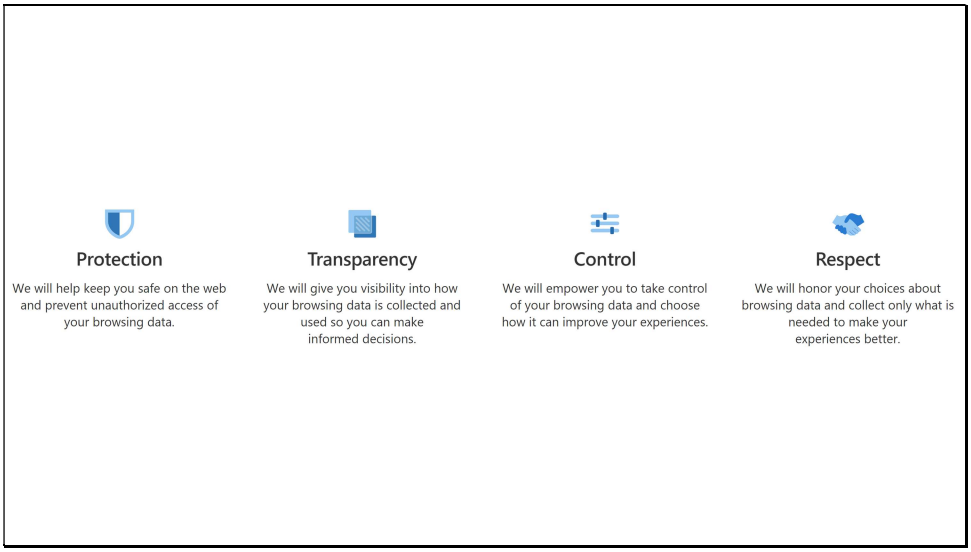
Slide 1

Hi everyone! I'm Scott Low, a PM on the Microsoft Edge HTML Platform team. Today, Melanie, one of my colleagues, and I are going to take you through a quick update of what our team has been up to in the privacy and trust space. We'll leave 10-15 minutes at the end for questions, so please feel free to ask anything that comes to mind then!

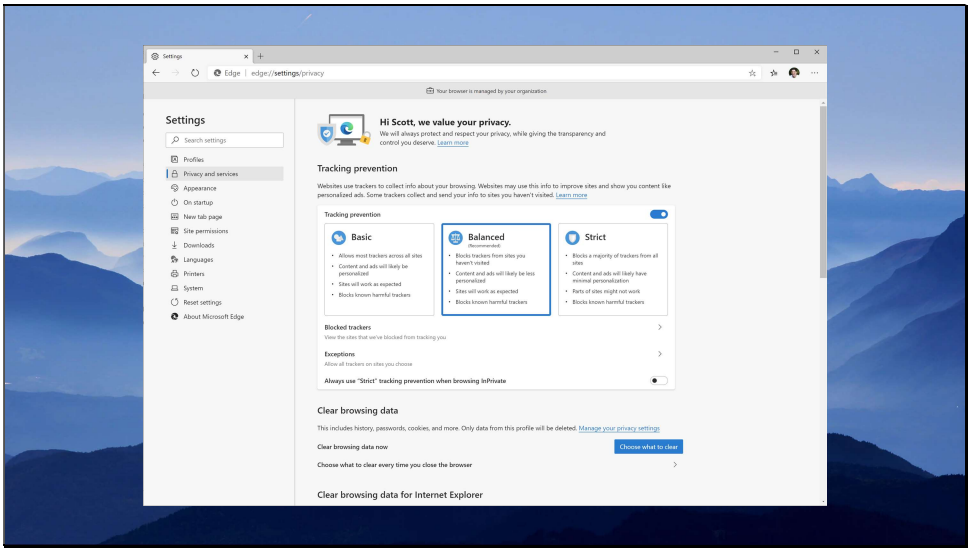
Slide 2



So before diving in, I wanted to start with a quick overview of our browser privacy promise that we published alongside our stable launch earlier this year. This is something that we developed based on listening to our users and the privacy-related problems they expressed and is the mantra we follow internally whenever we're working on new features.

