

May 11, 2023

Wait, A Privacy Incident is a Security Incident?

Presenters



**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

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



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: UID data determines ability to reduce class

Data available determines success

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

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.

▼ Request initiator chain

▼ <https://tags.tiqcdn.com/utag/aa/main/prod/utag.js>

▼ <https://secure-ds.serving-sys.com/SemiCachedScripts/ebOneTag.js>

▼ <https://secure.adnxs.com/px?id=1135302&seg=18541478&t=2>

▼ https://ad.doubleclick.net/ddm/activity/src=8587884;type=invmedia;cat=aa-ac00;dc_lat=;dc_rdid=;tag_for_ch

▼ https://ad.doubleclick.net/ddm/activity/src=8587884;dc_pre=CPGmvKz81_4CFQbNGAIdktAAaw;type=inv
https://adservice.google.com/ddm/fls/z/src=8587884;dc_pre=CPGmvKz81_4CFQbNGAIdktAAaw;type=in

One Advertiser & Multiple Trackers



Filter by HTTP status codes.

[Learn More](#)

- 0
- 1xx
- 2xx
- 3xx
- 4xx
- 5xx

Group by pages

All entries



adnxs



Time	Status	Response	Size	Time	Size	Time
01:14:01.655	307	—	—	1188 ms	1188 ms	1188 ms
GET https://ib.adnxs.com/getuid						
01:14:02.271	302	—	—	1162 ms	1162 ms	1162 ms
GET https://insight.adsrvr.org/track/pxl/						
01:14:02.275	302	—	—	1082 ms	1082 ms	1082 ms
GET https://secure.adnxs.com/px						
01:14:02.276	302	—	—	1187 ms	1187 ms	1187 ms
GET https://secure.adnxs.com/px						
01:14:02.751	302	—	—	334 ms	334 ms	334 ms
GET https://ib.adnxs.com/bounce						
01:14:03.418	302	—	—	140 ms	140 ms	140 ms
GET https://ib.adnxs.com/getuid						
01:14:03.446	302	—	—	233 ms	233 ms	233 ms
GET https://insight.adsrvr.org/track/pxl/						
...	302	—	—	243 ms	243 ms	243 ms

Request Response Response Content Cookies Timing

Request on 2023-05-03T01:14:01.655Z

General:

- Request URL:** https://ib.adnxs.com/getuid?https://pixel.sojern.com/idsync/apn?id=\$UID&sjrn_id=owed8shYwslJESbKwr1cXsuAqN8JG7XNDBP1e-dvmJ60Zay1N931MGbx0ivxkT_Y
- HTTP Version:** http/2.0
- Request method:** GET
- Remote Address:** 104.254.151.68

Headers:

- :authority** ib.adnxs.com
- :method** GET
- :path** /getuid?https://pixel.sojern.com/idsync/apn?id=\$UID&sjrn_id=owed8shYwslJESbKwr1cXsuAqN8JG7XNDBP1e-dvmJ60Zay1N931MGbx0ivxkT_Y
- :scheme** https

Lack of Version Control for Website Updates

Cookie Categories

Draft

Version 1
Published

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

Analyzing .HAR Files – Google Admin Toolbox



Select a HAR file

CHOOSE FILE

How to get a HAR capture

[HAR \(HTTP Archive\)](#) is a file format used by several HTTP session tools to export the captured data. The format is basically a JSON object with a particular set of fields. Note that not all the fields in the HAR format are mandatory, and in many cases, some information won't be saved to the file.

HAR files contain sensitive data!

- Content of the pages you downloaded while recording.
- Your cookies, which would allow anyone with the HAR file to impersonate your account.
- All the information that you submitted while recording: personal details, passwords, credit card numbers, etc.

If needed, you can edit a HAR file in a text editor and redact sensitive information.

You can get a capture of an HTTP session in many browsers, including Google Chrome, Microsoft Edge, and Mozilla Firefox.

