Jie Li, EPAM

What If We Don't Accept the Cookies?

Every day, we open dozens of websites, each requiring us to navigate different cookie consents before we can proceed to view the content. In Europe, reading through these cookie consents is frustrating, because all we sometimes want is a single Reject All button. Instead, we often encounter websites that only offer Accept All and Manage Cookies options. When attempting to manage cookies, we are faced with an extensive menu with multiple tabs designed to make us miss something. In addition, there's often a long list of data-collector "partners," each claiming some "legitimate interest" in tracking us, requiring manual deselection for each. This cumbersome process often leads many of us to compromise by clicking Accept All, simply because it takes a lot of time to review the tabs one by one for every website. The younger generation often doesn't bother scrutinizing the consent details, and they tend to click Accept All to save time and effort.

YouGov [1] did research in 17 countries to understand what people do upon seeing cookie consents. Consumers in Poland, Spain, and the U.K. are most likely (more than 60 percent) to always accept all cookies; consumers in the U.S. are the least likely (32 percent) to accept all cookies. There are key differences by age in the U.S. as well—only 28 percent of older consumers (34 or older) say they accept all cookies. Adults under the age of 34 are especially likely to say they tend to accept all cookie permissions (40 percent).

Not many of us are aware of what might happen if we accept or reject cookies, leading to a lack of informed consent and potential privacy concerns.

IMAGE BY DMITRY KOVALCHUK / SHUTTERSTOCK.COM

WHAT ARE COOKIES?

The cookies I'm describing are not the sweet, buttery treats we enjoy with our coffee or tea. Instead, they are digital tools that facilitate more precise identification and tracking of user behavior. This, in turn, enables more personalized advertising and more effective advertising campaigns [2]. Most of us have experienced this: browsing an online store and noticing that the ads you see on other websites feature products you've recently viewed. This targeted advertising is made possible by cookies—small text files stored on your device that monitor your browsing activities.

To gain an edge over competitors, advertisers and trackers aggressively collect user information to form detailed profiles.

Today, behavioral advertising drives much of the Internet, and user data has become a valuable asset traded within a complex and often ad hoc data ecosystem. It is a loosely organized, often unregulated network where user data is opportunistically collected, shared, and traded by various entities without standardized practices or clear user consent [3]. To gain an

