The Sedona Conference WG11 Brainstorming Group Outline – Online Tracking (April 2024)

The Sedona Conference WG11 Brainstorming Group Outline – Online Tracking (April 2024)

Brainstorming Group Members:

Nichole Sterling (Brainstorming Group Leader)
Jenn Hatcher
Ron Hedges
Wayne Matus
Jamie Pizzirusso
Jeremiah Posedel
David Sella-Villa
Kate Baxter-Kauf (Steering Committee Liaison)

THE SEDONA CONFERENCE WORKING GROUP 11 BRAINSTORMING GROUP OUTLINE ONLINE TRACKING

I. Background and History

A. How did we get here?
   1. During the 21st century, consumer data has become the primary economic resource supporting the availability of free websites and digital services.[1]
   2. This processing of consumer data is increasingly at odds with the recent proliferation of privacy and data protection laws.
   3. A growing interest of consumer protection enforcement in online tracking paired with inconsistent caselaw regarding privacy harms.[2]

B. How are we defining (online) tracking?
   1. Common definitions[3] for online tracking typically include these elements:
      a) **Monitoring** or recording what individuals do online and on internet-connected devices;
      b) **Collecting** information about individuals' interactions with websites, apps, and other online services; and
      c) **Analyzing** the information collected or recorded.

C. What do people complain about? What is the behavior that we are concerned with? The collection of information, the monitoring of individuals, the analysis of the information, or something else?
   1. Profiling is often seen as a separate and/or subsequent step to online monitoring or tracking. The EU's General Data Protection Regulation (GDPR) defines "profiling" as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." The California Consumer Privacy Act (CCPA) adopts a similar definition as that used in the GDPR and excludes profiling from permitted business purposes, which otherwise arguably permit some types of consumer tracking.
   2. "Inference" is a term injected into many of the new U.S. state comprehensive privacy laws. Under the CCPA, for instance, an "inference" is "the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or

[1] See, for example, Tanya Kant, "Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your 'Ideal User,'" *MIT Case Studies in Social and Ethical Responsibilities of Computing (SERC) Series* (Summer 2021), available at https://mit-serc.pubpub.org/pub/identity-advertising-and-algorithmic-targeting/release/2?readingCollection.
[2] See, for example, Danielle Keats Citron and Daniel J. Solove, "Privacy Harms," *Boston University Law Review* (Vol. 102, 2022), available at https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[3] See, for example, the Federal Trade Commission, How Websites and Apps Collect and Use Your Information, available at https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information.

data." Like profiling, an inference is a subsequent or next step that can follow tracking.

a) Is there a reason to separate online tracking from other tracking? Generally, we believe that the technology used for tracking and the location of the tracking should not create a significant distinction, and all similar types of tracking should be addressed together.

b) For purposes of this outline, we make an assumption that the tracking of interest has some sort of a privacy, data protection, and/or cybersecurity impact.

D. What data is important for tracking?

1. IP addresses
2. Device identifiers
3. Advertising IDs
4. User agent strings
5. Geolocation data
6. Referrer data
7. Clickstream data and behavioral data

E. Is it fair to assume that if someone is tracking particular data elements that a specific person is also being tracked? What is the scope of "identifiable" when it involves defining data elements as personal data?

F. What kinds of trackers are being used?

1. Cookies[4]
2. Pixels[5]
3. Beacons
4. Geofences
5. GPS (using satellites signals)
6. Cellular triangulation, which uses a variety of sources
7. Sensors, "smart" devices, connected devices, and IoT
8. Facial recognition

G. The End of Third-Party Cookies

1. In response to privacy concerns, major tech companies are planning to phase out the use of third-party cookies. This is supposed to take place, for instance, on Google's Chrome browser in 2024. However, merely phasing out the use of third-party cookies, will not resolve online tracking concerns.

a) Users can still be tracked through first-party cookies and other activities on companies own domains, which may continue to amass data in the hands of a few large players. The end of third-

[4] See, for example, All About Cookies at https://allaboutcookies.org/.
[5] See, for example, Federal Trade Commission, Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking (March 16, 2023), available at https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

party cookies will tend to favor those companies with the most access to users and their data.

b) AdTech and data brokers are moving to alternative tracking technologies, such as device fingerprinting, probabilistic matching, and use of device identifiers that do not rely on cookies, but can still track – in particular, these can be more difficult to detect and block or avoid.

c) Reliance on multi-party data aggregation and third-party sharing, which can lead to extensive profiling and data retention (as well as challenges with complying with data deletion requests on demand).