Internet Explorer/Edge

See detailed instructions in [Inspect network activity](#)

Firefox

Chrome

You can record your HTTP session using the Network

Analyzing .HAR Files – Google Admin Toolbox

Google Admin Toolbox HAR Analyzer Help

Filter by HTTP status codes. Group by pages All entries Terms to filter by

0 1xx
 2xx 3xx
 4xx 5xx

Time	Status	Method	URL	Duration	Size
23:39:05.842	301	GET	https://kpmg.com/	1096 ms	1096
23:39:06.938	200	GET	https://kpmg.com/xx/en/home.html	48 ms	48
23:39:07.027	200	GET	https://kpmg.com/etc/clientlibs/kpmgpublic/global/js/vendor/require.js	80 ms	80
23:39:07.029	200	GET	https://kpmg.com/etc/clientlibs/kpmgpublic/main.js	92 ms	92
23:39:07.049	200	GET	https://kpmg.com/etc/clientlibs/kpmgpublic/fonts/openSans/OpenSans-VariableFont_wd	231 ms	231
23:39:07.052	200	GET	https://kpmg.com/etc/clientlibs/kpmgpublic/pages/global.min-0f4914.js	136 ms	136
23:39:07.056	200	GET	https://kpmg.com/etc/clientlibs/kpmgpublic/global/css/global-c9615d.css	93 ms	93

Request | Response | Response Content | Cookies | Timing

Request on 2023-05-02T23:39:05.842Z

General:

- Request URL:** https://kpmg.com/
- HTTP Version:** http/2.0
- Request method:** GET
- Remote Address:** 184.30.31.90

Headers:

- :authority** kpmg.com
- :method** GET
- :path** /
- :scheme** https
- accept** text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Analyzing .HAR Files – Google Admin Toolbox

Google Admin Toolbox HAR Analyzer Help

Filter by HTTP status codes. [Learn More](#)

- 0
- 1xx
- 2xx
- 3xx
- 4xx
- 5xx

Group by pages

All entries

Terms to filter by

Time	Status	Method	URL	Size	Time	Icons
01:14:01.334	200	GET	https://connect.facebook.net/signals/plugins/identity.js	127 ms		
01:14:01.341	200	GET	https://connect.facebook.net/signals/config/1707646556144746	195 ms		
01:14:01.416	200	POST	https://adservice.google.com/pagead/regclk	221 ms		
01:14:01.447	200	GET	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/930734431/	861 ms		
01:14:01.624	200	GET	https://bs.serving-sys.com/Serving	656 ms		
01:14:01.654	302	GET	https://cm.g.doubleclick.net/pixel	1137 ms		
01:14:01.654	302	GET	https://cm.g.doubleclick.net/pixel	1047 ms		
01:14:01.655	307	GET	https://ib.adnxs.com/getuid	1188 ms		

Request Response Response Content **Cookies** Timing

Entry cookies

[Cookies](#) sent in the request

1P_JAR

- Value** 2023-05-03-01
- Path** /
- Domain** .google.com
- Expires** 2023-06-02T01:13:52.586Z
- Secure

NID

- Value** 511=d5GbjlbhcnGoGTR98RmY4MoTaZk1x4K_KWmEIZvqfArUpNfdsf9ei7WG-6WIuGJonEH07SBYYMp8yF75UYAwYOEdryKLKVVTrZ2fzzJuCMcoMwGKDsBabiCZtyGd7zzKdIlCxFjPLJkryp0OKgoY4vFar5uJPsrRpGpLKcPl6s
- Path** /
- Domain** google.com

