THE PATCHWORK OF CONSENT REQUIREMENTS AND HEALTH DATA:

WHAT SHOULD COMPANIES CONSIDER

May 2024

orrick

Agenda

- What is "Adtech"?
- How Does "Adtech" work?
- Health Data Compliance
- Configuration Mishaps

WHAT IS "ADTECH"?

The Adtech Ecosystem

AdTech Landscape 2021

playwire

WHAT IS "ADTECH"?

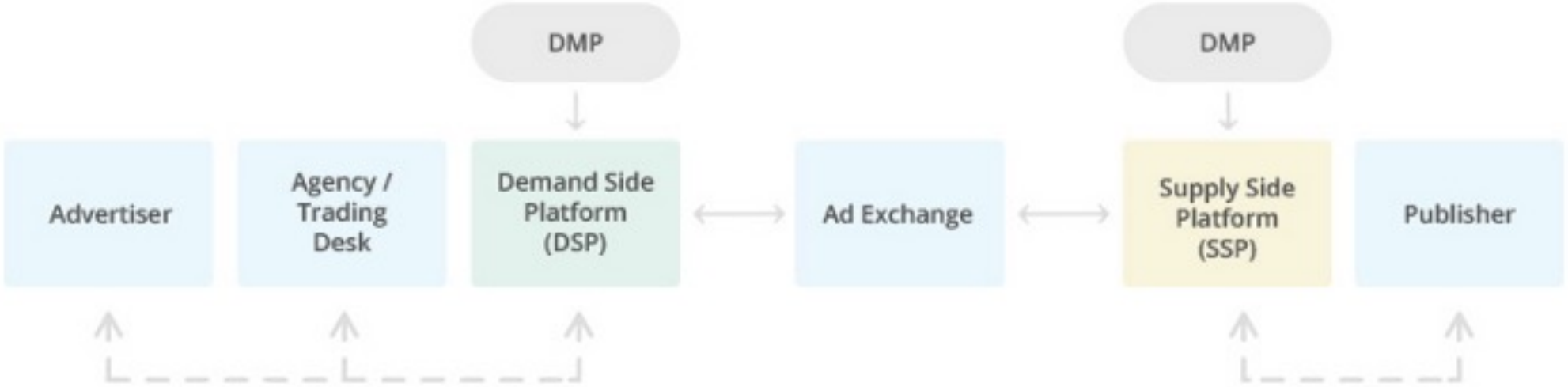
- Here are some words we'll be using (others will be described throughout the training):
  - Digital Property: A website, mobile application, OTT streaming service, or similar property (even a connected fridge!). Basically, anything connected to the Internet.
  - Publisher: These are owners of digital properties that have ad inventory for sale (e.g., New York Times, Hearst).
  - Advertiser: A brand that wants to buy a publisher's ad inventory.
  - Inventory: The total number of ad units on a publisher digital property that are available for advertisers to buy.
  - Ad Unit: A particular space on a publisher digital property that the publisher has designated as available for an ad.
  - Impression: The ad that is inserted into a particular ad unit.
  - Creative: The design of the ad itself (e.g., the art, font, look-and-feel)…it's what you see!
- Technically, the term "adtech" stands for "advertising technology," which relates to the *intermediaries* that provide the technology to facilitate the buying and selling of ad inventory (e.g., DSPs, SSPs) between advertisers and publishers.
- However, the term "adtech" has basically become a shorthand word for the general concept of **buying and selling of digital advertising "inventory" in an automated manner**.

HOW DOES "ADTECH" WORK?