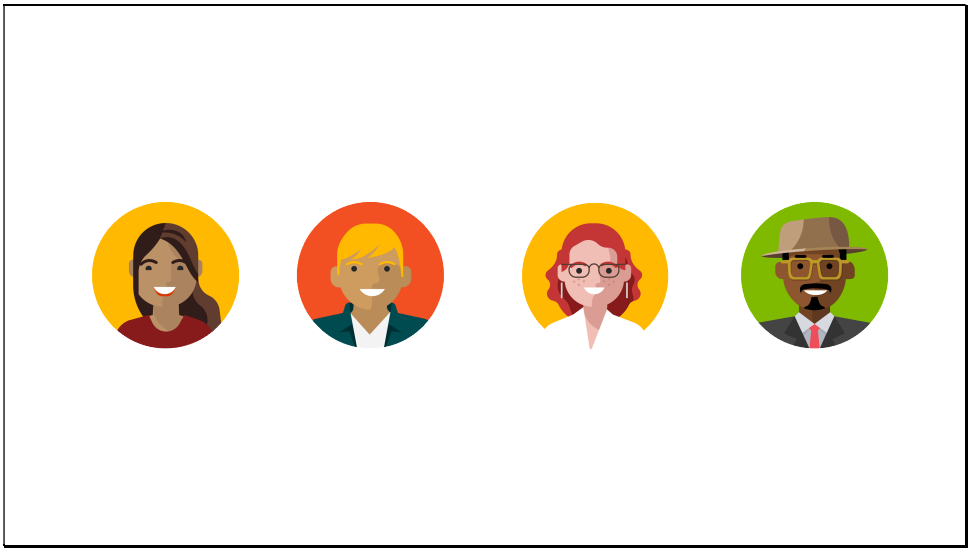
It's comprised of four pillars: protection, transparency, control and respect.

Slide 3



Our browser privacy promise is also what guided us to build and ship tracking prevention, a feature that by default protects users from being opaquely tracked online. Tracking prevention also balances compatibility by running client-side logic to determine the sites that a user has engaged with and ensuring that these sites continue to work as expected across the web. While we view tracking prevention as a good first start to meeting our browser privacy promise and our users' needs, we know that it's only the tip of the iceberg.

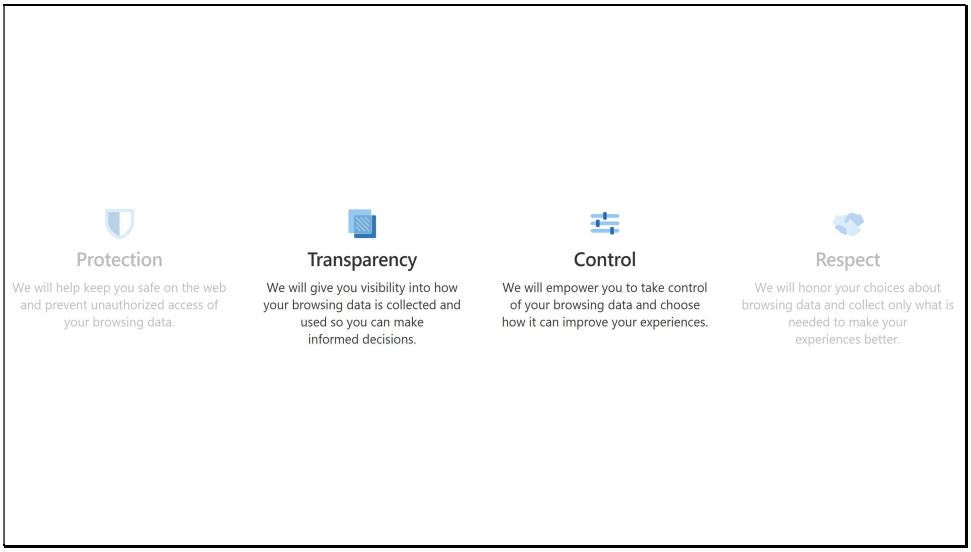
Slide 4



One thing that's super important to us is regularly engaging with customers to learn more about their unmet needs. From the numerous user studies we've run recently, we've heard a common theme. And that theme is that users generally understand that the web is free because of advertising. They also feel, however, that the value exchange between themselves and the companies who collect their data is lopsided; they want to be able to participate more equally in the data market that exists on the web today.

