Use https://tinyurl.com/tpac23-ffwfp if you're looking for the Fraud without Fingerprinting minutes.

Evolving anti-fingerprinting protections

Evolving Fingerprinting Protections Slides

Queue - add yourself at the bottom (include topic)

- Juan - to pontificate about market dynamics and legal accountability: coarse lists ossify into [unaccountable, abuse, monopolistic] credit bureau type actors if you're too slow on the declarative/fine-grain side or if the two never converge! lots of commenters referred to "arms races" or "cat-and-mouse" so i think an economic modeling of what incentives will do over 10 years might help :D
- QUEUE CLOSED

Attendees (sign yourself in):

1. Shubhie Panicker (Google Chrome)
2. Michael Ficarra (F5)
3. Brian May (dstillery)
4. Kaustubha Govind (Google Chrome)
5. Jean Luc Di Manno (Fime)
6. Philipp Pfeiffenberger (Google Chrome)
7. Tsuyoshi Horo (Google Chrome)
8. Vinod Panicker (Amazon Ads)
9. Johann Hofmann (Google Chrome)
10. Tim Huang (Mozilla)
11. Artur Janc (Google Security)
12. Paul Zühlcke (Mozilla)
13. Tony England(VISA)
14. Steven Valdez (Google Chrome)
15. Ane Fabo Aranzabal (google)
16. Zainab Rizvi (Google Chrome)
17. Benjamin VanderSloot (Mozilla)
18. Sam Macbeth (DuckDuckGo)
19. Ben Kelly (Google Chrome)
20. Ben Savage (Meta)
21. Mihai Cirlanaru (Google Android)
22. Joey Knightbrook (Snap)
23. Nick Doty (Center for Democracy & Technology)
24. Lee Wegener (Paypal)

25. Alex Koshelev (Meta)
26. Scott Hendrickson (Google)
27. Fabian Höring (Criteo)
28. Ben Wiser (Google Android)
29. Matthew Finkel (Apple)
30. Ari Chivukula (Google Chrome)
31. Kyra Seevers (Google Chrome)
32. Sam Weiler (W3C)
33. Sarah Nogueira (Criteo)
34. Elias Selman (Criteo)
35. John Wilander, Apple WebKit
36. Brianna Goldstein (Google Chrome)
37. Xiaohan Wang (Google Chrome)
38. Marek Blachut (HM Government)
39. Tara Whalen (Cloudflare)
40. Adam Rice (Google Chrome)
41. Sameer Tare (Mastercard)
42. Gerhard Oosthuizen (Entersekt)
43. Jonathan Kingston (DuckDuckGo)
44. Juan Caballero (Protocol Labs)
45. Nicola Tommasi (Google Chrome)

Minutes

I'm Shubie from Google. There's decent overlap in goals across browsers. We'd like a workshop after this. We want to understand the interest in this to see if there's enough participants to set up a workshop or another WG.

I have a couple of non-goals. We don't want to spend too much time discussing orthogonal privacy threats. Let's keep it focused on cross-site tracking. This discussion is not about use-cases that are disrupted by anti-tracking. I want to have people representing those but not in this forum, but this forum is not meant to discuss those use cases.

Last point is we don't want to spend too much time on user mediation.

With that I want to introduce this problem statement. I'm the eng lead on cross-site tracking. It's widespread and at large scale. The big idea is to increase the cost of tracking to reduce scale. Chrome is working on IP mitigations and more.

Feels like Browsers are largely aligned on anti-tracking. This act of joining user activity across websites. Users have a mental model of websites. Essentially Chrome is trying to prevent people from being recognized across these contexts. Chrome will impose limits with the objective of reducing cross site tracking.

Browsers are already using “tracker lists”. I’m aware of several browsers using “tracker lists”. Chrome is also heading in this general direction. We should acknowledge that it’ll take us time to evenly apply these across the board. Tracker lists are a *pragmatic first step*.

Focus of this discussion is on fingerprinting and tracker lists. Chrome is also developing anti-fingerprinting. This gives us common ground to start this discussion

How we define success? On one hand, we want to have features that users demand. On the other hand, we want to see industry behavior change away from fingerprinting and empower regulators

The status today is that all browsers have made significant progress in user features, but we're lacking on overall industry change and empowering regulators. Essentially, we're lacking a policy for the web.

Building blocks of tracking are: (a) cross site tracking threat; (b) data purpose, what is the intent for the collection of the data and © data practices, or how the collected data is handled.

From a user perspective, we have to consider user harm, user value or whether they consider there is a fair value exchange, and user consent.

John W (Apple): We don't view fingerprinting as a problem exclusively in a cross-site tracking context, we think that user recall is also critically important and should be considered in what we do here. For example, after clearing website data or moving between private browsing and normal browsing.
Shubhie: We would definitely like to include that topic.

Shubhie (presentation cont'd): creating tracker lists has significant judgment involved on all the dimensions we talked about earlier. Whether it's a 3P/1P context, data collection purposes and data practices as well as user considerations.

When addressing tracking/fingerprinting, we affect a large number of 3P use cases. I have a list of types of 3P tracker use cases that is semi-ordered. The list is semi-ordered because we see these categories as having diminishing returns in terms of the privacy gain. It will take a long time to address the long tail.

Tracker lists are a pragmatic way of starting to tackle this problem.

Sameer: What is acceptable declared data purpose here?

Shubhie: We don't have a standard on this yet. This is what I'm trying to make the case for here. We don't have an agreed upon standard, but we have tracker lists that are trying to make these judgment calls.

