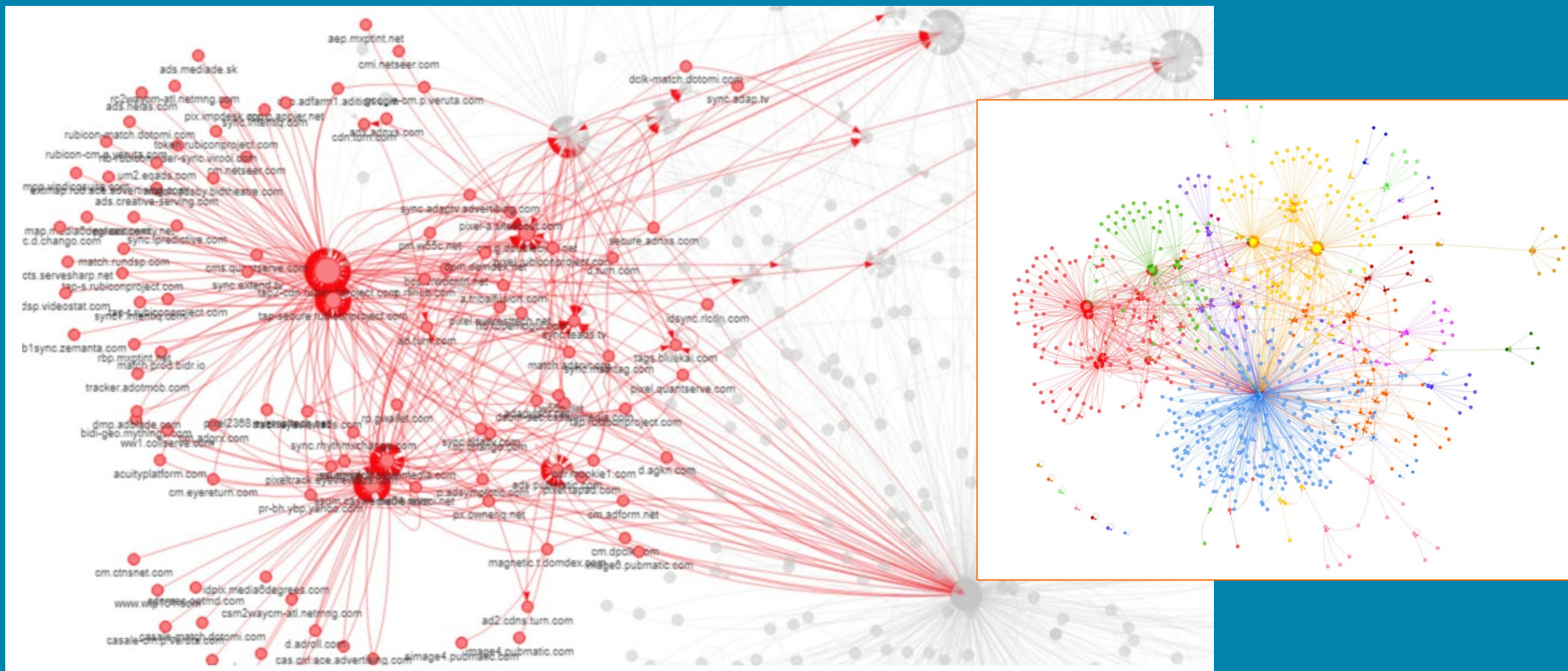
Decentralized,
trustless,
permissionless, and
interoperable.

Tools involving markup data, crowd-sourced content, data mining and machine learning to establish semantic connections, so that machines understand and interpret what humans exactly want – contextual, relevant results.



The screenshot shows the Storj website homepage. The browser address bar displays 'storj.io'. A blue banner at the top reads 'Maximize Performance for Big Data (Featuring The University of Edinburgh)' with a 'Watch the webinar →' button. The navigation menu includes 'Product', 'Pricing', 'Partners', 'Resources', and 'Company'. On the right, there are 'Sign in' and 'Get started' buttons. The main content area features the headline 'Fast, secure cloud object storage.' followed by three bullet points: 'Achieve better global performance', 'Get unparalleled security and control', and 'Cut your cloud costs and carbon footprint'. Below these are 'Get started →' and 'Request a demo' buttons. A large video player is embedded, showing a network visualization with a play button and the text 'Meet some of the businesses using Storj to fuel their growth.' The footer contains logos for CIMMYT, TRIBESOCIAL™, ULTIMATE division, BOONJI PROJECT, POKT, and INTER ARCHI.