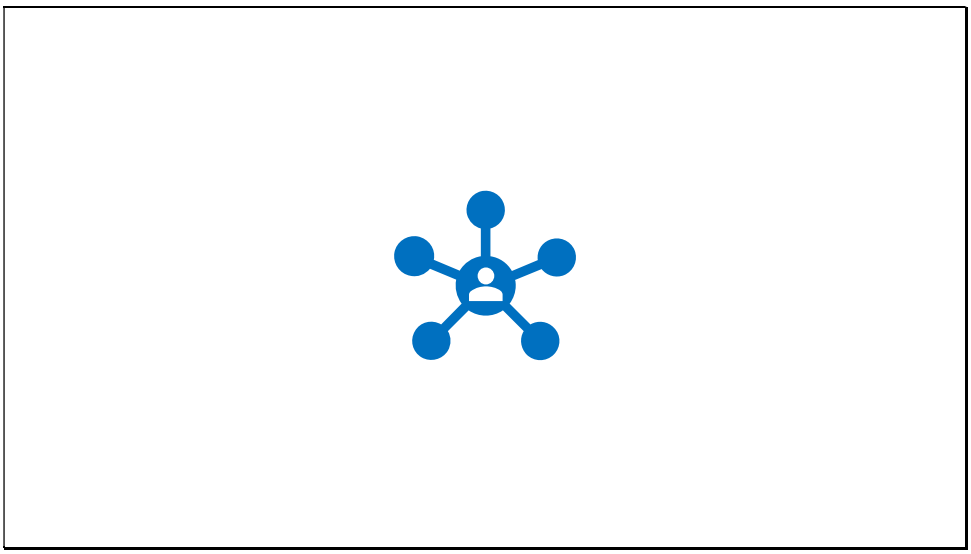
We also heard from most users that they felt like they have no transparency into or control over the data that is collected and shared while they browse.

Slide 5



The feedback on transparency and control was heard consistently across our surveys and interviews and has led us to double down on these pillars of our browser privacy promise.

Slide 6



To that end, we've been exploring ways that the complicated relationships between users and data consumers such as advertisers and publishers can be highlighted in a way that gives users more transparency and control.

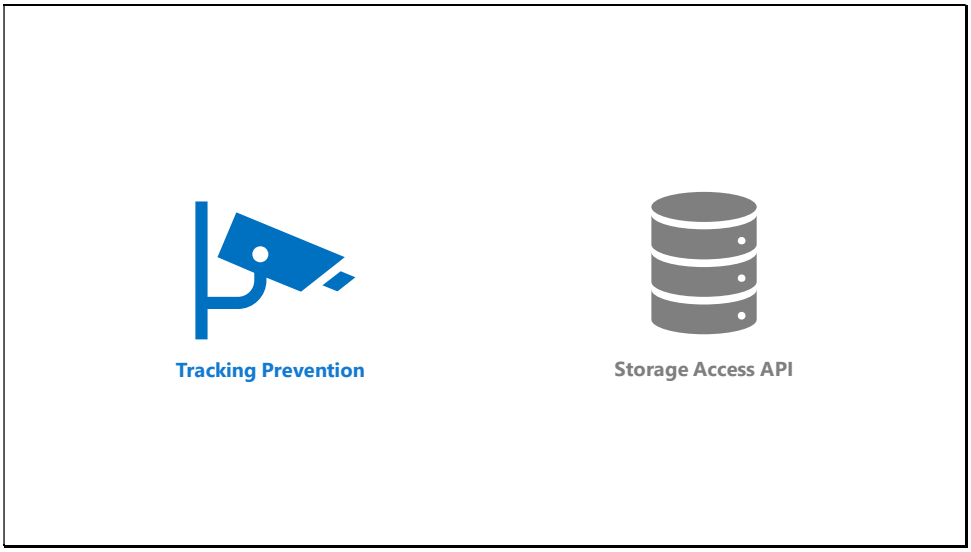
We envision the browser fulfilling its name as a user agent, acting on behalf users to give them a centralized dashboard where they can view their data and control what types of data are being shared and who they are being shared with. We've seen such concepts test well in user research and are hoping to have more to share in this space by the end of the month.