2. Third-party cookies have some legitimate uses that may be lost, such as companies that rely on third-party cookies for security or anti-fraud purposes.

3. Technologies, including privacy enhancing technologies, are quickly evolving in this space, but many seem to solve primarily for the loss of tracking capabilities, just in a potentially more privacy forward manner. Data clean rooms, for example, and other developing tools like secure multi-party computation, may help to mitigate some privacy concerns.

II. Proposed Principles

A. What are we solving for?

B. Can principles help?

III. Principle One – Tracking should be fair.

A. What should be considered "fair" tracking?

1. Fair tracking is understandable, relevant (or purpose limited), reasonable, anticipated or expected, not discriminatory or biased, and not misleading or deceptive.
2. Fair tracking is time limited both in terms of data storage and the validity of any necessary consents.
3. Should the developing concept of "fairness" through FTC caselaw be the de facto standard? Is the FTC taking us in the wrong direction?
4. Fairness must balance both consumer and business needs.

B. The Privacy Paradox – Consumers want at least some benefits of tracking, such as personalization, but also want privacy and control of personal data. How should these be balanced?

1. What level of harm or damages to individual rights and freedoms is acceptable or unacceptable?
2. What level of harm or damages to businesses is acceptable or unacceptable?
3. How do you prevent bias or other unfair impacts without data?

C. Can we identify permissible (or "fair") uses of tracking, such as preventing ad fraud, detecting anomalies in website usage, and identifying bot (or other types of invalid) traffic?

D. What is the commercial value of tracking data? An online profile? An identity?[6] Should people be permitted to exchange their data for goods and services?
   1. Meta, for instance, floated a proposal, which European regulators recently addressed, to charge for ad-free services in the European Union.[7]

IV. Principle Two – Tracking must be transparent to consumers.

A. Does it matter if consumers know they are being tracked?
   1. In short, yes, but whether there is a legal obligation to tell them specifically depends on the law. For example, GDPR Recital 60 makes it clear that individuals "should be informed of the existence of profiling and the consequences of such profiling." Profiling is also explicitly included in the obligations related to automated decision-making in that law, which permit a right to object to the processing. Individuals may object to profiling related to direct marketing as well.
   2. Apart from legal obligations, tracking can make consumers feel uncomfortable and even violated – what we might call the "creepy factor" for lack of a better term. Consumers have reported being surprised by tracking that they were not made aware of, feeling that the tracking was excessively intrusive or personalization was so accurate it felt uncanny. Consumers have complained about feeling like ads were following them around the internet and about a general lack of transparency about or control over how their data was being used to track them. While clearly some tracking is accurately explained and used for legitimate purposes, users of tracking technologies should strive to avoid the creepy factor, which can be done through accurate and understandable explanations and offering real control to consumers over both their data and when tracking occurs. Consumer trust is critical in this space.

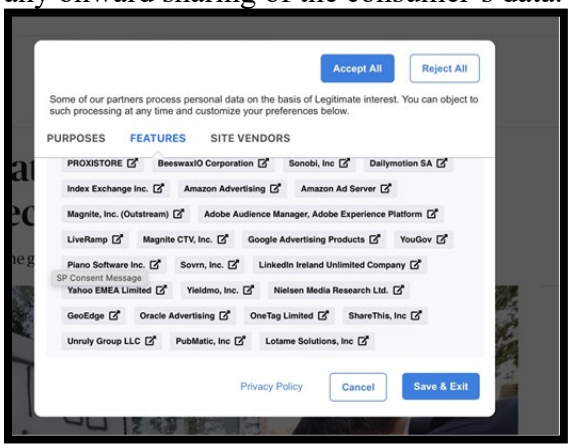
B. Does it matter who is tracking?
   1. First party – The consumer may have better visibility into the tracking and knows who he or she is interacting with.
      a) Walled gardens – Closed or restricted data environments belonging to a single entity that controls access to and use of the data. Examples include Apple, Amazon, Facebook, and X.
   2. Third party – More easily concealed and not always obvious to the consumer whose data is being tracked.