Analyzing .HAR Files – Google Admin Toolbox

Google Admin Toolbox HAR Analyzer Help

Filter by HTTP status codes. [Learn More](#) Group by pages All entries

0 1xx
 2xx 3xx
 4xx 5xx

Terms to filter by

Time	Status	Method	URL	Size	Time	Icons
01:14:02.273	302	GET	https://insight.adsrvr.org/track/pxl/	1144 ms	🔗	
01:14:02.273	302	GET	https://rwdtracking.com/p/v/1/61b3cb70f87081249889d321/format/img	1253 ms	🔗 🗨️	
01:14:02.274	302	GET	https://insight.adsrvr.org/track/pxl/	1185 ms	🔗	
01:14:02.274	307	GET	https://pixel.sojern.com/pixel/img/200728	291 ms	🔗	
01:14:02.275	302	GET	https://secure.adnxs.com/px	1082 ms	🔗	
01:14:02.276	302	GET	https://secure.adnxs.com/px	1187 ms	🔗 🗨️	
01:14:02.306	200	GET	https://www.google.com/pagead/1p-user-list/930734431/	1330 ms	🔗 🗨️	
01:14:02.565	302	GET	https://cm.g.doubleclick.net/pixel	130 ms	🔗	

Request Response Response Content **Cookies** Timing

[Cookies sent in the request](#)

No cookies available.

[Cookies received from the server](#)

TDCPM

- Value** CAESFgoHcnViaWNvbhILCN7fm_a23-U7EAUYSgBMgslwruFo83f5TsQBUIWihQIARIQCgxzdXBwbHI2ZW5kb3IQAVoHMWlh2FmbWABcgdydWJpY29u
- Path** /
- Domain** .adsrvr.org
- Expires** 2024-05-03T01:14:03.000Z
- Secure

TDID

- Value** 9220db28-d612-47a3-ae5-521314a449e5
- Path** /

DATA SOURCES FOR INVESTIGATION

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



Consent Rates

Action Rate



Consent Rate



Decline Rate



No Action Rate

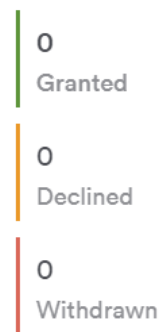


Consent Rate Trendline

Last 7 Days data from To-Date



Consent by Residency



Cookie Category and Consent Status

Category	Consent Status	Consent Status Count
----------	----------------	----------------------