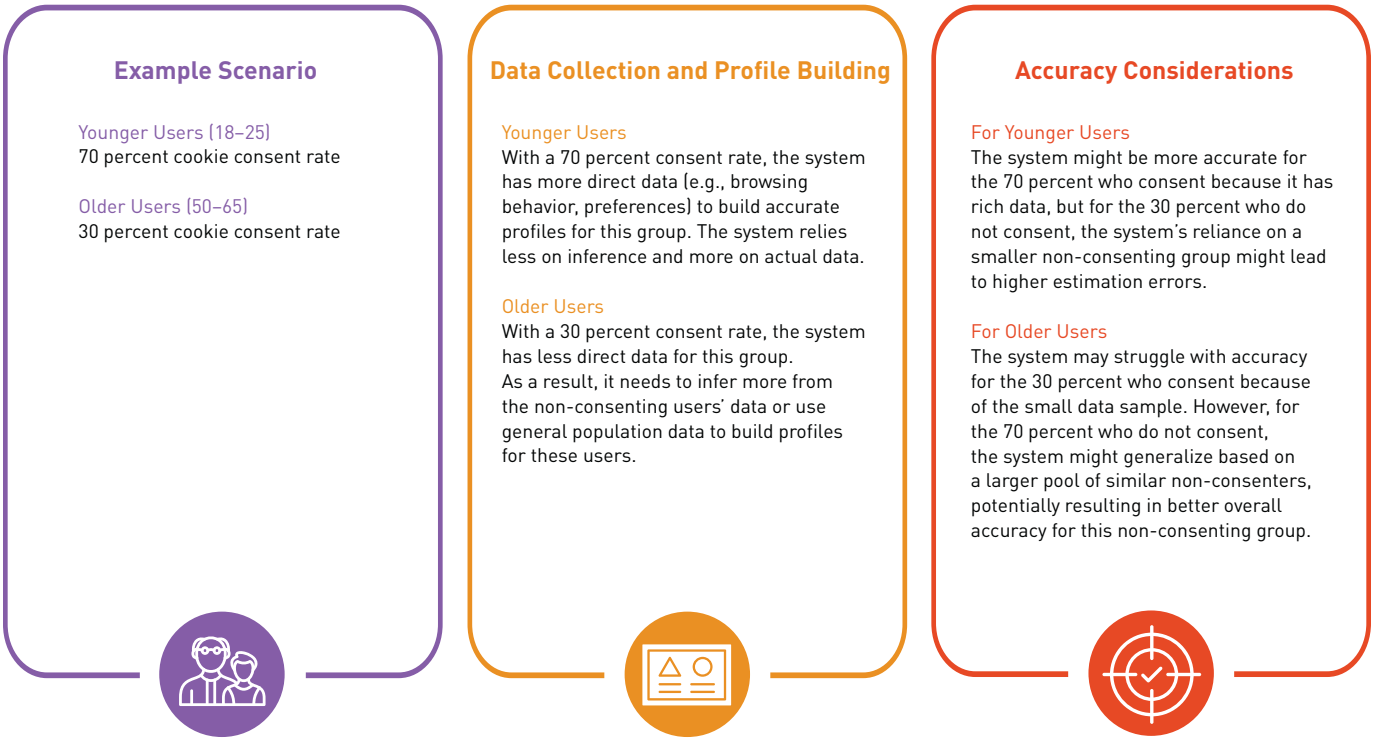

Figure 1. An example scenario is illustrated to explain why, in some cases, better accuracy of user profile estimations may be achieved for the majority of those who do not consent.

edge over competitors, advertisers and trackers aggressively collect user information to form detailed profiles that include interests, preferences, personal identifiers, and geolocations—data that can be sold to third parties for purposes beyond the user's control [2].

WHAT IS LIKELY TO HAPPEN IF WE ACCEPT ALL OR REJECT ALL COOKIES?

You may wonder what is likely to happen if you don't want the hassle of manually managing cookies and clicking Accept All every time. It is likely that your online activities will be extensively tracked by various websites and third-party advertisers. This can lead to the creation of detailed profiles about your interests, preferences, and behavior, which may be used to target you with personalized ads. Your data could be shared with or sold to other companies, potentially leading to privacy concerns, as you have less control over who has access to your information and how it is used. Over time, this can result in a significant reduction in your online privacy.

If you click Reject All, you may initially experience some inconvenience, as some websites rely on cookies to provide essential functions, such as keeping you logged in or remembering your preferences. You will likely see a decrease in personalized content and ads. Erik Miehling et al. [3] explore the effects of cookie consent decisions on the accuracy of user profile estimations in recommendation systems. The study reveals that demographic-dependent consent rates can lead to disparities in estimation accuracy. For example, lower cookie consent rates (e.g., 30 percent who consent and 70 percent who do not consent) mean the system has less direct data from those who consent and relies more on inferences to understand this demographic. As a result, the system is forced to generalize based on the larger group of people who did not consent, which may inadvertently result in better accuracy for the majority of those who do not consent. The example scenario shown in Figure 1 illustrates why, in some cases, better accuracy of user profile estimations may be achieved for the majority of people who do not consent.

Noa Leach [4] has pointed out that declining cookies could potentially be worse for your privacy than accepting them. In addition, algorithms may assume that users who often reject all cookies belong to the non-consent demographic and apply what is known as "collaborative filtering" to tailor content for them. This means the system observes what other users in this group search for and offers them similar content [3,4].

To enhance user empowerment, transparent frameworks must be proposed to offer concise legal explanations up front.

DARK PATTERNS AND COOKIE CONSENT REGULATIONS

There is an ongoing movement toward more consumer

empowerment online, a key objective of the General Data Protection Regulation (GDPR) that went into effect in the EU in 2018. The GDPR aims to give consumers greater control over their data online, thus enhancing their ability to protect their privacy [5].

We often see cookie consent banners without a Reject button on the first layer (Figure 2a). It is also common to see websites using high- and low-contrasting colors for buttons, where the Accept button is made more prominent. This includes the use of larger fonts and higher contrast for the Accept All option, drawing users' attention while minimizing their focus on other available options, such as rejecting cookies (Figure 2b). Some banners use misleading or manipulative language that makes users more likely to accept cookies without fully understanding what they are consenting to. This often involves positive framing (e.g., "We use cookies to enhance your experience"), which emphasizes the benefits while omitting important details, such as the use of cookies for targeted advertising (Figure 2c).