---

[6] See, for example, Mackeeper, "Most Desired Data. Whose is the most in demand, and how much is it worth?" (November 16, 2020), available at https://mackeeper.com/blog/most-desired-data/.
[7] See, for example, The Guardian, "Facebook and Instagram could charge for ad-free services in EU" (October 3, 2023), available at https://www.theguardian.com/technology/2023/oct/03/facebook-instagram-charge-ad-free-eu-meta-mobile-desktop. *Note that this draft was completed prior to the EDPB's published opinion of Meta's proposal.*

a) Data brokers – Under California law (1798.99.80), a data broker is "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship."

3. Any data sharing between parties should be disclosed specifically to the consumer, who should be able to have choice regarding that data sharing and any onward sharing of the consumer's data.



V. Principle Three – Consumers must be given real choice regarding tracking.

A. The relevant law may define the type of choice a consumer is provided – opt-in consent or the right to opt out. No matter the type of choice provided, that choice must be clearly and easily offered to the consumer and the choice needs to be effective.

1. Privacy obligations vary as to whether people must be provided with the right to opt in (or consent) to the tracking prior to the use of tracking technologies to collect personal data or whether tracking technologies may be used but people must have the right to opt out at any time.

a) Opt-in vs. opt-out regimes – illustrative examples:

(1) France under its implementation of the ePrivacy Directive and regulatory guidance requires opt-in consent to the storage of information on or retrieval of information from a user's equipment that is not strictly necessary.

(2) Canada's Anti-Spam Legislation (CASL) permits express and implied consent. Implied consent with an opt-out mechanism is typically acceptable for cookie use and online behavioral advertising.

(3) The CCPA does not require opt-in consent, instead requiring businesses to permit consumers to opt out of "sale" or "sharing" of personal information as those terms are broadly defined by the law and its implementing regulations.

b) Other considerations:

(1) Consumer choices may need renewal or updating and should not be presumed to be valid forever.

(2) The collection and use of sensitive personal data often requires consent even where other types of personal data may be collected and used without consent.
(3) The collection and use of the personal data of minors and other vulnerable populations can require special consent obligations.
(4) The transfer of personal data out of a particular jurisdiction can be subject to additional obligations, including consent obligations.

c) Can we combat consent fatigue?
(1) Cookie banners may be of limited use due to the prevalence of dark patterns as well as the impulse of most users to click through quickly.[8]
(2) Consent management technologies and vendors can have some inconsistencies and oddities, due in part to starting with a GDPR model that is less flexible than in many other jurisdictions.
(3) Most people today use multiple devices, browsers, and other technologies capable of tracking users. Can we manage to permit a user-level consent across all uses?

B. Consumers must be appropriately informed about their options and the consequences of their choices.
1. What is required to be appropriately informed?
a) Informed consents and adequate transparency. Most laws state that consents are not valid unless they are informed, specific, and freely given. A consumer's consent must not be ambiguous and should be recorded.[9]
b) Do consumers know what is being consented to? Generally, the answer seems to be that they do not.[10]
c) Is information provided to explain the advantages and potential harms of the proposed tracking?
d) How granular should the information be? What about the consent and making sure it is appropriately specific?

[8] See, for example, Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor, "'Okay, whatever': An Evaluation of Cookie Consent Interfaces," Proceeding of the 2022 CHI Conference on Human Factors in Computing Systems (April 2022), available at https://dl.acm.org/doi/abs/10.1145/3491102.3501985.
[9] See, for example, the European Data Protection Board's Guidelines 05/2020 on consent under Regulation 2016/679, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[10] See, for example, Report from the Annenberg School for Communication at the University of Pennsylvania, Americans Can't Consent to Companies' Use of Their Data (The Admit They Don't Understand It, Say They're Helpless to Control It, and Believe They're Harmed When Firms Use Their Data – Making What Companies Do Illegitimate) (February 2023), available at https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

e) Do users understand the extent of the consent (including how long the data will be processed and how it will be shared with or used by others)?

2. Take a connected car as an example, the car may be simultaneously using driver and passenger phone integrations, vehicle-specific apps, data from vehicle parts and systems, and other connected vehicle data. Can most users understand these data collections and flows, third-party uses, or potential risks and benefits of using the technologies to be able to make an informed decision regarding consent?

C. Is consent fundamentally worthless at this point? What about opt outs? If so, what could replace them? If consent, or the choice over one's own data collection and use, is not fundamentally worthless, would having a unified global standard solve many problems related to tracking? What about a global opt-in or opt-out standard that puts choice in the hands of the user rather than each business?