NO DATA

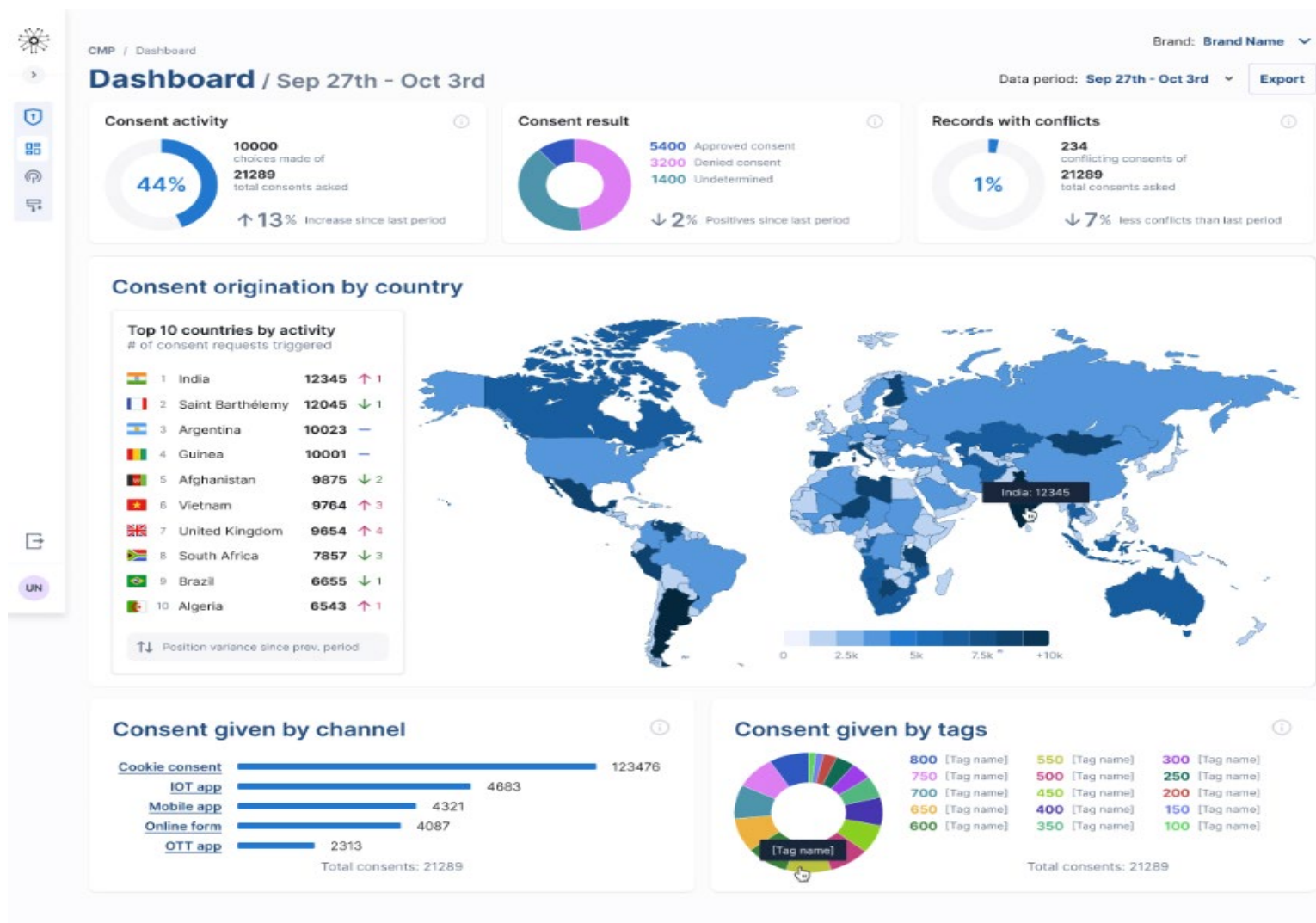


Privacy Management tools – OneTrust

The screenshot displays the OneTrust Privacy Management tool interface. On the left is a dark sidebar with navigation options: Websites, Cookiepedia, Categorizations, Setup, Setup Wizard, Geolocation Rules, Templates, Vendors, Integration, and Scripts. The main content area is titled "Scan Results" and includes sub-navigation for Branding and Login Settings. A "Show" dropdown is set to "01/22/2020 12:43 PM". In the top right, there are buttons for "Recategorization", "Scan Now", and "Export". Below this is a tabbed interface with "Overview" selected, and other tabs for Cookies, Tags, Forms, Pages, and Storage. The main dashboard features six summary cards:

- Tracking Technology:** 10 TOTAL. Legend: Cookies (green), Web Beacons (blue), HTML Storage Objects (teal).
- Cookies:** 10 COOKIES. Legend: Strictly Necessary Cookies (green), Unknown (grey). Includes a "What this means" icon.
- Tags:** 11 TAGS. Legend: JavaScript (green), Images (blue), Object (red), Embed (orange), Iframe (teal), Web Beacons (black). Includes a "What this means" icon.
- Forms:** 0 FORMS. Legend: Personal Information (green), Other Fields (blue). Includes a "What this means" icon.
- Pages:** 34 PAGES SCANNED. Includes a "Details" button.
- Local Storage:** 0 OBJECTS FOUND. Includes a "Details" button.

Web Logs



Tag Manager



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

The screenshot displays the Google Analytics interface. At the top, there is a navigation bar with the 'Analytics' logo, account information ('All accounts > Example Example'), a search bar with the text 'Try searching "Behavior overview"', and utility icons for a grid, help, and a menu. Below the navigation bar is a 'Home' section. The main content area is divided into two panels. The left panel features a summary row with four metrics: 'Users' (0), 'New users' (0), 'Event count' (0), and 'Average engagemen' (0m 00s). Below this is a large empty chart area with a horizontal axis labeled from '26 Apr' to '02 May'. At the bottom of this panel, there is a 'Last 7 days' dropdown menu and a 'View reports snapshot' link. The right panel shows 'USERS IN LAST 30 MINUTES' (0) and 'USERS PER MINUTE' (0). Below these are 'COUNTRY' and 'USERS' dropdown menus, and the text 'No data available'. At the bottom of this panel is a 'View realtime' link.