We're also running research on ways that we can give users value back for their data beyond just transparency and control. While we've seen the idea of free digital subscriptions and coupons test well with users, we are still early in our research and plan on continuing to work with users to see what other types of value back resonate well.

Slide 7

The notion of a browser-based privacy dashboard is still a long ways away, and there are several unknowns that will need to be solved for. In the interim, however, we want to continue to invest in browser features that meet our browser privacy promise and give users more transparency and control over how their data is shared on the web. To that end, I'd like to share a few investments we're making in the areas of Tracking Prevention and the Storage Access API

Slide 8



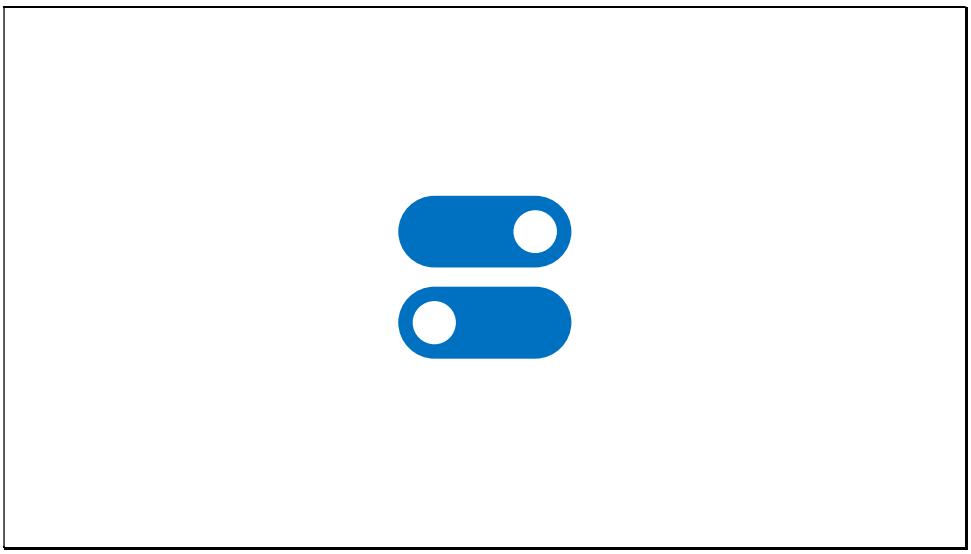
Today, our tracking prevention implementation uses a list-based classifier for identifying trackers. Based on our analysis of this list, however, it is largely north American focused, and likely underserves our customers in other parts of the world. As a result, we plan on experimenting with machine-learning models that we'll use in conjunction with our existing list to help increase our coverage. We'll share more in some upcoming blog posts, but it's worth mentioning that we're aware of the security concerns that have been raised with other ML-based classifiers and are working on ways to overcome them.

Slide 9

Another piece of feedback we've heard from many users of tracking prevention is that they want more insights into where they're being tracked and what trackers are being allowed by our feature.

We've taken this feedback into account and are exploring an improved view that will give users this information in an easy to consume way. It's worth mentioning that this is entirely powered using new client-side infrastructure we built to keep track of resources loaded on specific pages, so no information will be sent to Microsoft as part of this process.

Slide 10



We also heard that the option we provided to turn tracking prevention on and off for specific top-level sites wasn’t granular enough for our users; they instead wanted additional fine-grain control over which trackers are allowed and blocked.

