May 11, 2023

Wait, A Privacy Incident is a Security Incident?

Privacy+ Security Forum

Presenters

Privacy+ Security Forum

Jonathan Fairtlough

Principal

KPMG LLP

Wynter Deagle

Partner

Sheppard Mullin

Anne-Marie Dao

Associate

Sheppard Mullin

AGENDA

1. Privacy Incident Response
2. Common Issues Leading to Privacy Incidents
3. How Plaintiffs Find Violations
4. Data Sources for Investigations
5. Privacy Incident Litigation

PRIVACY INCIDENT RESPONSE

Privacy+ Security Forum

What Is It?

The growth of privacy statutes, the rise of AG enforcement and the survival of privacy-based claims at a motion to dismiss, have created a new class of Incident Response - one driven by privacy violation claims.

Privacy IR has many of the hallmarks of a Cyber IR:

- Demand from a third party for payment
- Rapid investigation under privilege to determine:
  - Scope of violation
  - Number of persons impacted
  - Location and status of impacted parties
  - Nature of data involved
- Recovery of impacted site or process

Similar Paths to Urgency

Privacy+ Security Forum

IR: Notice via attacker
PIR: Notice via demand letter

Short time frame to avoid public issue

IR: Investigation into scope of attacker access
PIR: Investigation into scope of impacted users

Facts needed to quickly determine scope

IR: Forensic log data determines investigation
PIR: UUID data determines ability to reduce class

Data available determines success

Extortion Demand

Privacy+ Security Forum

Your network has been infected!

Your sensitive data has been stolen and your documents, photos, databases and other important files have been encrypted.

To avoid release of your data and decrypt your files you need to buy our special software – clavis99 Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time.

clavis99 Decryptor price

You have 2 days, 02:26:15

- If you do not pay on time, the price will be doubled
- Time ends **Mar 1 12:11:15**

Current price 215.50 btc

5,000,000 USD

After time ends 431.00 btc

10,000,000 USD

INSTRUCTIONS | CHAT SUPPORT | ABOUT US

Demand Letter

Re: Class Action Lawsuit for Wiretapping/CIPA Violations

Ladies and Gentlemen:

This law firm has been retained by a California consumer to prosecute a class action lawsuit against you for violating California Penal Code Section 631 *et seq.* ("CIPA"), which prohibits unauthorized "use in any manner" of certain electronic communications.

Our client visited your website and used your chat feature. We have since confirmed that you secretly record such communications and allow a third party to intercept and eavesdrop on such communications in real time. You do so without obtaining express, prior consent from visitors.

You may be liable for $5,000 in statutory damages to each Californian you have wiretapped. The validity of our position was recently confirmed in the case of *Byars, et al v. Goodyear Tire & Rubber Company*, C.D. Cal. Case No. 5:22-cv-01358.

This letter is written as a courtesy to advise you that we intend to file suit very soon; no further notice will be provided. If you believe we are mistaken, your counsel should immediately contact us.

Sincerely,

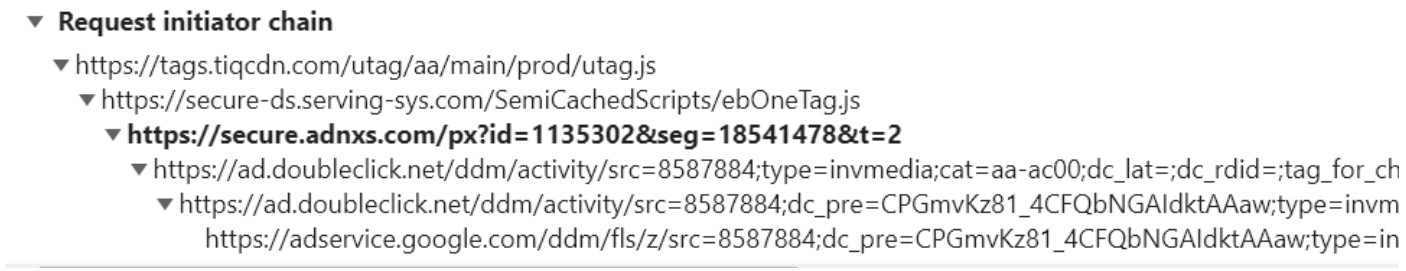
Scott J. Ferrell, Esq.
A 'Top 100' Southern California Super Lawyer