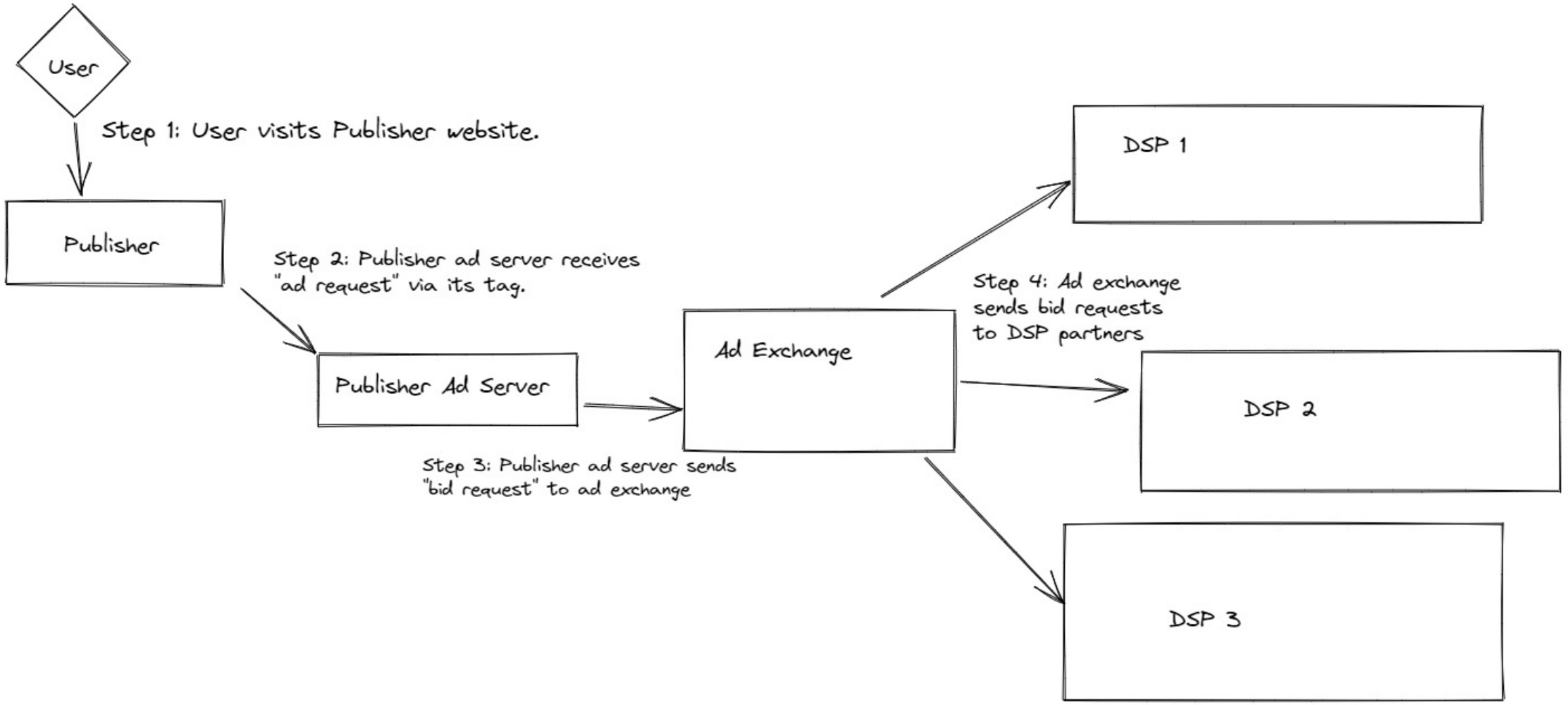
Custom Audiences

- Retargeting via uploads of CRM data (e.g., email address, phone number, typically in hashed format)
- Retargeting via pixels/API
  - Events (standard or custom)
  - Page URL and website metadata
  - IP address/user agent string (device make, device model, browser information, OS information)
  - 1st-party/3rd-party cookie ID
  - Hashed email address
  - Hashed phone number
- Look-a-like audiences