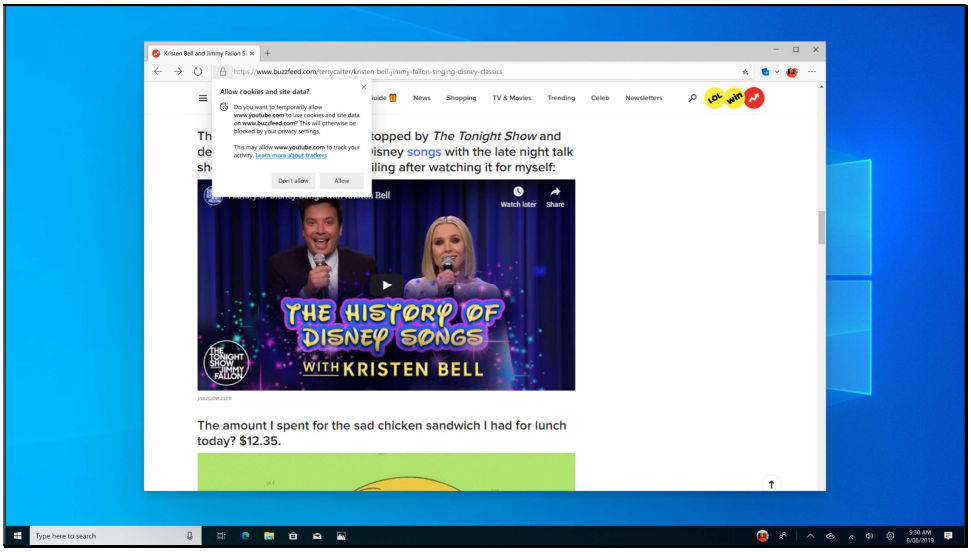
To address this, we’re also exploring ways of giving users more control in our UX flows, empowering them to allow/deny trackers on a per organization basis.

Slide 11

So that was a quick overview of some of the work we're exploring in the tracking prevention space. Before moving on, I do want to say that we're excited about the conversations that are occurring in the Privacy CG around the standardization of some tracking prevention mechanisms as we believe that standardized browser behavior will ultimately be better for compatibility.

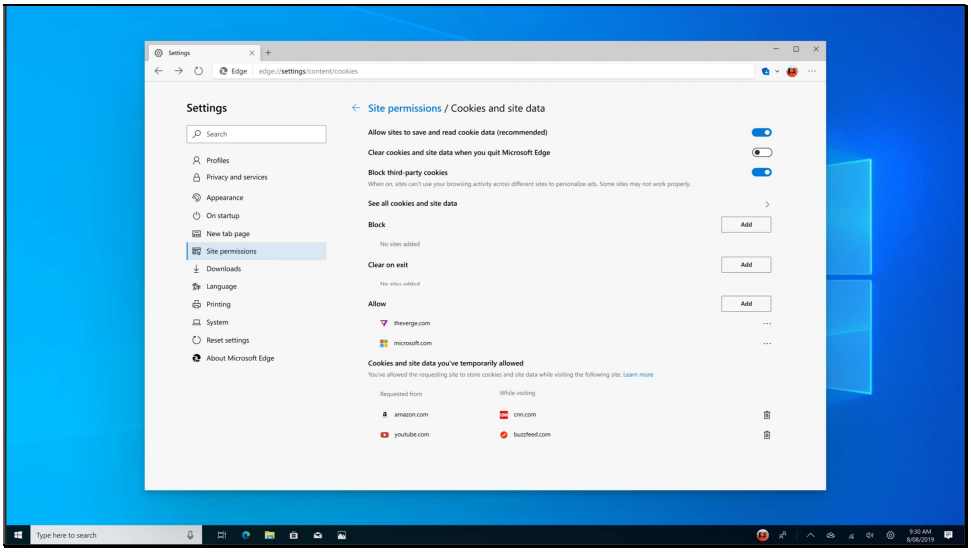
Another feature we've been working on upstream is the Storage Access API. This API is designed to give users the ability to more easily understand where they may be put at risk of tracking, and to help them balance the tradeoffs between tracking and compatibility accordingly. We're currently landing the last PRs upstream for this work and are aiming to start experimenting with it in Canary and Dev in Edge 84.