COMMON ISSUES LEADING TO A PRIVACY INCIDENT

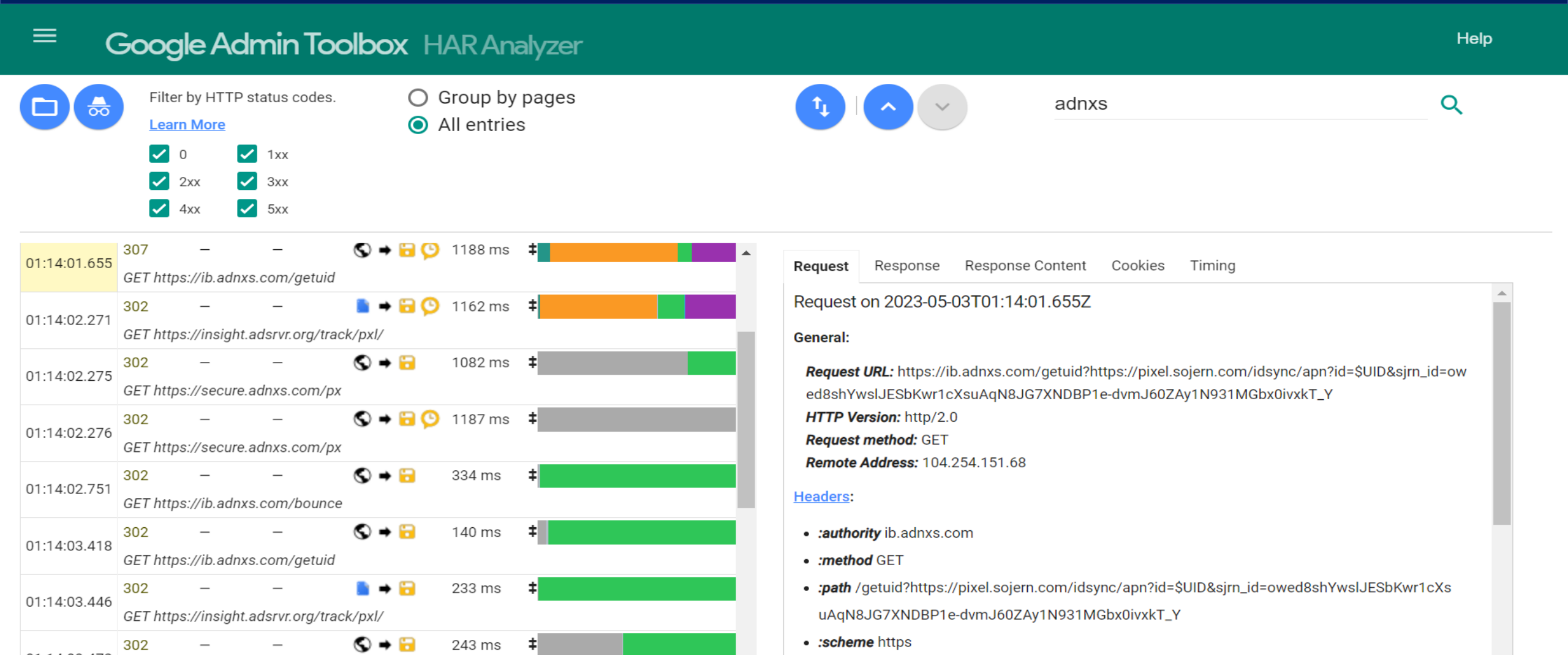
Privacy+ Security Forum

Server Side Cookies

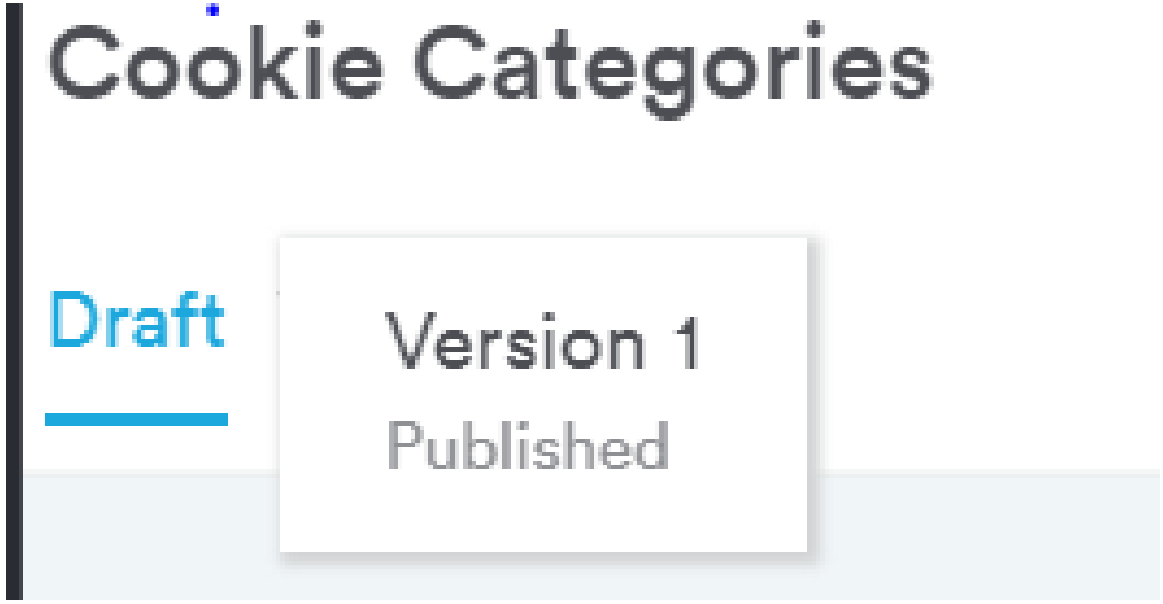
- Select cookie consent banners don’t control Server-Side cookies. These server-side cookies can initiate other cookies that are controlled by consent banner applications, causing the users consent to be ignored inadvertently.
- These server-side cookies/initiators can cause problems when trying to manage user cookie consent.
- These cookies can be identified through Google Chrome’s Network tab. After selecting a request that set a cookie, you can view the “Initiator” tab, with the top level being what initiated the cookie.



One Advertiser & Multiple Trackers



Lack of Version Control for Website Updates



Improper Cookie Classification

Cookie Category
Essential

Description
These cookies are essential to support core site functionality such as providing secure log-in.