These banners make it difficult for users to reject cookies, violating their right to freely give consent, as users are not provided with an easy option to refuse [6]. In 2022, French regulator CNIL fined Google 150 million euros and Facebook 60 million euros for making it difficult and confusing for users to reject cookies [7]. Recently, in many EU countries an obvious Reject All button has started to appear on an increasing number of websites.

However, there are still websites bypassing GDPR consent to track users by using cookie synchronization, a method employed by third-party trackers and advertisers to share user data across domains, bypassing the same-origin policy [2]. Each tracker assigns a unique ID to a user, and cookie synchronization allows them to exchange these IDs with other third parties, unifying their knowledge of the user's browsing history across different websites.

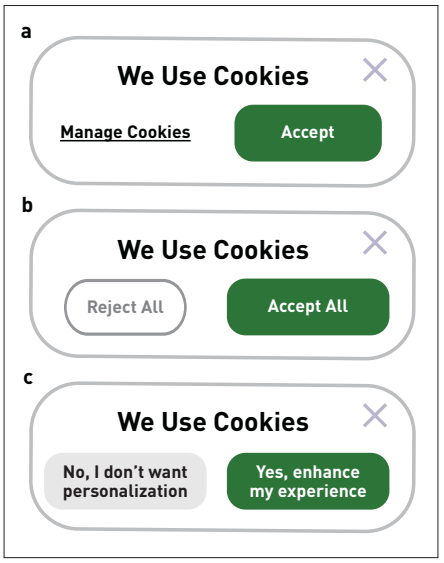

Figure 2. a) Cookie banner without a Reject button; b) cookie banner using a prominent color for the Accept All button; c) cookie banner using manipulative language that emphasizes the benefits of accepting cookies.

CONCLUSION

You may wonder what we can do to better protect our online privacy, as both accepting and rejecting cookies can lead to accurate profiling (as shown in Figure 1). Should we randomly alternate between acceptance and rejection to disrupt the algorithm? Or perhaps switch to a private browsing mode to prevent cookies from being stored between sessions, or adjust browser settings to block third-party cookies by default? With increasing "cookie consent fatigue," there's still no clear guidance on how to best protect our privacy.

Joanna Strycharz and colleagues [5] investigated how knowledge affects users' ability to reject cookies and found that legal knowledge significantly boosts users' motivation to reject cookies, whereas technical knowledge has a lesser impact. This highlights the importance of legal understanding in motivating users to protect their privacy online. To enhance user empowerment, transparent frameworks must be proposed to offer concise legal explanations up front, with detailed options accessible for further reading. Design improvements should include standardized Reject All buttons and clearer explanations of consequences for acceptance or rejection.

I hope you enjoy the sweet part of the cookie, but always be aware and empowered to remove the crumbs that don't serve you. After all, not all cookies are good for your digital diet.

ENDNOTES

1. Nguyen, H. Global: How consumers respond to cookies disclosures. YouGov, Aug. 13, 2021; https://business.yougov.com/content/37531-global-cookies-disclosures-behavior-survey
2. Papadopoulos, P., Kourtellis, N., and Markatos, E. Cookie synchronization: Everything you always wanted to know but were afraid to ask. *The World Wide Web Conference*, ACM, New York, 2019, 1432–42.
3. Miehling, E., Nair, R., Daly, E., Ramamurthy, K.N., and Redmond, R. Cookie consent has disparate impact on estimation accuracy. In *Advances in Neural Information Processing Systems 36*, A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, eds. Neural Information Processing Systems Foundation, 2023.
4. Leach, N. Why declining cookies could now be worse for your privacy than accepting. *BBC Science Focus Magazine*, Dec. 9, 2023; https://www.sciencefocus.com/news/declining-cookies-worse-for-privacy
5. Strycharz, J., Smit, E., Helberger, N., and Van Noort, G. No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior 120*, 2021, Article 106750.
6. Recital 43: Freely given consent. Intersoft Consulting, Apr. 27, 2016; https://gdpr-info.eu/recitals/no-43/
7. Vincent, J. France fines Google and Facebook for pushing tracking cookies on users with dark patterns. *The Verge*, Jan. 7, 2022; https://www.theverge.com/2022/1/7/22871719/france-fines-google-facebook-cookies-tracking-dark-patterns-eprivacy

Jie Li is an HCI researcher with a background in industrial design engineering. Her research focuses on developing evaluation metrics for immersive experiences. She is [redacted] a creative cake designer and the owner of Cake Researcher, a boutique café.
→ jasminejue@gmail.com

DOI: 10.1145/3702655