Real-Time Bidding Data Flows



Source: Van Eijk, R. (2019), Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification (diss. Leiden), <https://ssrn.com/abstract=3319284>

What to Make of this History?

- **It's generally accumulative; not zero-sum** – We still have technologies and policies in use today from the Web 1.0 era.
 - Cookies, HTTP, and JavaScript are all still around and hard to replace. (See Google's Privacy Sandbox)
- **It's more than just the web** – Apps, devices, and internal corporate computer systems also depend on web 2.0 / 3.0 technologies.



Top Tracking Technologies



Cookies

Canvas Fingerprinting



Link Tracking

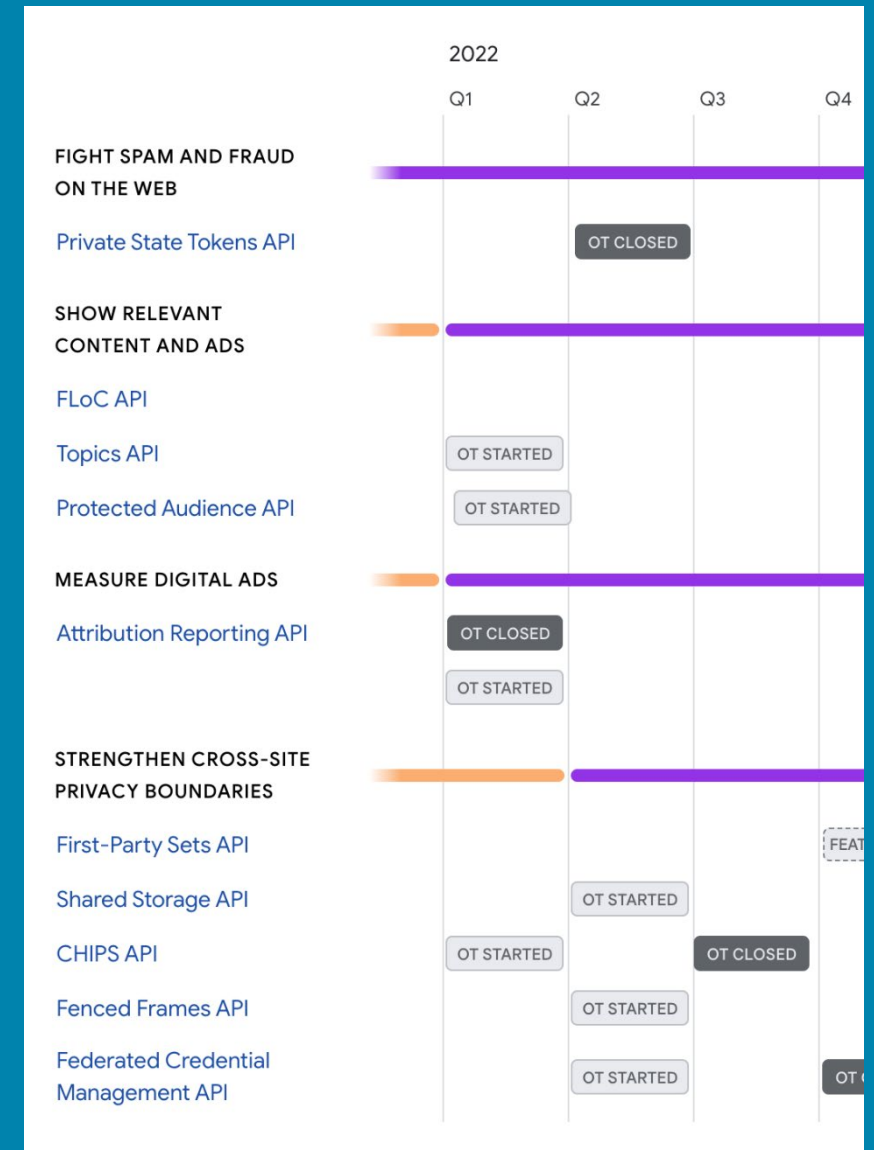
Bounce Tracking



Query Parameter Tracking

Proposed Purpose-specific Tracking Standards

- Also known as the **Google Privacy Sandbox**
- **Advertising** – TOPICS API, Protected Audience API.
- **Measurement** – Attribution Reporting API
- **Spam and Fraud Prevention** – Private State Tokens API
- **Cross-site Privacy Boundaries** – First-Party Sets, Shared Storage API