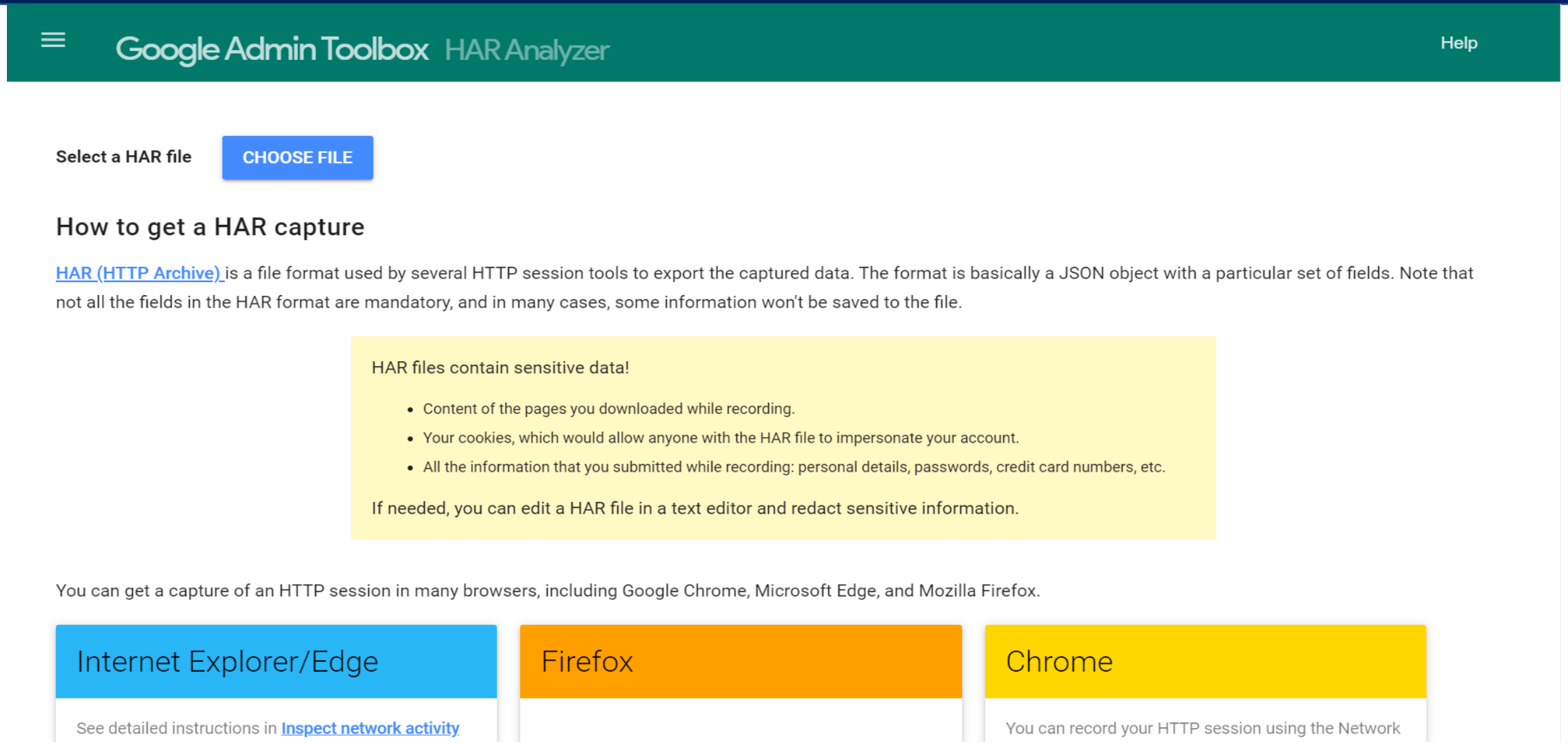
534 Cookies

- Facebook
- Amazon
- Linkedin
- Snapchat

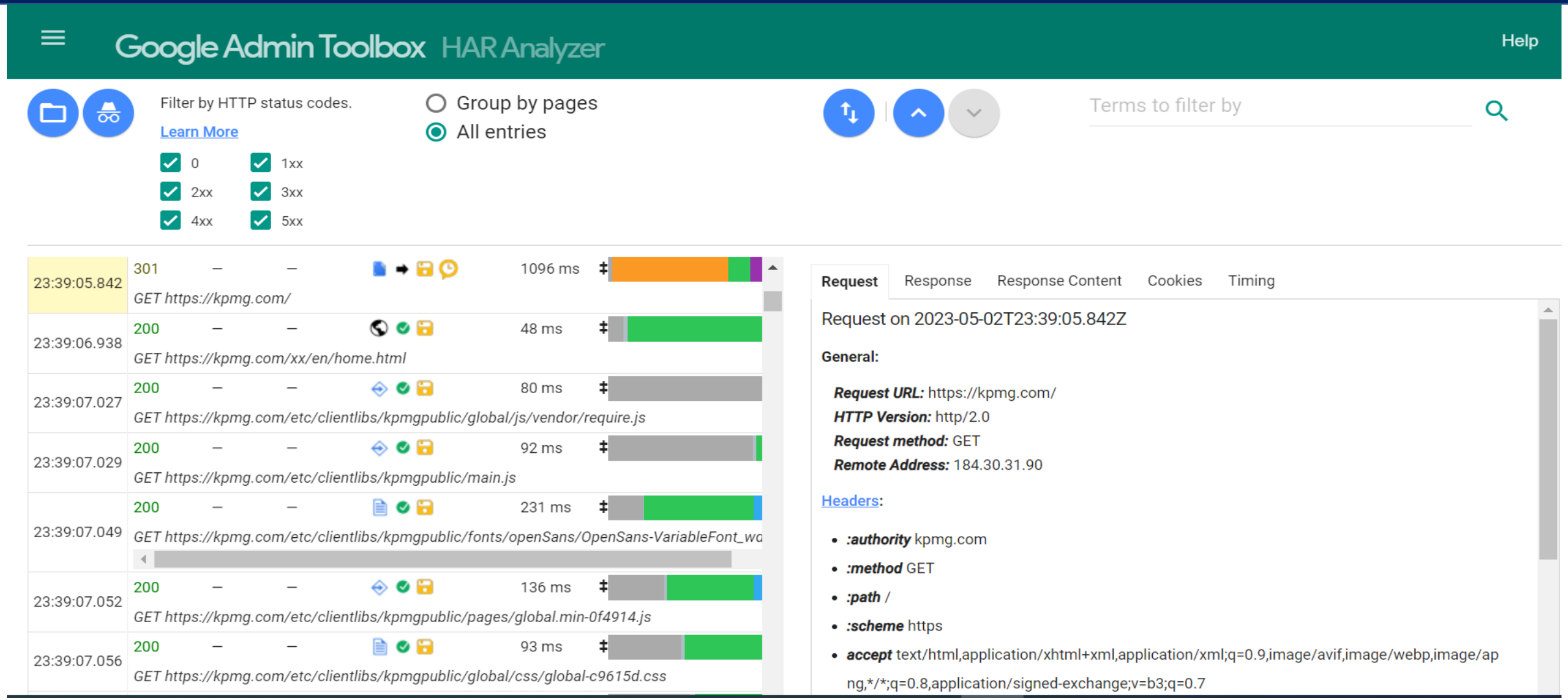
HOW PLAINTIFFS FIND VIOLATIONS

Privacy+ Security Forum

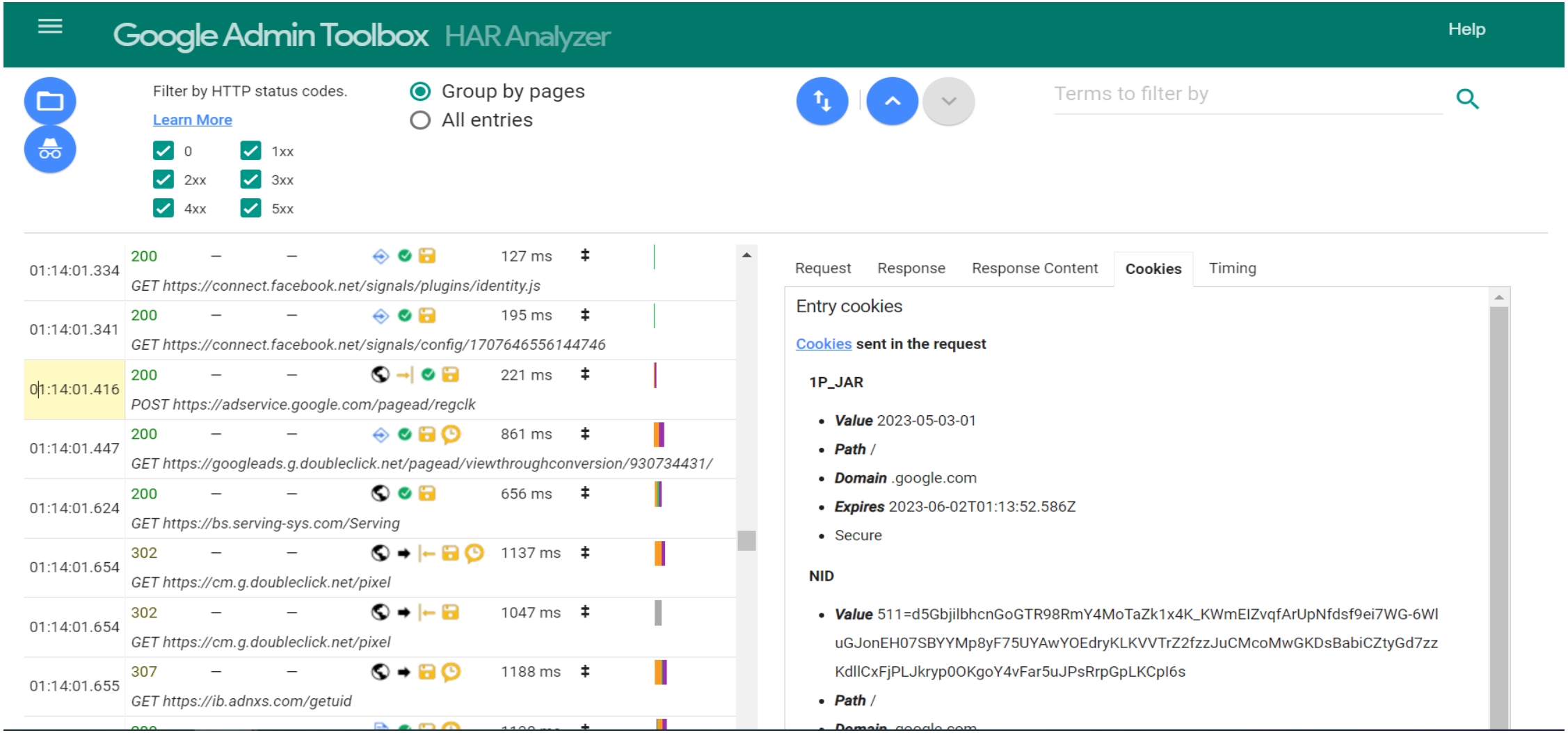
Analyzing .HAR Files – Google Admin Toolbox



