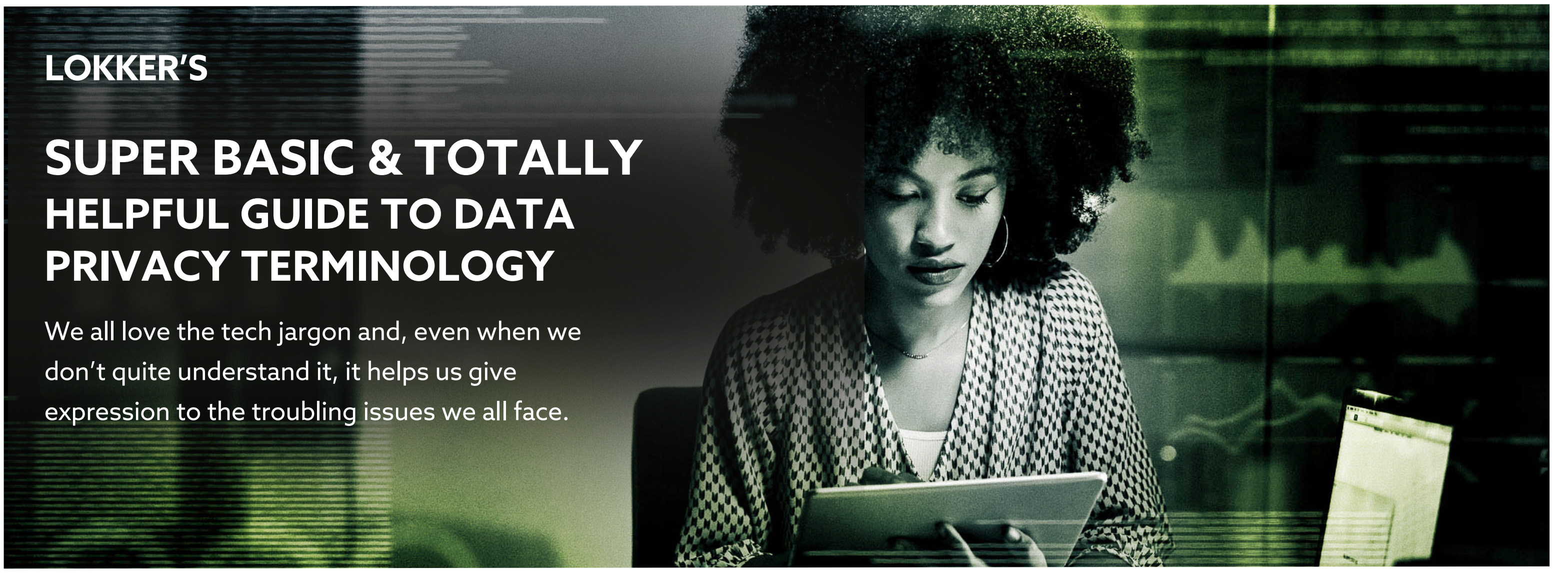
LOKKER
POWERING PRIVACY



LOKKER'S

SUPER BASIC & TOTALLY HELPFUL GUIDE TO DATA PRIVACY TERMINOLOGY

We all love the tech jargon and, even when we don't quite understand it, it helps us give expression to the troubling issues we all face.

To help us all better understand what we're dealing with this Data Privacy Week, we've decided to create a clear and simple explanation of the web privacy terminology we use, hear, and casually throw around with our colleagues and friends.