Sameer: I'm representing the payments pillar. We need to know that a user is on a genuine device

Shubhie: Today you have to work with

Brian: I'm curious on how you categorize these 3P use cases. For example, I don't know why ad targeting or ad measurement are things that need to be categorized as things to eliminate vs the the harms of unwanted tracking.

Shubhie: this is a representation of the current state of the world, not our opinion.

Ben (Meta): I have a question about a specific list in which Google parameters were not eliminated. Was there a mechanism by which this was done that would be accessible to others?

Shubhie: I don't have the information on this particular case. But what I'm arguing is precisely whether there should be a more standard/shared way of doing this.

(Presentation cont'd)
There are two types of declarations that tend to be accepted by tracker list companies to be excluded from their lists. Generally by including the appropriate disclosures in privacy policies or explicitly mentioning the data purpose and data retention period.

So, with tracker list companies making these judgments to build their lists and these lists being used by browsers in their anti-tracking features, we're already de facto applying some form of policy. Is there an opportunity to do this in a more standard way?

Gerhard: Certain standards, like 3DSecure take a long time to roll out, unfortunately those standards were built on fingerprinting principles and it will take time to change. Is there a way to use those as footholds to come up with standards that aren’t fingerprinting based? 4 years between versions of standards.

Shubhie: That makes sense and aligns with the point around the time scale, where we need to both find shorter term pragmatic solutions but also long-term better approaches.

Gerhard: our ability to clearly set the boundaries of what is good will really help.

Shubhie: Agree. Today there's a lot of confusion and lack of clarity by dev

Brian: One of the important aspects of the policy-side of things is that users are still engaged with whatever to do here. For example, having users being able to pick the tracker list that they want to use, or to tweak the list.

Shubhie: Thank you for that, that's a really good suggestion.

(Presentation cont'd) We're on the right path here using tracker lists, we're making tangible progress. But this approach has fundamental limitations, it is very easy to evade. We need a better long term approach that provides clarity to all 3P trackers and eventually 1Ps as well. This is only possible if we think beyond technical approaches. We need declarations or policy-based approach.

Lee: When we talk about policies, generally the policy is what we want to do and procedure is how. Are you saying that the policy is defining fingerprinting and the 3P tracker lists are the procedure?
Shubhie: Policy is a loaded word, we can use non-technical approach more generally.

Jon (Apple): Following up on Gerhard's question, I wonder if the timescale for adoption would be accelerated if the companies are not able to fingerprint anymore

Gerhard: Moving away from fingerprinting would be much easier if we could use existing constructs. E.g. you can still use an iframe, but do it in this way. Doing this in a way that asks for incremental changes that leverage existing mechanisms / frameworks, it will be easier to make progress faster.

Shubhie: It is also about juggling the different timescales of the different solutions.

Gerhard: Exactly. There needs to be clear understanding of what it is that we want, but then there's a middleground on how to make incremental strides that drive towards the newer longer-term spec.

Jon (Apple): Could the spec happen sooner than 4 years if we set the right incentives?

Shubhie: We need both, the carrot and stick

Gerhard: There's a process to this. It takes time to adopt and enforce. When you move to enforce directly, there will be friction. And we need to balance between speed and introducing this friction.

(Presentation cont'd)
Shubhie: What do we need at a minimum? Where do we take this beyond the current tracker list approach? We need to define: clearly establish the role of 1P vs. 3P and what is cross-site, data purposes, data practices that are ok or not and how to detect that, and also user considerations. Beyond some common definitions, each browser could have their own ability to define their

Another topic for discussion if there's interest is detection mechanism.

Fabian (Criteo): There's a fundamental issue with "block lists". A real bad actor will simply rotate their domains. Can we instead do allow lists?
Shubhie: This can be the long term approach. Block lists are practical way to start.
Fabian: Are blocklists even good in the short-term? Because the real bad actors will simply rotate.
Johann: It's not so easy to rotate because you have to get your domain out there.
Shubhie: It's a spectrum

Ben (Mozilla): If circumvention techniques become really common and we get into a cat and mouse game then defining what is cross-site or 3P/1P is important but contentious. A voluntary declaration will require a lot more policy infrastructure to enforce effectively.
Shubhie: Recognize that problem, but we ended there with our current strategy anyway.
Ben (Mozilla): a policy declaration will end up with a list that has all websites. It would be preferable to have technical solutions.

Shubhie: Agree that technical solutions are desirable when possible, but these aren't mutually exclusive from policy/non-technical mechanisms

(Presentation cont'd)
Developer declarations might be useful for browsers to implement protections, for regulators and also for developers. Ideally it would integrated in developer tooling, for example, we can hint to a website developer if they include a domain that is considered to be tracking by browsers.

Maybe this could fit into a bigger privacy label effort?

Sam: I'm interested in detection pipelines more than policy approaches. I'm wondering if we can make progress in detection.

Sameer: Offer for collaboration. Maybe we could have work streams per use case. For anti-fraud in particular, we have a specific set of data that we want to collect.

Brian: The intent of a blocklist is to prohibit the browser from accessing that domain or prohibiting that domain from accessing certain APIs?

Shubhie: This talk is about a number of fingerprinting protections, which might do one or the other.

Nick: Thanks for this talk. I'm willing to work on declarations work, particularly as circumvention might make protections less effective over time. Even as we should continue technical mitigations and reducing fingerprintability across the platform, also need some declaration and out-of-band enforcement, so that circumvention doesn’t undermine the technical protections. Volunteering to help with a workshop.

Gerard: +1 for declarations that can be used by a browser to provide some visibility or even friction, so that a declaration can be challenged/tested. This site indicates that it’s using fingerprinting to protect a payment – is that what the user is seeing?