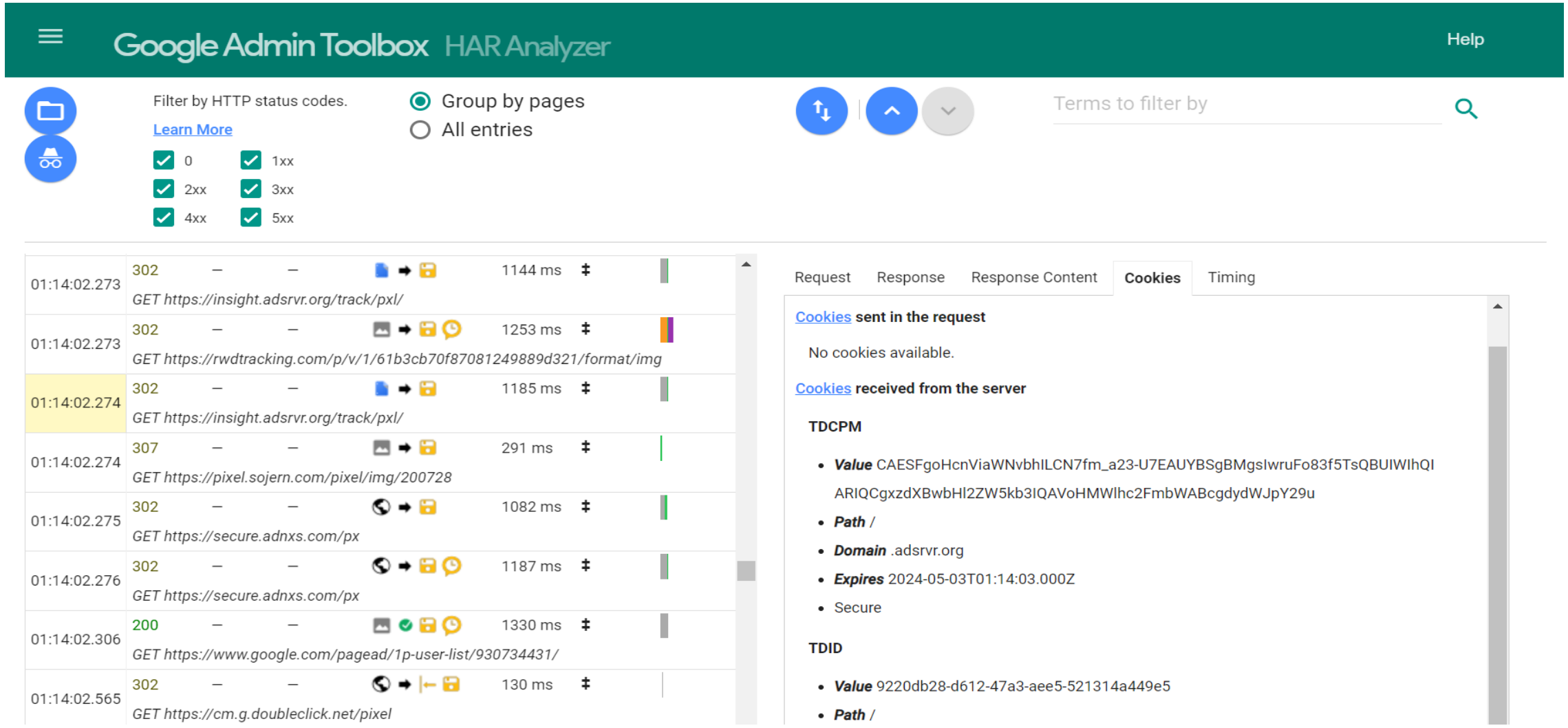
Analyzing .HAR Files – Google Admin Toolbox