FTC Focus on Trackers



Overview of Privacy Oversight

FTCA

Federal data-specific laws (e.g., HIPAA)

Comprehensive state laws

Web-specific state laws



FTC Authority

- Primary authority under Section 5 of the FTC Act
- May bring enforcement actions against organizations following data security incidents that FTC believes involve:
 - **Deceptive practices** – misrepresenting privacy and security measures
 - **Unfair practices** – inadequate security measures
- Has expressly stated its intent to further expand its role in setting and enforcing cybersecurity and data privacy standards



Enforcement Against Health Tech Companies: Spotlight on Flo Health



Complaint Allegations:

- Disclosed user data via event records to 3rd parties without affirmative consent
- Privacy policy misrepresentations about disclosure to 3rd parties
- Violated 3rd party disclosure requirements
- EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield framework violations
- Encouraged millions of users to input “vast quantities” of health information

Consent Order Provisions:

- ✓ Prohibited from misrepresenting:
 - How and why it collects, uses, retains or discloses user data
 - Amount of consumer control over data
 - compliance with any privacy, security, or compliance program
- ✓ Direct 3rd parties to delete user data
- ✓ Provide notice to individuals via email

FTC investigated data privacy and security practices as far back as 2016, shortly after app launch



Health Breach Notification Rule Enforced



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement ▾ Policy ▾ Advice and Guidance ▾ News and Events ▾ About the FTC ▾

For Release

FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising

Under proposed order, GoodRx will pay a \$1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google, and other companies

February 1, 2023

f t in

Complaint Allegations:

- 3rd party pixels recorded users' Rx info, health conditions, and PII (e.g., name and IP address)
- No contractual protections for PHI use by advertisers
- No FTC reporting
- Privacy policy misrepresentations
- HIPAA compliance seal on website

Consent Order Provisions:

- ✓ Affirmative user consent via "clear and conspicuous" disclosure in privacy policy, or terms of service / use
- ✓ Comprehensive privacy program with annual reporting
- ✓ Direct 3rd parties to delete user data and confirm in written form
- ✓ Provide notice to individuals via email, app, and website posts

“

Digital health companies and mobile apps should not cash in on consumers' extremely sensitive and personally identifiable health information.