Analytics | All accounts > Example Example | Try searching "Behavior overview" | ?

Home

Users: 0 | New users: 0 | Event count: 0 | Average engagemen: 0m 00s

USERS IN LAST 30 MINUTES: 0

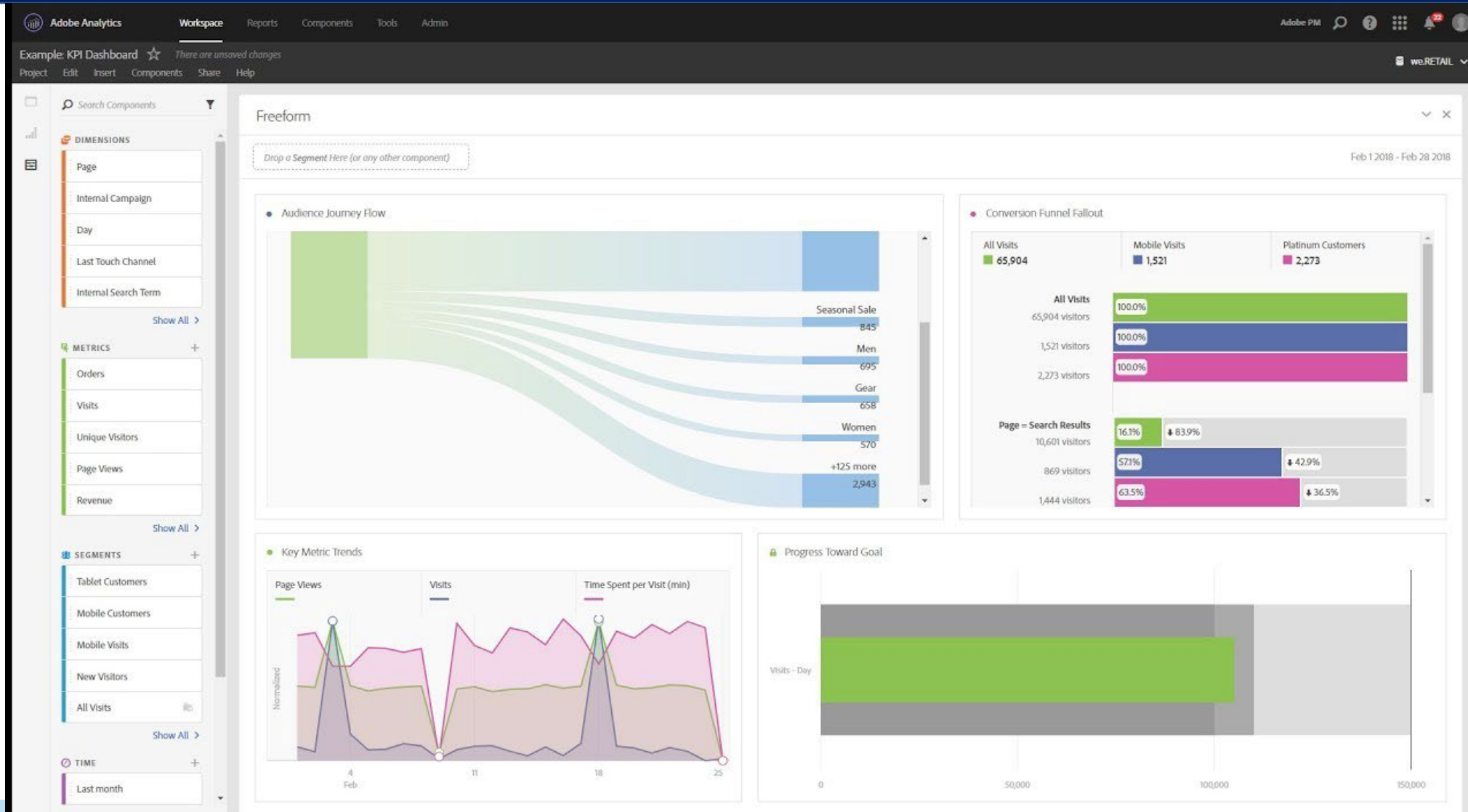
USERS PER MINUTE: 0

COUNTRY | USERS

No data available

Last 7 days | View reports snapshot | View realtime

Analytics Tools - Adobe Analytics



PRIVACY INCIDENT LITIGATION

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 = gglWeqepTLbjoT0WgL
openid_p = 101045999
c_user = 055522222
sct = 1237000000
