

Data in 4 Flavors, and the Demise of the Cookie

Opinions expressed by *Entrepreneur* contributors are their own.

You're reading Entrepreneur United States, an international franchise of Entrepreneur Media.

Scan the news recently and you'll find that digital privacy is a trending topic. The spotlight is on Big Tech companies like Facebook, Google, Amazon and Apple, and the ways they are changing their policies with respect to consumer data. What some are calling the "Privacy Renaissance" is upon us, and consumers are increasingly taking charge of what personal details are shared, and with whom.

Birth of the cookie

To better understand the shifting privacy landscape, it is best to explore the roots of online privacy, which reach back to 1994. That year, a young engineer named Lou Montulli was working at Netscape, the company that created the first web browser and which helped spark the global adoption of the Internet. Montulli was trying to solve a core problem of the web: that HTTP, the protocol that accepts requests and responds with web pages, was "stateless". This meant that a website wouldn't know that you were the same person as you navigated from one page to the next – a pretty big problem if one was trying to build an early ecommerce site. For example: there was no way to add an item to a shopping cart and have that item persist as visitors navigated to the next web page.

Enter the cookie. Montulli came up with a clever solution that

allowed state to be maintained atop a stateless protocol, calling it a “cookie” – a tiny text file associated with a specific web domain holding information about interactions, and stored on a web browser. This innovation allowed ecommerce to flourish... made it possible for websites to automatically log people in, and laid the groundwork for the ad-tech industry. In time, privacy concerns about cookies tracking people across the web led to a wave of governmental regulation (including GDPR and CCPA), and privacy features emerged around 2015 from popular web browsers like Chrome, Safari and Firefox.

It can be difficult for an average person to make sense of cookies and more importantly the different types of data (see below). Like any complex topic, it can be helpful to remove technical language and think about practical analogues.

Related: The Cookie Is Actually Crumbling in Advertising: Here's What to Know in B2B vs. B2C

Data in the real world

Say you decide to drop into Acme, Inc., a luxury retailer on 34th Street in Manhattan. You take a stroll through the store and see Truman, a customer associate you've gotten to know over the past few months. He helped you find just the right suit for your wedding, and also set up a wedding registry with some favorite items from the store – dinnerware, kitchenware, furniture, bedding, bath goods and more. That registry is a good example of zero-party data. You proactively shared your wish list and would expect that Truman recognizes you when you come back and has it ready and waiting.

Truman also doubles as a personal shopper and prides himself on getting to know your style, tastes and preferences. He knows you'd never wear pleated pants, colorful socks or stodgy neckties, and also that you are eager to know when the new fall collection arrives. Truman pencils these observations

about your behavior down in a black notebook for future reference. What you love about the guy is that he knows you so well, and makes your time at Acme both efficient and delightful. His black book is an example of first-party data. When you're inside the store, Truman is capturing the tastes that you have implicitly shared, and the way he leverages that knowledge to tailor your shopping experience is a big part of why you're such a loyal shopper there.

When you sign up for the Acme credit card, you may be engaging in a second-party data transaction. The financial services company that issued that card needs personal information to verify your creditworthiness to issue a line of credit (and a generous loyalty program signing bonus). You opted in to this card and understand why this is necessary.

Related: Transparency and Data: The Struggle for Brands in 2021

Unbeknownst to you, Truman has a weekly dinner called "Merchant Monday" with counterparts from other retailers. At this dinner, he exchanges notes about all his clients with other customer associates so they can tailor their own conversations. In return, the other associates share what they've learned with Truman in a quid pro quo. This is an example of a third-party data exchange.

Trust, and the future

For most consumers, zero-party and first-party data usage is benign – something that gives them a personalized experience they have come to expect, with a value exchange that feels transparent and equitable. But if the last scenario seems frightening to you, you are not alone. Third-party data has historically been collected and exchanged, primarily in the display ad ecosystem and in the private exchanges built by tech giants like Facebook and Google. All of this has drawn regulatory scrutiny, privacy legislation and web browser

privacy protection updates, and as a result, third-party data sharing is much harder to accomplish today.

Related: 10 Questions to Ask When Collecting Customer Data

While these might seem like somewhat abstract or legislative matters, these changes have direct ramifications to businesses of all sizes and across all industries, as companies grapple with adjusting their “top of funnel” customer acquisition strategies that relied heavily on the tracking that third-party cookies enabled. The good news is that there are alternatives, and savvy marketers are doubling down on collecting and activating their zero-party and first-party data, especially in owned channels like email and mobile. While the shift has posed short-term hurdles for marketers, ultimately the demise of the third-party cookie and other types of third-party data collection should have most people breathing a sigh of relief, and will do much to restore consumer trust in all forms of advertising.

<https://www.entrepreneur.com/article/392635>