Analyzing .HAR Files – Google Admin Toolbox



Analyzing .HAR Files – Google Admin Toolbox



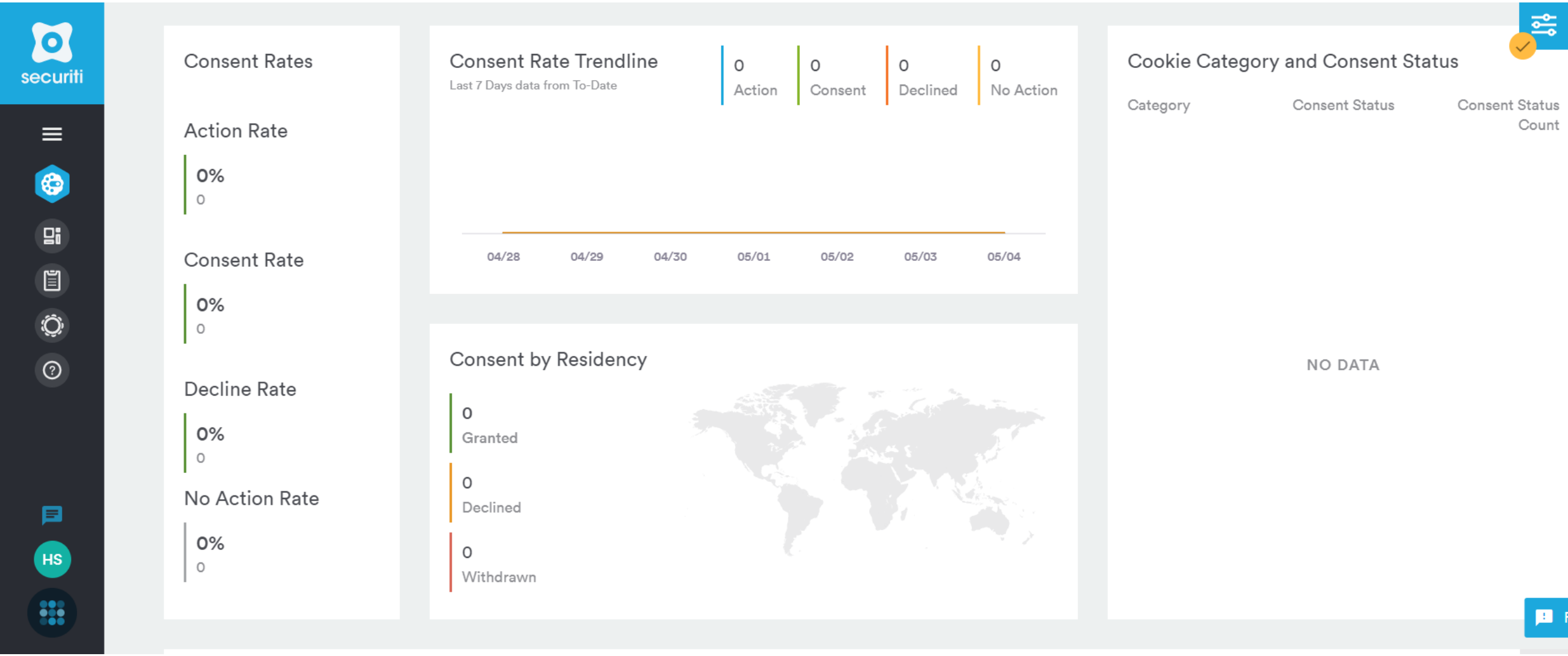
DATA SOURCES FOR INVESTIGATION

Privacy+ Security Forum

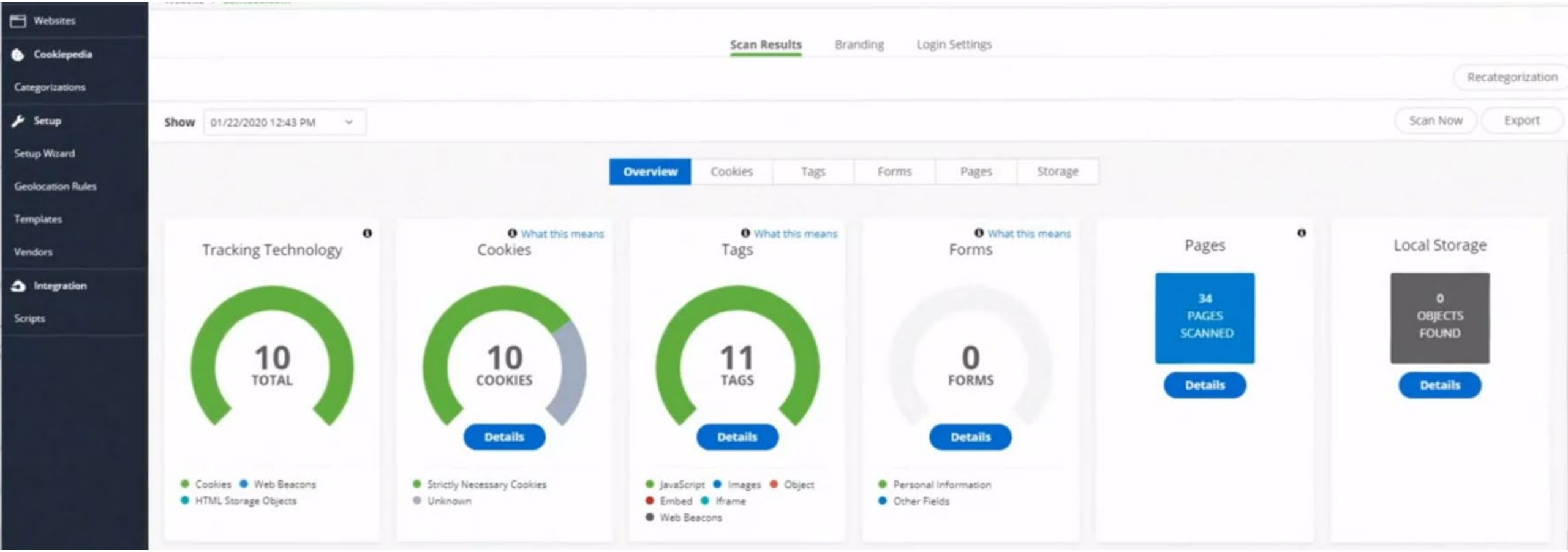
Web Logs

```
02:29:12 127.0.0.1 GET / 200
02:29:35 127.0.0.1 GET /index.html 200
02:41:06 127.0.0.1 GET / 304
02:52:36 127.0.0.1 GET /shop.php 200
03:17:03 127.0.0.1 GET /admin/style.css 200
04:04:54 127.0.0.1 GET /favicon.ico 404
04:38:07 127.0.0.1 GET /js/consent.js 200
```