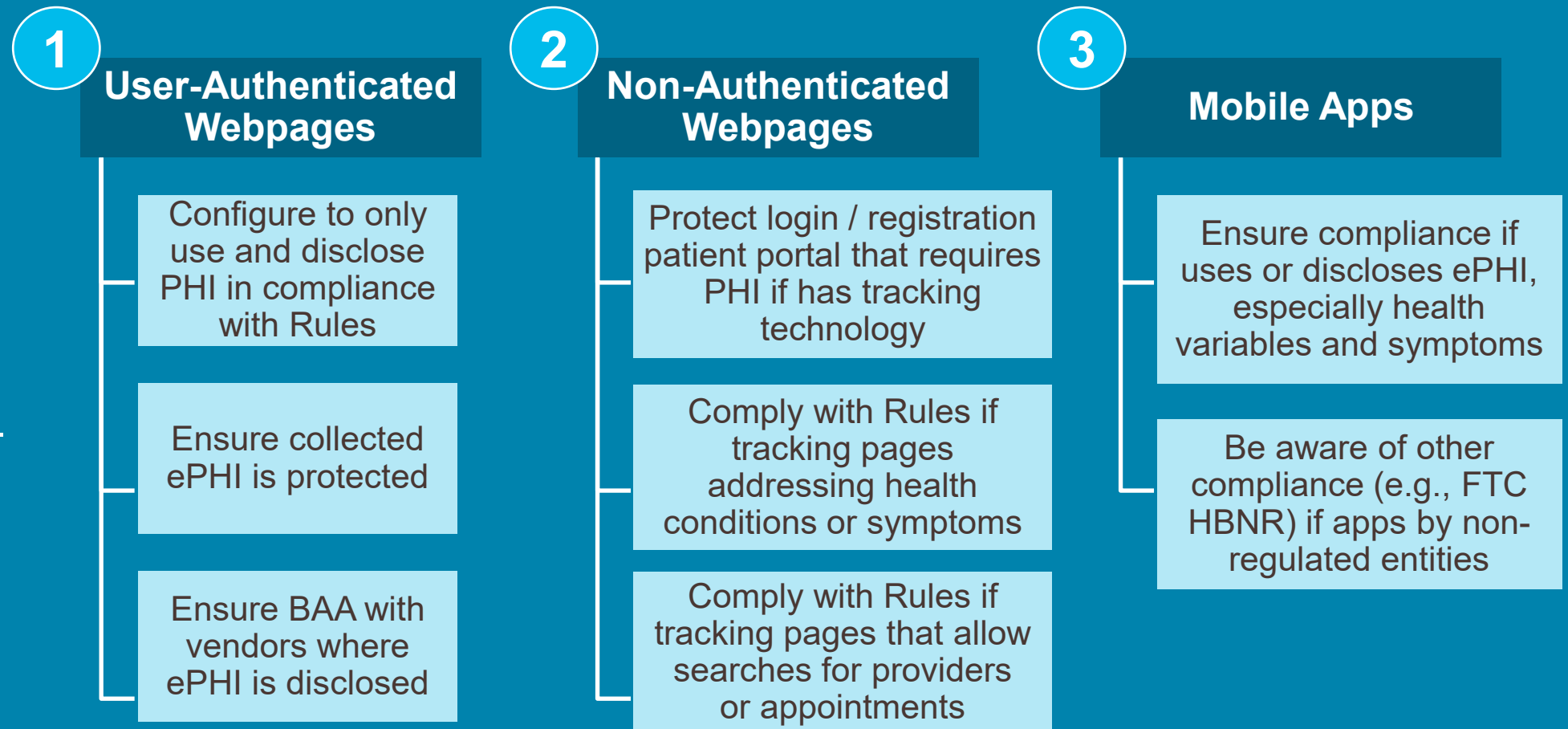
— Samuel Levine, Director,
FTC Bureau of Consumer
Protection