1. Consider whether to recommend temporal restrictions on the retention of data, to maintain compliance with, for example, the data minimization requirements under privacy laws.
2. The role of the new California Delete Act in this space.

VI. Principle Four – Sensitive data collected or inferred during tracking should be subject to heightened protections.

A. What should be considered sensitive data?

1. Is it the data type or the data use that is sensitive?[11]

B. Does it matter who and/or what is being tracked?[12]

1. Minors and other vulnerable populations.
2. Sensitive types of personal data, including:
   a) Browsing history and search queries containing sensitive personal data;
   b) Location tracking (precise vs. general);
   c) Inferences about demographic information and personal preferences;
   d) Health information;[13]
   e) Financial data and purchase history;

[11] See, for example, Federal Trade Commission's press releases regarding the data broker, X-Mode / Outlogic (https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-order-x-mode-successor-outlogic-prohibiting-it-sharing-or-selling-sensitive-location) and Cerebral (https://www.ftc.gov/news-events/news/press-releases/2024/04/proposed-ftc-order-will-prohibit-telehealth-firm-cerebral-using-or-disclosing-sensitive-data).

[12] For general background, see Pew Research Center, Key Findings about Americans and Data Privacy (October 18, 2023), available at https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

[13] See, for example, Federal Trade Commission's press releases regarding BetterHelp (https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising) and GoodRX (https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices).

f) Profiling;
g) Sensitive interactions or sensitive content consumption; and
h) Authentication information and biometrics.

3. Data elements that individually are not personal data but that collectively (or depending on use, including subsequent use) may be personal data (or even sensitive personal data).

VII. Principle Five – Tracking data should be used only for the relevant purpose(s) disclosed at the time of collection and not retained in an identifiable form for longer than strictly necessary.

A. Many laws permit data to be used for "compatible" purposes to those disclosed at the time of collection. However, the lack of definition for "compatible" may lead to excessive interpretation.

B. Businesses should consider when data is realistically no longer needed in its identifiable form and develop procedures for appropriately de-identifying data.

C. Inferences about third persons may be made from many types of data. Should these be considered relevant purposes, even if disclosed at the time of collection?

VIII. Principle Six – Universal technical standards for data collection, sharing, and use that could be controlled by consumers would benefit both consumers and businesses.

A. Consider the role of integration (for example, IAB consent string and browsers). Standards would need to be interoperable between companies and from companies to consumers.

B. Consider the need for a technology agnostic standard that would permit choices to be associated with a consumer across platforms and media (for example, on laptop, phone, and smart TV).

C. A universal standard would likely need to be both easy for consumers to use and functional across modalities.

IX. Principle Six – Not all data is equal. Neither is all tracking. Courts and regulators should carefully consider the allocation of liability and responsibility when regulating tracking.

A. Who bears/should bear responsibility and/or liability?

B. Enforcement and Regulation of Online Tracking Technologies
1. Regulatory enforcement of online tracking.

a) The roles of data protection authorities, state attorneys general, and other privacy regulators (such as the California Privacy Protection Agency and Federal Trade Commission (FTC)).[14]
b) The use of fines and other penalties, regulatory actions, regulatory inquiries and audits, compliance orders, data processing bans or limitations, and criminal penalties to enforce compliance.

2. Violations of privacy laws and the role of private players.
   a) Private rights of actions – most do not explicitly include tracking technology violations, but breaches affecting the collected data could fall under the private rights of action in, for example, U.S. state comprehensive privacy laws.
   b) Class/collective actions (for example, in the United States, United Kingdom, and the Netherlands[15]).
   c) Privacy advocacy groups (such as the American Civil Liberties Union,[16] noyb,[17] and Digital Rights Ireland).
   d) Does reputational harm play a role in maintaining compliance?
3. Online tracking can violate other laws and rights,[18] including:
   a) Constitutional rights under the Fourth and Fourteenth Amendments.
   b) Consumer protection laws – For example, tracking technologies and statements made about them can be false, deceptive, and/or unfair leading to enforcement by the FTC or under the state-level consumer protection laws. Consumer protection laws also tend to provide broader private rights of action than privacy laws.
   c) Wiretapping laws – Class action litigation in this space focuses on the used of session replay cookies and also chatbots used on websites. Both technologies may permit the recording of interactions with a website without obtaining consent from the user.[19]
   d) Video Privacy Protection Act (VPPA) – Recent class action litigation has looked to the VPPA to enforce against website publishers that share data with third parties, primarily Meta through its Meta Pixel. These litigations allege that the use of tracking technologies on webpages that display video relay