WHAT?	WHAT IS IT?	WHAT IT ISN'T	WHAT'S THE RISK?
Third Party	Someone (or an organization) who is not the owner of the website (1st party) nor the authorized visitor to the website (2nd party).	Where you want to be after the first party you went to had no snacks and the second party was only playing EDM.	If you don't know WHO is accessing your site's data or your customers' information, do you really want them on your site? Or perhaps you know your 3rd parties, but do you know with whom they are sharing information? (4th parties, and so on...)
Browser Cookie	The 'browser cookie' (or "HTTP cookie") is a bit of software code that is stored on your computer so that each time you use your web browser to access a site on the Internet, your activities are 'customized.'	Spyware that monitors all of your web browsing, purchases, emails, dating site activity, or investment decisions. Or is it??	If the websites you visit are placing cookies, or software, on your computer they could be harvesting a lot of personal information that, on the benign side, is used to target you with specific ads when browsing; on the malicious side, could be stealing your usernames and passwords that you use on secure sites, like your bank or your social media sites.
Scripts	Website software is often called 'website scripts' because they give instructions on what information to display and how to show it to the user.	What everyone in L.A. seems to have in their back pocket	While scripts, generally, provide core functionality for a website (a script to play a video in a specific format, or to remember what items I put in my online shopping cart), some scripts come from "third parties" (see above) and can also be used for sending personal information to organizations that you didn't authorize to use it.
JavaScript	JavaScript is a type of language for web software development and writing 'scripts' (above). JavaScript is also often used to create the 'cookie' (above).	Recipe for the perfect cortado.	As above, JavaScript can be employed to show core website features or used to write a script that invisibly sends credit card information entered on a web form to an organized crime syndicate in N. Korea.

WHAT?	WHAT IS IT?	WHAT IT ISN'T	WHAT'S THE RISK?
Fingerprinting	Software code used by the web browser to identify and often track online activities. The digital "fingerprint" contains unique elements of the computer, the web browser software, and your connection to the internet.	A biometric 'key' for accessing the restroom at Starbucks.	Fingerprinting enables clever cybercriminals to compile information about you without your knowledge. And, with enough experience, can combine bits of data to create a more accurate profile of you for future targeting of ads, offers, or attempts to steal your online usernames and passwords.
Ad Tracker	These trackers are small bits of code placed on a webpage as hidden JavaScript or links (usually by third parties) to help advertisers monitor advertising activity.	A GPS locator for Don Draper.	When advertisers want to measure the effectiveness of their online advertisements, they employ a method called 'ad tracking' to report on how often an ad was presented, if it was clicked, and if the ad led to a purchase. Depending on the source of the ad tracker, the host site could be in a foreign country, could be capturing more information about user activity, and data could be shared with organizations that the advertiser never intended.
Foreign Domain	If the domain or website address you are visiting is based in "Country A," a foreign domain would be some content or script on that website domain that is coming from another country that is not "Country A."	A winemaker from an area outside of Bordeaux.	Website content or code that is hosted on a server in another country can indicate risk. Cybercriminals from outside of the US, for example, often attempt to inject malware (malicious software) from their home country. In addition, if data entered on a website form is being sent to a foreign country, it may also indicate a data breach or breach of privacy policies.
SSL Certificate	The "Secure Sockets Layer" certificate is an indication of a site's authenticity as well as certification of secure data transfer when using the site.	Authority to teach "Swedish as a Second Language."	If a secure, 'SSL certified' site is collecting information and sending it to an external domain or web address (URL) that is not SSL Certified, it indicates a risk of unprotected data sharing and perhaps unauthorized data sharing.
Young Domain	A website or URL of a domain that has been registered less than 1 year ago is considered 'new' or 'young.'	A rapper from Atlanta.	If data is being shared with or getting content from a web domain that was only recently registered, this may indicate an attempt from a hacker who has recently established a web domain in an attempt to hijack users or intercept data.
DLP	Data Loss Prevention is a broad term in cybersecurity and privacy that refers to methods a website owner can take to keep private information safe, specifically from being sent to unauthorized third parties	A Domestic Lite Pilsner, the lower calorie alternative to the more robust IPA.	If a data form on a website is compromised by malicious JavaScript, the data a user enters on that page could 'leak' to an unauthorized third party. If the data includes usernames, passwords, or personally identifiable information (PII), the loss could trigger significant data breach protocols and violate the host's data privacy policy.