xs = 123a00905e8967f91ec5886cf73dd4a32f7
act = 4798256774586%2F0

Example of Cookie (post log out)

datr = zxyZT0t2PLYpipRzS-6tjKP
openid_p = 101045999
act = 4798256774586%2F0
L=2
Locale = en_US
lu = gglWeqepTLbjoT0WgL
Lsd = lpr1
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



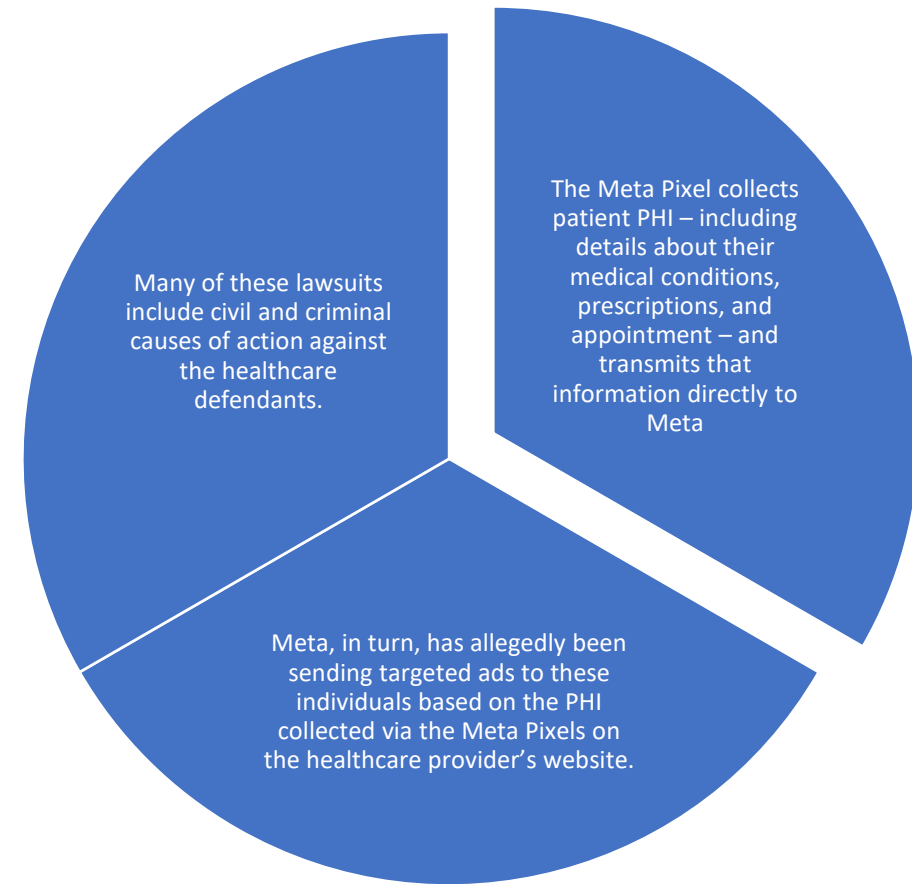
VPPA & The Meta Pixel



- 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

jfartlough@kpmg.com

213-598-4181

<https://www.linkedin.com/in/jonathan-fartlough-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/>