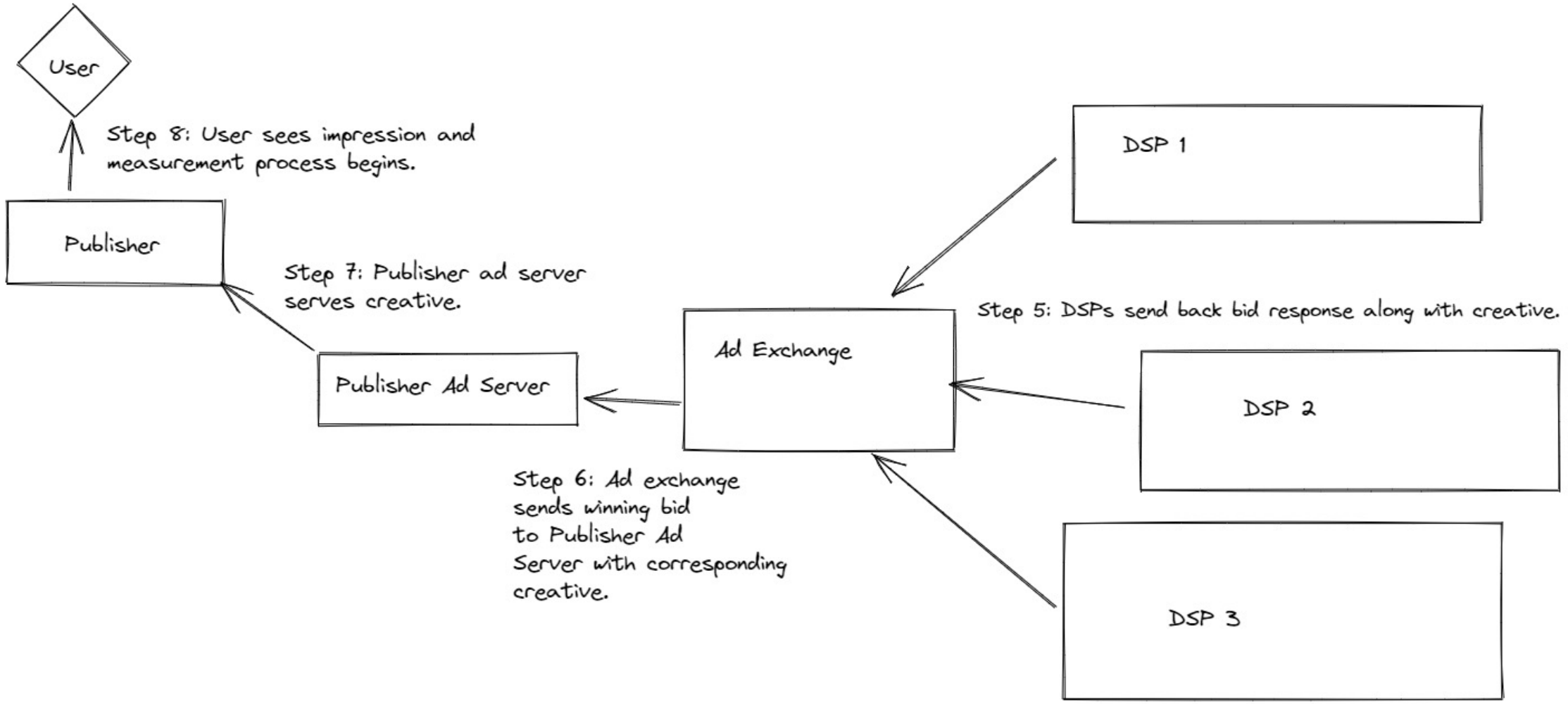
Real-Time Bidding



RTB SUMMARY DIAGRAM (PART 1)



RTB SUMMARY DIAGRAM (PART 2)