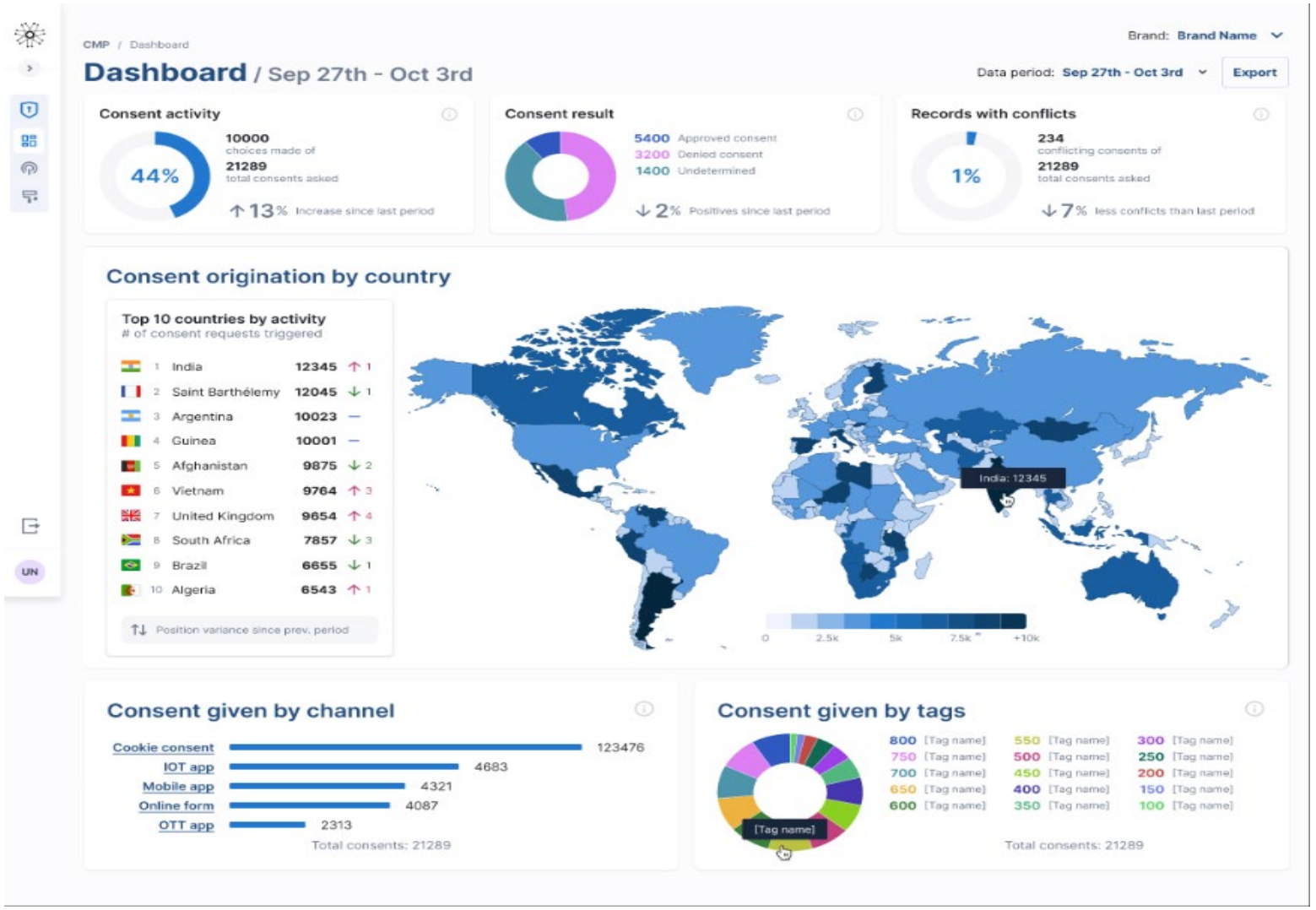
Privacy Management tools – Securiti AI



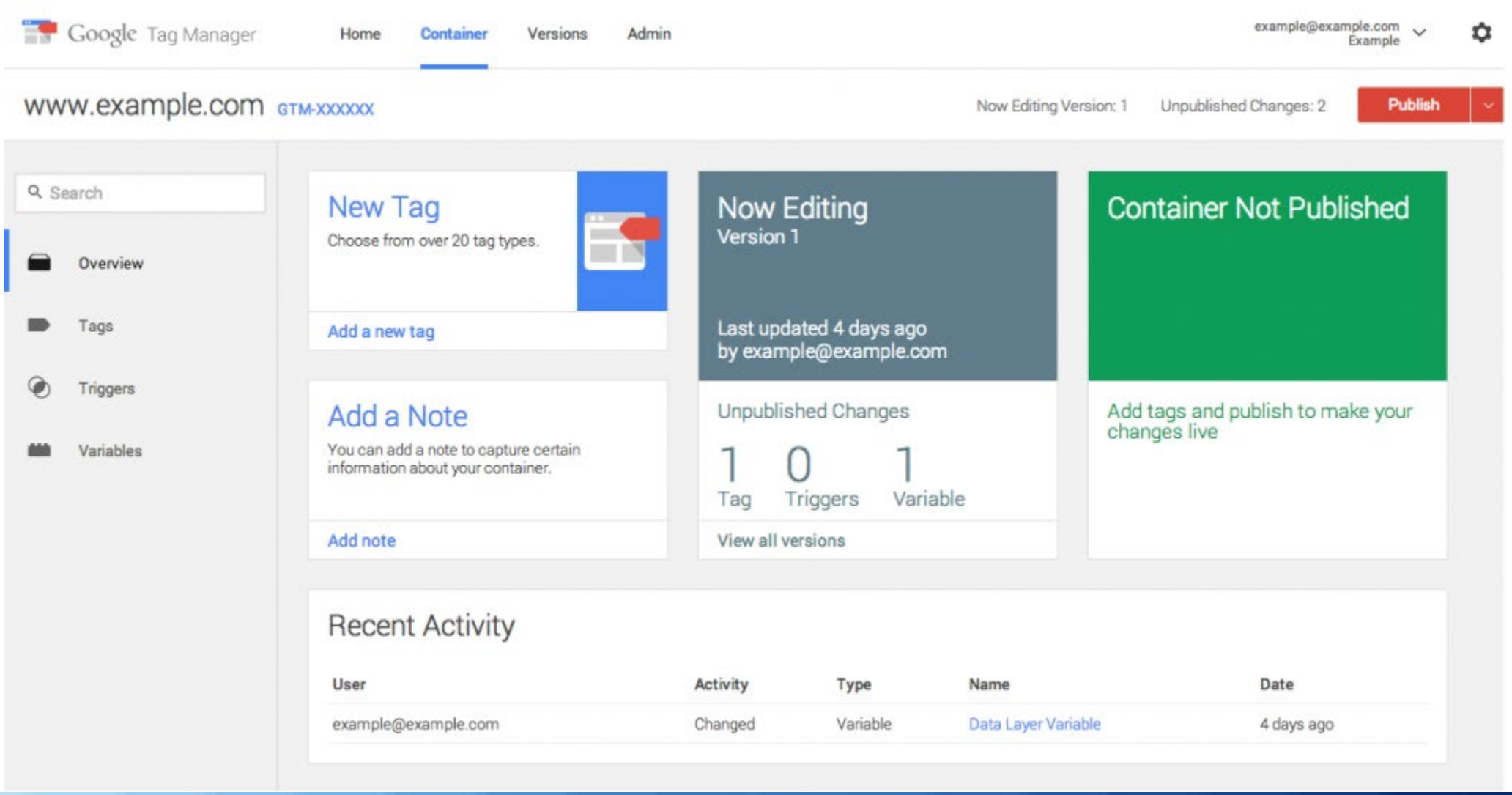
Privacy Management tools – OneTrust



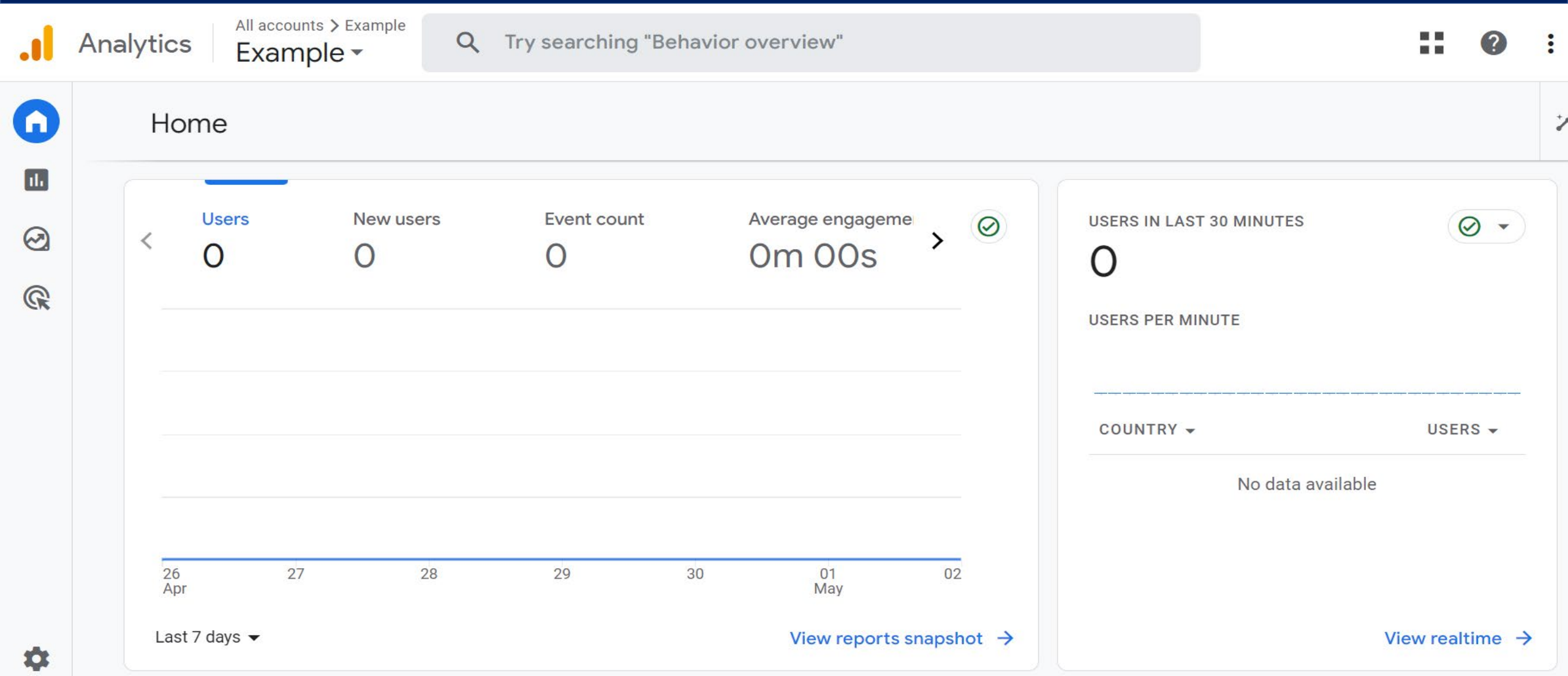
Web Logs


CMP / Dashboard
Brand: Brand Name
Dashboard / Sep 27th - Oct 3rd
Data period: Sep 27th - Oct 3rd
Export
Consent activity
44%
10000
choices made of
21289
total consents asked
↑13% Increase since last period
Consent result
5400 Approved consent
3200 Denied consent
1400 Undetermined
↓2% Positives since last period
Records with conflicts
1%
234
conflicting consents of
21289
total consents asked
↓7% less conflicts than last period
Consent origination by country
Top 10 countries by activity
# of consent requests triggered
1 India 12345 ↑1
2 Saint Barthélemy 12045 ↓1
3 Argentina 10023 —
4 Guinea 10001 —
5 Afghanistan 9875 ↓2
6 Vietnam 9764 ↑3
7 United Kingdom 9654 ↑4
8 South Africa 7857 ↓3
9 Brazil 6655 ↓1
10 Algeria 6543 ↑1
Position variance since prev. period
India: 12345
0
2.5k
5k
7.5k
+10k
Consent given by channel
Cookie consent 123476
IOT app 4683
Mobile app 4321
Online form 4087
OTT app 2313
Total consents: 21289
Consent given by tags
[Tag name]
800 [Tag name]
750 [Tag name]
700 [Tag name]
650 [Tag name]
600 [Tag name]
550 [Tag name]
500 [Tag name]
450 [Tag name]
400 [Tag name]
350 [Tag name]