HHS OCR Tracking Technology Guidance

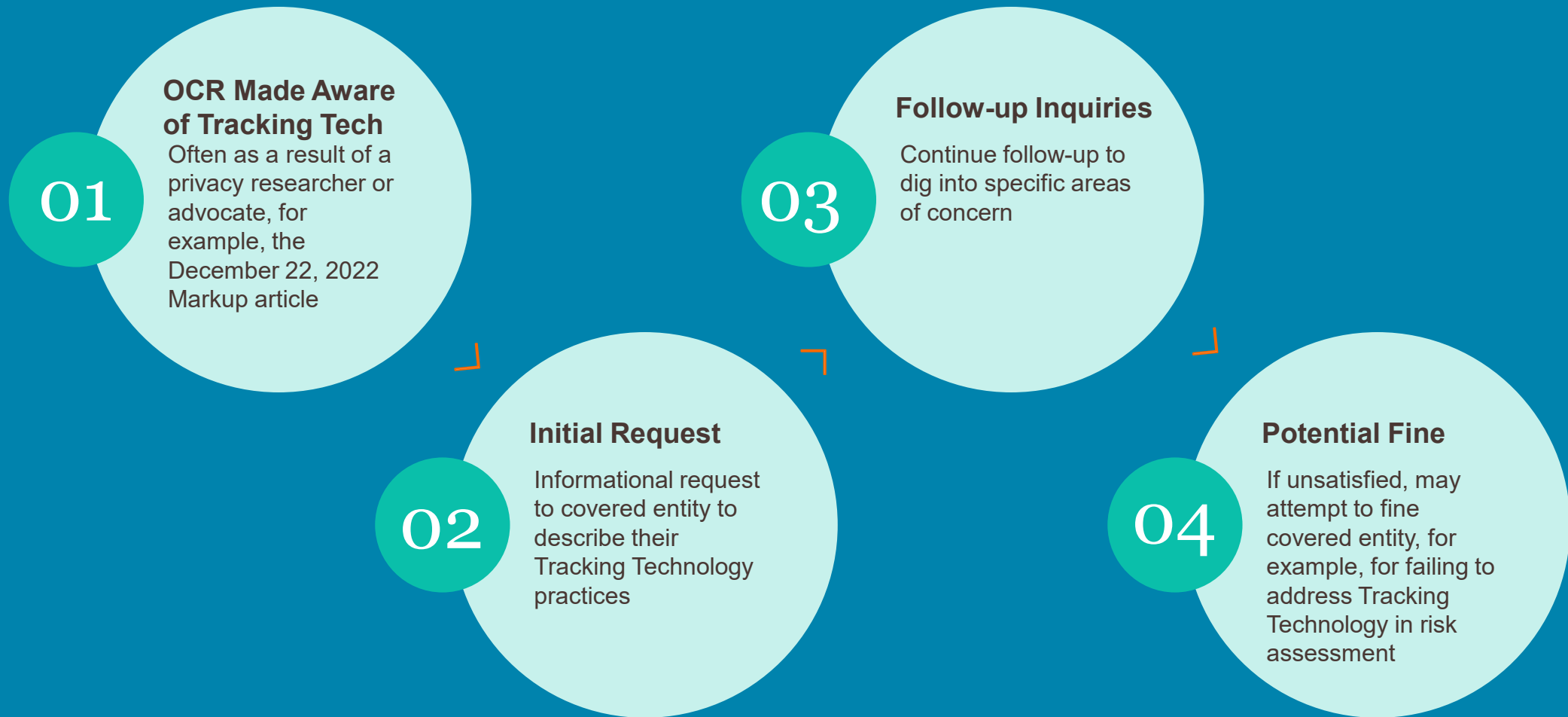


HHS OCR Bulletin: Guidance on the Use of Online Tracking Technologies, Dec. 2022

Outlines 3 use cases when HIPAA Privacy, Security, and breach notification rules apply to third-party-developed tracking technologies.



Common OCR Approach to Tracking Tech.



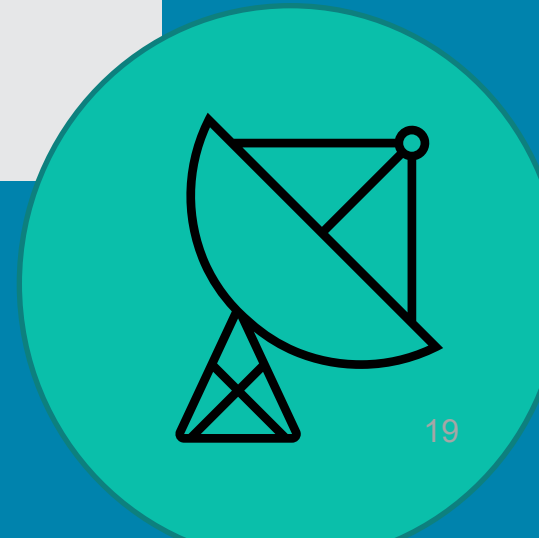
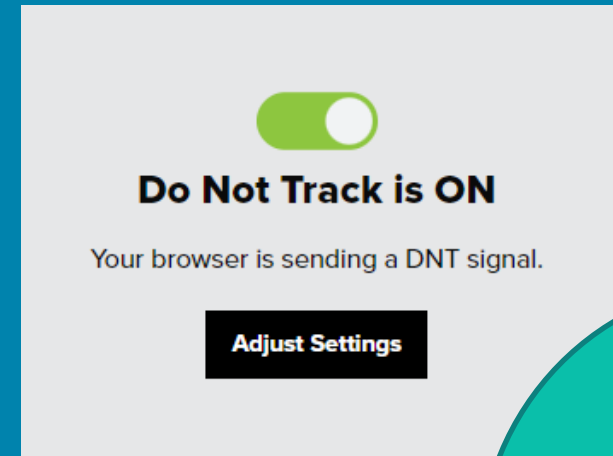
Opt Out Signals



Opt Out Signals 1.0: Do Not Track

Do Not Track (“DNT”) signals were first proposed in 2009, with industry and regulatory support following thereafter. California amends CalOPPA in 2013 to address DNT signals.