Bid Requests

```
id: "BIDREQUEST_ID"
imp {
  id: "1"
  banner {
    w: 728
    h: 90
    pos: BELOW_THE_FOLD
    expdir: LEFT
    expdir: RIGHT
    expdir: UP
    expdir: DOWN
    format {
      w: 728
      h: 90
    }
  }
  tagid: "TAG_ID"
  bidfloor: 0.61
  bidfloorcur: "USD"
  secure: true
  metric {
    type: "click_through_rate"
    value: 0
    vendor: "EXCHANGE"
  }
  metric {
    type: "viewability"
    value: 0
    vendor: "EXCHANGE"
  }
  metric {
    type: "session_depth"
    value: 86
    vendor: "EXCHANGE"
  }
  [com.google.doubleclick.imp] {
    billing_id: "BILLING_ID"
    dfp_ad_unit_code: "/DFP_NETWORK_CODE/AD/UNIT/
PATH"
    ampad: AMP_AD_ALLOWED_AND_NOT_EARLY_RENDERED
  }
}
site {
  page: "PAGE_URL"
  publisher {
    id: "SELLER_NETWORK_ID"
    [com.google.doubleclick.publisher] {
      country: "GB"
    }
  }
```

What this specific person is reading right now

```
    [com.google.doubleclick.site] {
      amp: DIALECT_HTML
    }
  }
  device {
    ua: "Mozilla/5.0 (Linux; Android 4.4.4; SM-T560
  Build/KTU84P) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/63.0.3239.111 Safari/537.36"
    ip: "IP_ADDRESS"
    geo {
      lat: 42.6495361328125
      lon: 23.35913848876953
      country: "BGR"
      city: "Sofia"
      utcoffset: 120
    }
    make: "samsung"
    model: "sm-t560"
    os: "android"
    osv: "4.4.4"
    devicetype: TABLET
    w: 1280
    h: 800
    pxratio: 1
  }
  user {
    id: "GOOGLE_USER_ID"
    buyeruid: "HOSTED_MATCH_USER_DATA"
    customdata: "HOSTED_MATCH_USER_DATA"
    data {
      id: "DetectedVerticals"
      name: "DoubleClick"
      segment {
        id: "5444"
        value: "0.3"
      }
      segment {
        id: "1080"
        value: "0.2"
      }
      segment {
        id: "1710"
        value: "0.1"
      }
      segment {
        id: "1715"
        value: "0"
      }
      segment {
        id: "96"
        value: "0"
      }
```

Distinctive information about this specific person's device

This specific person's IP address

This specific person's GPS coordinates

Various ID codes identifying this specific person, facilitating re-identification and tying to existing profiles

This specific person's inferred interests. This could include highly sensitive special category data such as 571 eating disorders, 410 left-wing politics, 202 male impotence, 862 Buddhism, 625 AIDS & HIV, 547 African-Americans, etc. See Goolge's "publisher verticals" list.

U.S. COMPLIANCE REGIMES

FTC Enforcement Actions

The FTC has been actively enforcing the FTC Act and the HBNR:

Settlement	GoodRx	BetterHelp	Easy Healthcare
Alleged Violations	The FTC alleged that GoodRx violated **Section 5** and the **HBNR** by sharing personal health data through tracking technologies operated by Facebook, Google, and other online advertising platforms, ***despite*** public statements that they did not sell or share data.	FTC alleged BetterHelp violated **Section 5** by providing sensitive health data to platforms such as Facebook and Snapchat for advertising purposes without consumer consent, ***despite*** promising consumers it would not use or disclose health data except for limited purposes.	FTC alleged Easy Healthcare violated **Section 5** and the **HBNR** by disclosing health data to third parties, including through the use of SDKs, for advertising purposes without notice to or consent from consumers ***despite*** representations to the contrary. FTC also alleged failure to implement reasonable privacy and security measures.
Penalties	$1.5 million	$7.8 million	$100,000

FTC Enforcement Actions

The FTC has been actively enforcing the FTC Act and the HBNR:

Settlement	Flo Health	Cerebral	Monument
Alleged Violations	FTC alleged Flo Health violated **Section 5** by providing sensitive reproductive health data to platforms such as Facebook and Google for advertising purposes without limiting how these third parties could use the data, ***despite*** promising consumers it would not use or disclose health data except for limited purposes.	The FTC alleged that Cerebral violated **Section 5** by disclosing sensitive personal health information and other sensitive data to third parties for advertising purposes and by engaging in unfair and deceptive practices regarding Cerebral's security practices and cancellation procedures. The complaint also charges that Cerebral and its former CEO allegedly violated OARFPA by engaging in unfair and deceptive practices with respect to substance use disorder treatment services.	The FTC alleged Monument violated **Section 5** by misrepresenting and failing to implement reasonable privacy measures to prevent disclosure of health information by disclosing users' personal health data to third-party advertising platforms for advertising without consumer consent, after promising to keep such information confidential. The FTC also alleged violations of OARFPA by misrepresenting its disclosure of consumers' personal information for advertising purposes.
Penalties	No monetary penalty.	$5.1 million (for partial refunds to impacted consumers) $10 million (suspended to $2 million penalty payment due to the company's inability to pay the full amount)	$2.5 million

FTC Health Breach Notification Rule (HBNR)

Applies to non-HIPAA entities – vendors of Personal Health Records and PHR-Related Entities, including health apps, connected devices, and similar products.

Trigger

- Acquisition of unsecure PHR identifiable health information caused by:
  - Cybersecurity intrusion
  - Unauthorized disclosure of sensitive information

Breach Notification

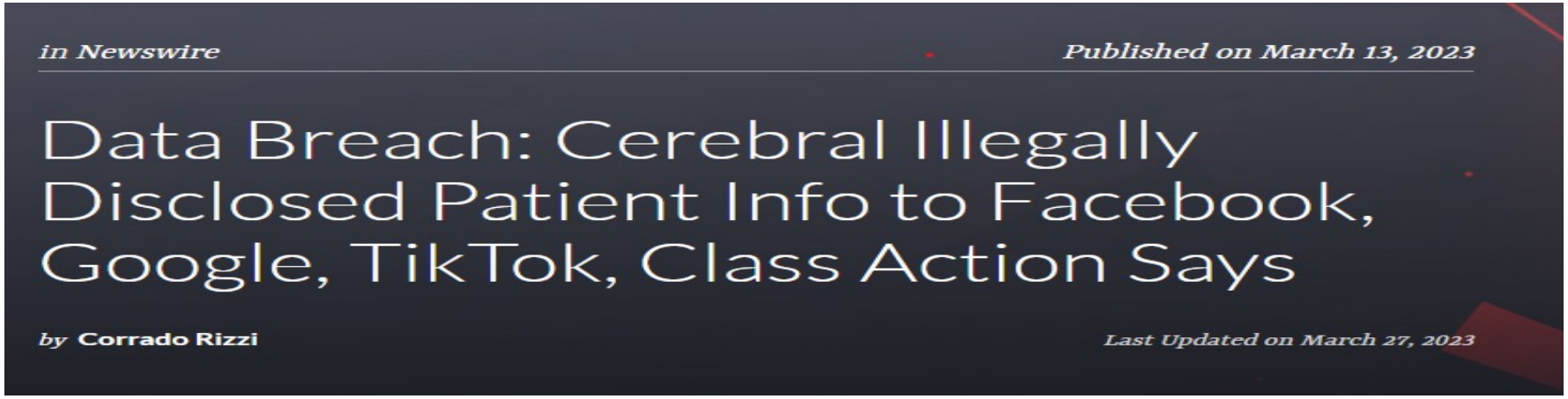
- Must notify individuals, FTC (if over 500 individuals, within 60 days), and in some cases, the media

Enforcement

- Restored vigor
- To date, only a handful of companies have reported

Healthcare Pixel Litigation Themes

- Since June 2022, **hundreds** of class action lawsuits have been filed against hospitals and healthcare companies nationally for their use of tracking technologies.
  - While most cases are still in the early stages, a suit filed in Massachusetts settled for **$18.4 million** in early 2022 (before OCR released its guidance).