300 [Tag name]
250 [Tag name]
200 [Tag name]
150 [Tag name]
100 [Tag name]
Total consents: 21289

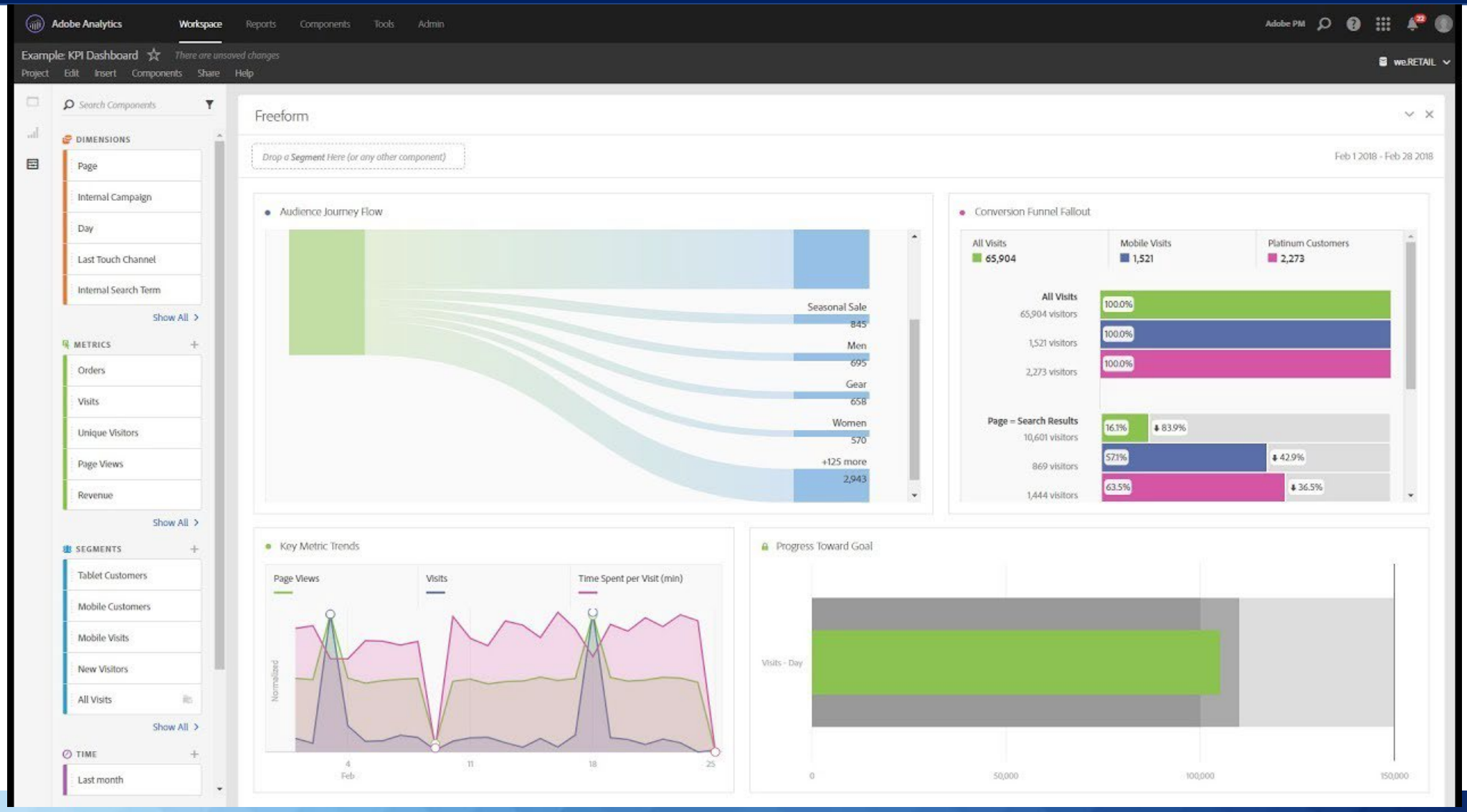
Tag Manager


Google Tag Manager
Home
Container
Versions
Admin
example@example.com
Example
www.example.com
GTM-XXXXXX
Now Editing Version: 1
Unpublished Changes: 2
Publish
Search
Overview
Tags
Triggers
Variables
New Tag
Choose from over 20 tag types.
Add a new tag
Add a Note
You can add a note to capture certain information about your container.
Add note
Now Editing
Version 1
Last updated 4 days ago
by example@example.com
Unpublished Changes
1 Tag
0 Triggers
1 Variable
View all versions
Container Not Published
Add tags and publish to make your changes live
Recent Activity
User
Activity
Type
Name
Date
example@example.com
Changed
Variable
Data Layer Variable
4 days ago

Analytics Tools - Google Analytics



Analytics Tools - Adobe Analytics



PRIVACY INCIDENT LITIGATION

Privacy+ Security Forum

How Did We Get Here

Facebook Tracking Litigation (2011 -2020)

- Two Flavors of Cookies: Session (C_user) and Tracking (datr)
- When logging out, tracking cookies did not expire.
- If not logged out, session cookies did not expire
- FB tracked users' internet activity on non-FB website pages that displayed a "Like" button and connected back to user's FB profile