- **What:** A web browser setting that requests that a web application disable its tracking of an individual user.
- **Legal obligation:** Disclose how a business’s online services respond to DNT signals
 - *This is still an active legal requirement!*

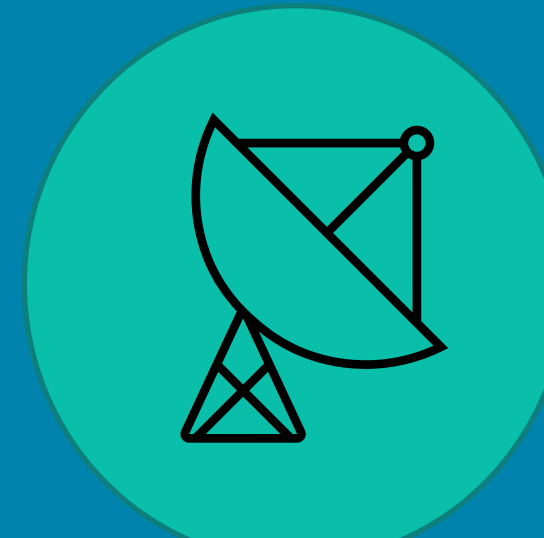


Opt Out Signals 1.1: Preference Proliferation

DNT signals fail to gain traction. Industry groups and browsers develop own privacy preference mechanisms.

Factors contributing to lackluster response:

- No legal enforcement mechanism
- No universal standard on how to respond
- AdTech incentive



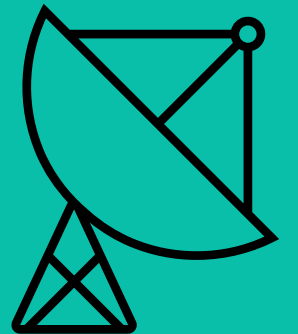
Opt Out Signals 2.0: User-enabled global privacy controls

“User-enabled global privacy controls” appears in CCPA regulations (2020).

- **What:** a browser plug-in or privacy setting, device setting, or other mechanism that communicates or signals the consumer’s request to opt out of sales of personal information
- **Legal obligation:** process such signals as a “Do Not Sell” request under CCPA

§ 999.315. Requests to Opt-Out.

- (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information.
- (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.
- (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
- (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information.
 - (2) If a global privacy control conflicts with a consumer’s privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control over the consumer’s privacy setting or participation in the financial incentive program.



Opt Out Signals 2.1: GPC Signals

California AG announces first public CCPA enforcement action. Global Privacy Control (“GPC”) signals central to enforcement.

- **What:** a browser-level signal, maintained either by a browser or browser extension, that a user or privacy-focused technology can set.
- **Legal obligation:** process such signals as a “Do Not Sell or Share” requests under CCPA.
- Colorado and Connecticut will require compliance in 2024 and 2025, respectively.

YOUR PRIVACY CHOICES

DO NOT SELL OR SHARE MY PERSONAL INFORMATION

If you have not yet opted out of sale/sharing of your personal information, please submit the form below.

The information you provide below, if needed, will facilitate your request to opt-out of sale/sharing. If you do not provide the information requested below, we may not be able to identify you and process your request to opt-out. Any information you provide below will not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing.

For more information about our privacy practices, please review our [Privacy Policy](#).

If you are logged into your Sephora account and have already been opted-out of sale/sharing of your personal information, the form will not appear.

If you do not have a Sephora account or if you are not logged into your Sephora account, your request to opt-out of sale/sharing will be linked to your browser identifier only and not linked to any account information because the connection between your browser and the account is not known to us.

OPT-OUT PREFERENCE SIGNAL (GLOBAL PRIVACY CONTROL)

You may use an Opt-Out Preference Signal, such as the Global Privacy Control (GPC), to opt-out of the sale/sharing of your personal information.


If you do not have a Sephora account or if you are not logged into your Sephora account, your request to opt-out of sale/sharing will be linked to your browser identifier only and not linked to any account information because the connection between your browser and the account is not known to us.