Related Emerging Issues – Session Replay and Chatbots

- ***Session Replay***. A session replay code enables website operators to record and replay user interactions with their websites, including clicks, scrolls, hovers, web pages visited, and data submissions. This information is often used for marketing purposes. Session replay has been the subject of recent state wiretap law litigation.

- ***Chatbots***. Websites use chatbots to respond to user questions about companies and their services, and the chatbots may retain transcripts of the communications. Individuals are suing companies that use this technology, alleging that it is a violation of wiretapping laws.

Potential Statutory Liability

- **California Confidentiality of Medical Information Act ("CMIA")**
  - *Damages if Disclosure Led to Economic Loss or Personal Injury*: Compensatory damages, punitive damages up to $3,000 and attorneys' fees not to exceed $1,000, and costs of litigation for any violating disclosure of medical information that resulted in economic loss or personal injury to the patient.
  - *Damages for Negligent Disclosures:* Nominal damages of $1,000 per violation, and actual damages, if any, for any negligent disclosure of medical information.
- **California Invasion of Privacy Act ("CIPA")**
  - *Damages*: $5,000 per violation or three times actual damages, if any.
- **Electronic Communications Privacy Act ("ECPA")**
  - *Damages*: The greater of: (i) the sum of actual damages suffered by the individual and profits made by the violator as a result of the violation; or (ii) statutory damages of $100/day for each day of the violation or $10,000, whichever is greater, per person.

Washington and Nevada Consumer Health Privacy Laws

- Regulated Entities must **obtain consent** before **collecting** or **sharing** consumer health data except to extent necessary to provide the requested product or service.
- Regulated Entities must obtain **valid authorization** prior to selling or offering to sell consumer health data.
  - Such authorization must be **separate and distinct** from the consent to collect or share and include:
    - The specific consumer health data to be sold
    - Contact information for the person collecting, selling, and purchasing the data
    - The consumer's signature
    - A one-year expiration date

State Consumer Privacy Laws: Health Data Consent

	California	Virginia	Colorado	Connecticut	Utah
Consent Required	**Opt Out**	**Opt In**	**Opt In**	**Opt In**	**Opt Out**
Requirement	Businesses must provide option to limit the use of my personal information for purposes outside of the provision of the services. Note processing health data without the purpose of inferring characteristics about a consumer is not subject to an opt-out.	Controllers may not process sensitive data concerning a consumer without obtaining the consumer's consent	Controllers must obtain consent to process sensitive data, including sensitive data inferences.	Controller may not process sensitive data concerning a consumer without obtaining the consumer's consent.' Cannot sell, or offer to sell, consumer health data without first obtaining the consumer's consent.	Present notice and an opportunity to opt out of the processing of sensitive data
Definition of Consent / Notice Requirement	Businesses that use or disclose a consumer's sensitive personal information for purposes other than those authorized by the statute must provide a clear and conspicuous "Limit the use of my sensitive personal information" link on homepage. Note this link may be substituted for the "Your Privacy Choices" link (accompanied with the required opt-out CCPA icon).	"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.	Consent to process sensitive personal information means clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement, such as by a written statement, including by electronic means, or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.	"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" does not include (A) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (B) hovering over, muting, pausing or closing a given piece of content, or (C) agreement obtained through the use of dark patterns.	"Notice" of the collection the right to opt-out of the processing of sensitive personal information is not defined by the statute.

Risk Mitigation Strategies

- Obtaining opt-in cookie consent – Collecting consent before ad trackers collect consumer health information
- Providing just-in-time notice of collection to inform data subjects of data collection (particularly session recording, live chat or chatbots, health surveys)
- Implementing a cookie management tool
- Executing data protection agreements with service providers
- Obtaining acceptance of comprehensive Terms of Service
- Maintaining a transparent Privacy Notice/Consumer Health Privacy Notice

Speakers

Thora Johnson
Partner
Washington, DC
thora.johnson@orrick.com

Sundeep Kapur
Senior Associate
Washington, DC
skapur@orrick.com