How Did We Get Here

Example of Cookie (being set)

datr = zxyZT0t2PLYpipRzS-6tjKP

lu = ggIWeqepTLbjoT0WgL

openid_p = 101045999

c_user = 055522222

sct = 1237000000

xs = 123a00905e8967f91ec5886cf73dd4a32f7

act = 479825677458 6%2F0

Example of Cookie (post log out)

datr = zxyZT0t2PLYpipRzS-6tjKP

openid_p = 101045999

act = 479825677458 6%2F0

L=2

Locale = en_US

lu = ggIWeqepTLbjoT0WgL

Lsd = Iprr1

Reg_fb_gate = www.facebook.com%2Index.php

Reg_fb_ref = www.facebook.com%2Findex.php

Litigation Result

Claims: violations of the Wiretap Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and several California consumer protection statutes

Settlement – $90million

Plus - 9 Years of Attorneys Fees

Wiretapping

California Invasion of Privacy Act (CIPA)

- **In a nutshell:** 1967 law that prohibits reading, attempting to read, or learning the contents of a communication without the consent of all parties to the communication.
- **Violations**: $2,500, or by imprisonment in the county jail not exceeding one year, or both. Repeat offenders can be punished by a fine up to $10,000 or by imprisonment in the county jail not exceeding one year, or both.
- **Class Action Dream**: CIPA allows for a private right of action with no burden to prove actual damages, and allows for statutory damages.

A Tale of Two Claims: Session Replay

Section 631(a) of the CIPA generally restricts a third party's unauthorized wiretapping or eavesdropping on an ongoing communication between two parties.

Plaintiffs' core theory in these cases is that the use of session replay technology constitutes illegal wiretapping or eavesdropping in violation of Section 631(a).

Theory had previously been rejected by federal district courts.

Javier v. Assurance IQ, LLC

- Website through which users could request life insurance quotes
- CIPA claims against website operator and software maker
- 9th Circuit reversed dismissal finding allegations that he did not consent to having his session tracked *before* agreeing to the website's privacy policy were sufficient
- Court did not address three defenses: (1) that the plaintiff gave "implied consent", (2) that the software provider is not a "third party" under CIPA, and (3) that the statute of limitations had run.
- January 2023: dismissed again on SOL with leave to amend.

A Tale of Two Claims: Chatbots

"Litigation Tester" visits a website and uses the chat to voluntarily communicate with customer service (usually just types returns and then leaves)

Form demand letter offering to settle a threatened CIPA lawsuit for 6-7 figures

A cookie-cutter lawsuit is filed with hyperventilating allegations that the plaintiff was "shocked and appalled" to discover that the "Defendant secretly records those conversations and pays third parties to eavesdrop on them in real time."

Video Privacy Protection Act (VPPA)

Born after the video rental history of U.S. Supreme Court nominee Robert Bork was leaked to the media. (His history was innocuous.)

Prohibits a “video tape service provider” from disclosing data identifying individuals’ requested or obtained video materials.

Because “video tape service provider” encompasses purveyors of “audio-visual materials” similar to video tapes, plaintiffs have broadly interpreted the definition to include website or mobile app providers that offer videos on their platforms.

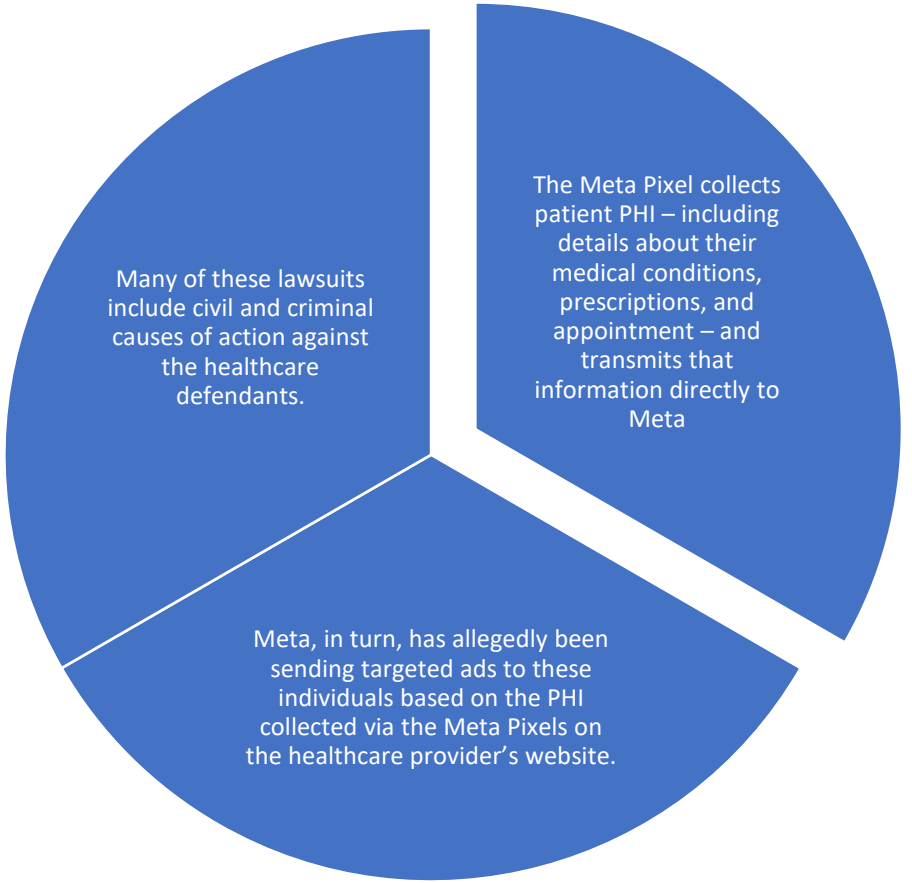
Violations: actual or liquidated damages of at least $2,500 per affected consumer, punitive damages, attorneys' fees and costs

VPPA & The Meta Pixel

- Data sharing on websites often comes in the form of cookies and code imbedded on websites that tracks the activity of website users.
- Meta's Pixel is code embedded on the websites of several companies that tracks certain activity of website users.
- Plaintiffs allege that the information is transmitted to Meta, which can then link the information to the users' Facebook accounts.
- This can include information about a user's video watching habits, which plaintiffs allege violates VPPA

Healthcare Industry Grapples with Misconfigured Meta Pixel

- A Meta Pixel is a small piece of JavaScript code, commonly referred to as a web beacon, that allows you to track visitor activity on your website.
- An investigation by *The Markup* in June 2022 found that 33 of the top 100 hospitals in the United States use the Meta Pixel on their websites.
- Many hospitals and health systems have these web beacons embedded on their websites and inside password-protected patient portals.



Key Takeaways/Action Items

Understand the tracking tools being used (cookies, Meta Pixel etc.), how they are configured, and which pages they are firing on
Consent is a defense
Update privacy policies and terms of use
Consider use of effective privacy management tools
Be prepared to leverage investigative tools
Add a privacy incident to your table-top exercises

Questions & Contacts

Jonathan Fartlough

jfairtlough@kpmg.com
213-598-4181
https://www.linkedin.com/in/jonathan-fairtlough-6984a942/

Wynter Deagle

wdeagle@sheppardmullin.com
o: 858-720-8947
https://www.linkedin.com/in/wynterlavier/

Anne-Marie Dao

adao@sheppardmullin.com
858.509.3691
https://www.linkedin.com/in/anne-marie-dao/