[14] See, for example, the Electronic Privacy Information Center's Enforcement of Privacy Laws, available at https://epic.org/issues/data-protection/enforcement-of-privacy-laws/. See also the California Attorney General's CCPA Enforcement Case Examples at https://oag.ca.gov/privacy/ccpa/enforcement.
[15] See, for example, Freshfields Bruckhaus Deringer, "A transforming landscape: Collective Actions in Data and Tech" (July 26, 2023), available at https://riskandcompliance.freshfields.com/post/102ikep/a-transforming-landscape-collective-actions-in-data-and-tech#page=1.
[16] See, for example, the ACLU's Privacy & Technology Court Cases, available at https://www.aclu.org/court-cases?issue=privacy-technology.
[17] See, for example, noyb, "226 complaints lodged against deceptive cookie banners" (August 9, 2022), available at https://noyb.eu/en/226-complaints-lodged-against-deceptive-cookie-banners.
[18] See, for example, ClassAction.org, Data Breach and Privacy Lawsuits, available at https://www.classaction.org/privacy-and-data-breach.
[19] See, for example, *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022) and *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022).

information about the users' video content viewed in violation of the VPPA. This information can be particularly invasive if the user is logged into one or more accounts that permit the information to be linked to other profile information. VPPA includes statutory damages of $2,500/violation.

e) Unfair competition and antitrust – The European Commission has looked into, for example, Google's anticompetitive conduct in the online advertising technology sector.[20]

f) Children's Online Privacy Protection Act – Limits how businesses can collect data about children under the age of 13 and includes parental consent obligations.

g) Illinois Biometric Privacy Act (BIPA) and other biometric laws.

h) Industry-specific laws and issues:

(1) Health care

(a) Health Insurance Portability and Accountability Act (HIPAA), Office for Civil Rights (OCR), and the Meta Pixel – OCR issued guidance that says "regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures."[21] Multiple lawsuits and enforcement actions have followed. In July 2023, the FTC and OCR jointly issued letters warning hospital systems and telehealth providers about the privacy and security risks from the use of online tracking technologies, including the Meta Pixel and Google Analytics.[22]

(b) Washington's My Health My Data and other health data related geofencing bans.[23]

(2) Tax preparation – In September 2023, the FTC warned five tax preparation companies that they could face civil penalties if they used or disclosed confidential consumer data for unrelated purposes, such as advertising, without obtaining consent first. The notices specifically called out the use of tracking technologies in this context.[24] This notice was immediately followed by a class

---

[20] See the European Commission's Press Release from 22 June 2021, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143.

[21] See U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (December 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. See also, The Markup, "Facebook Is Receiving Sensitive Medical Information from Hospital Websites" (June 16, 2022), available at https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[22] See https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

[23] For an overview, see Andreas Kaltsounis and Nichole Sterling, "4 New State Geofencing Bans and How They Differ" Law360 (August 4, 2023), available at https://admin.bakerlaw.com/wp-content/uploads/2023/08/Law360-4-New-State-Geofencing-Bans-And-How-They-Differ.pdf.

[24] See, for example, FTC Warns Tax Preparation Companies About Misuse of Consumer Data (September 18, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-warns-tax-preparation-companies-about-misuse-consumer-data.

action lawsuit filing against H&R Block alleging that it worked with Meta and Google to make money from scraping tax return data. This lawsuit was filed under the Racketeer Influenced and Corrupt Organizations Act (RICO), more commonly aimed at organized crime.[25]

(3) Connected cars – In July 2023, the California Privacy Protection Agency launched a plan to look into the data privacy practices of automakers regarding connected vehicles.[26]

C. Government regulation vs. regulation by private players, such as Apple's and Google's device ID tracking requirements. Have the private players developed better tools to enforce user privacy (although arguably for their own benefit)?

[25] The full complaint is available at https://www.wisnerbaum.com/documents/COMPLAINT-against-Alphabet-Inc.-Google-LLC-HR-Block-Inc.-Meta-Platforms-Inc-09-27-23.pdf.

[26] See California Privacy Protection Agency, CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies (July 31, 2023), available at https://cppa.ca.gov/announcements/2023/20230731.html.