Slide 12



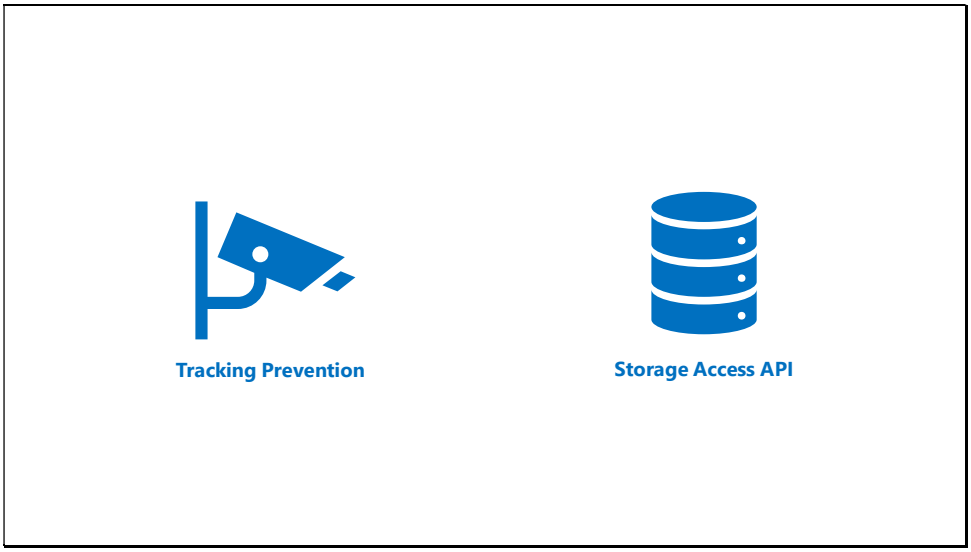
Here again, we ran user testing to lock on prompt text that was informative, yet simple. If anyone is interested in seeing the results of this research, please let me know and I'd be happy to share it!

Slide 13



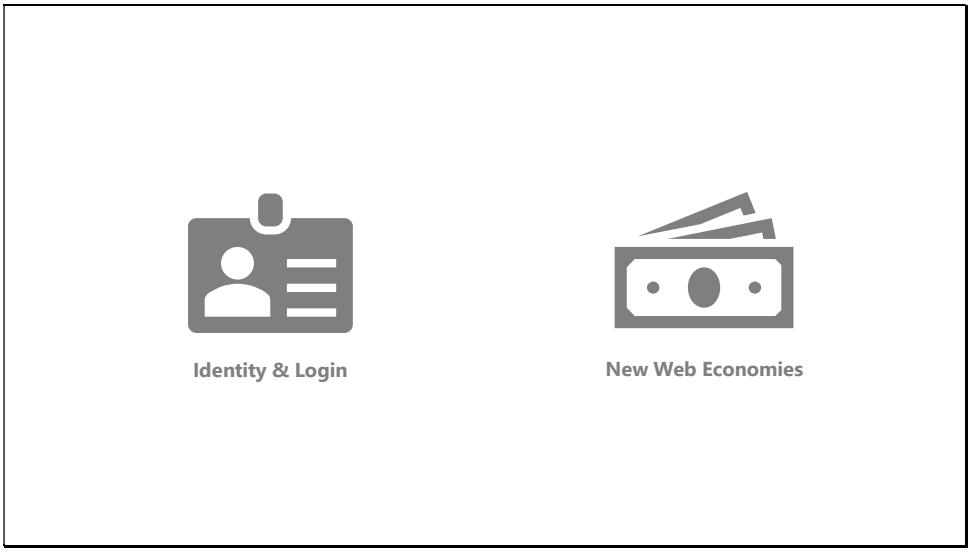
We also ran user testing on a settings UX to give users more transparency and control over the storage access grants they have allowed.

Slide 14



That was a quick update on some of the privacy improvements we've made and are planning to make. I'd like to hand this off to Melanie now to talk about Identity/Login and New Web Economics, two other areas we're interested in exploring.