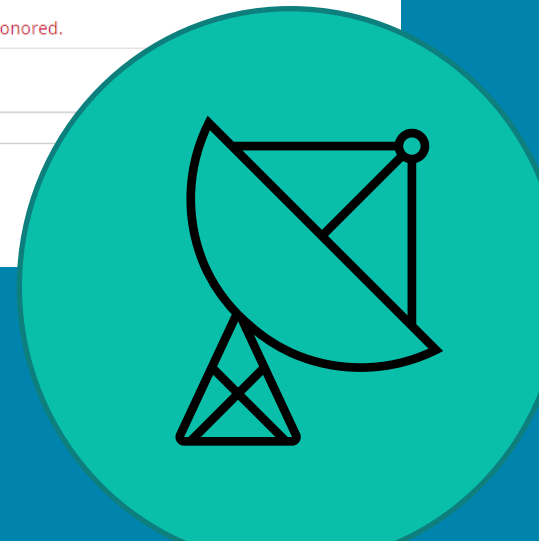
If you would like us to make the connection between your browser and your account, and you have not yet opted out of sale/sharing your personal information, please submit the form below.

Your Opt-Out Preference Signal has been honored.

Please provide the following details:

<input type="text" value="First Name"/>	<input type="text" value="Last Name"/>
<input type="text" value="California"/>	

Powered by 










Opt Out Preference Tools

Tools supporting the *Global Privacy Control (GPC)* signal are available for desktop and mobile devices.

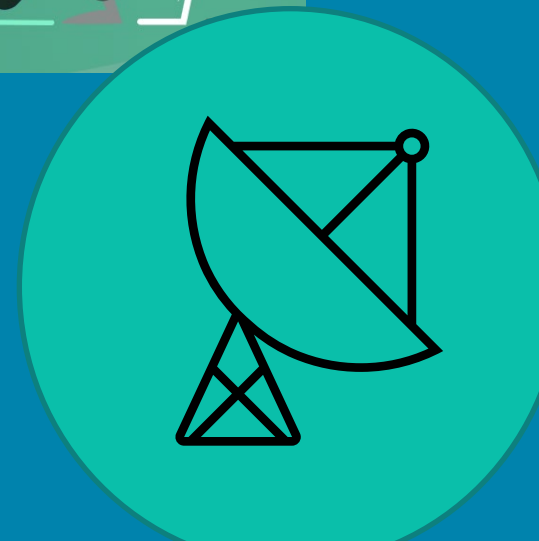
The GPC specification only details how the signal is sent and received.

Open questions remain for handling conflicts, user experience, and data provenance and analysis.

	Abine
	Brave Privacy Browser
	Disconnect
	DuckDuckGo Privacy Browser
	Firefox
	OptMeowt by privacy-tech-lab
	Privacy Badger by EFF

A Closer Look at CCPA Obligations

1. Businesses **MUST** recognize and process opt-out preference signals.
2. Businesses **MUST** carry over preferences to the extent that the business “knows” the consumer. This extends to future sessions, browsers, devices, profiles, and offline activity.
3. Businesses **MUST** disclose how opt-out preference signals will be processed and how consumers can use this signal.
4. Privacy preference reconciliation is permitted but poses operational difficulties.
5. Inaction is not consent.



Washington's My Health, My Data Act

The law applies to controllers conducting business in Washington and regulates “consumer health data”, which includes:

- Individual health conditions, treatment, diseases, or diagnoses
- Social, psychological, behavioral, and medical interventions
- Use or purchase of prescribed medication
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
- Data that identifies a consumer seeking health care services



Washington's My Health, My Data Act



Prohibits collection and disclosure unless obtain opt-in consent or activity is necessary to provide requested product or service



Requires "valid authorization" from consumer before "selling" regulated data



Prohibits certain geofencing activity



Requires "health data privacy policy" and extends traditional data subject rights



Enforced by AG and private parties as violation of Unfair Business Practices Act

Questions



Igor Gorlach
Partner (HOU)
King & Spalding



Nicholas Maietta
Associate (D.C.)
King & Spalding



Sydney Teng
Associate (CLT)
King & Spalding



Aaron Massey
Senior Policy Analyst
Future of Privacy Forum