Slide 15

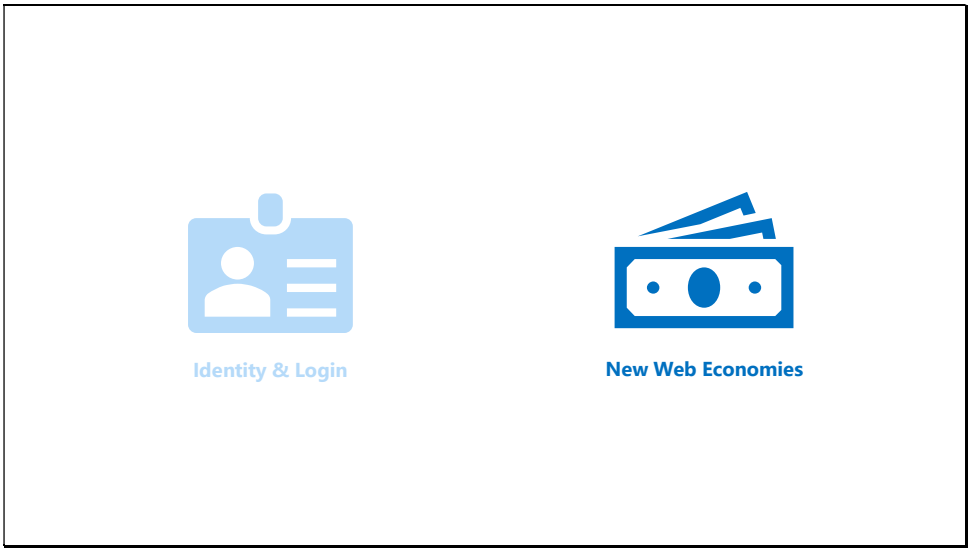


Scott covered a few of the investments we've been making into web privacy lately. I thought I'd touch very briefly on a couple of topics we're interested in exploring with the members of this group in the future: privacy-preserving Identity & Login, and New Web Economies.

Slide 16

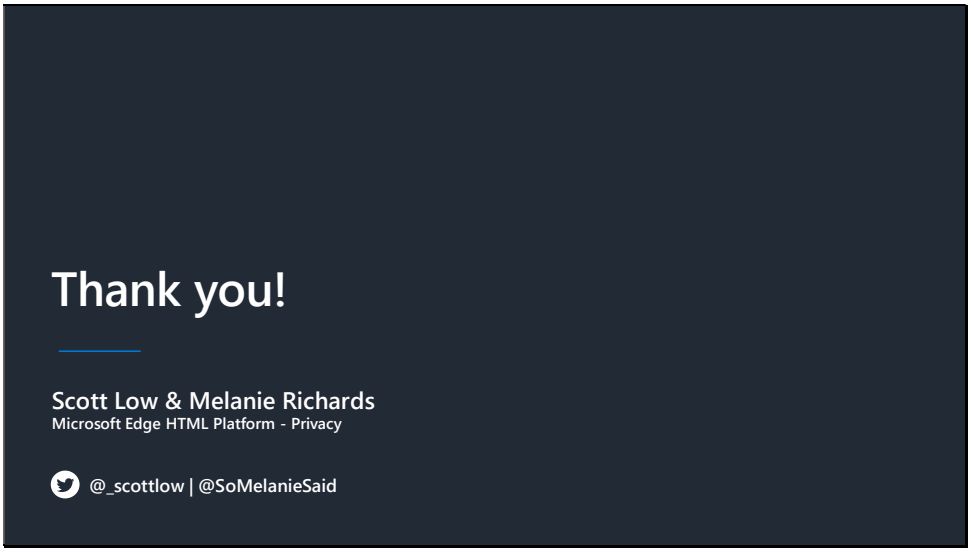
For Identity and Login: we know federated auth flows may become broken with some of the privacy features being proposed and built, so having the browser mediate the experience with the right privacy promises is an area we would like to explore further.

Slide 17



And in web economies, there are proposals in the W3C to move the current economic model to more privacy-preserving practices, and we expect to continue discussing these. But we also want to explore how we could potentially supplement this model with new web economies, that is, viable income streams for publishers, content creators, and consumers that align with user privacy expectations and require minimal-to-no data collection.

Slide 18



These are just two topics we're interested in, so speaking more broadly, we're looking forward to continued discussion in the CG on how we can collectively close privacy gaps on the web platform, and solve valid use cases in more privacy-preserving fashions. That's all from us today, looking forward to the rest of the F2F!