Partnerize

Everything you need to know about privacy in partnerships.

Over the past 18 months, the world has experienced a surge in digital dependence. These shifts in behavior continue to unfold with a growing reliance on ecommerce (digital sales are expected to reach $906B this year), increased adoption of social media (13% increase in users globally) and a 57% majority vote for "watching tv and movies at home" as a top-three entertainment source.

As consumer favoritism of digital experiences continues to grow, marketers are shouldering the responsibility of achieving omnipresence, battling the rising cost of customer acquisition and delivering a cohesive user experience across the buyer journey—touchpoint consistency demanded by modern consumers. And these consumer demands have evolved to include expectations for how brands handle their personal information.

With an ever-growing list of logins, social media platforms, apps and streaming services, etc., it's natural that consumers are becoming more skeptical of the methods and locations brands leverage to store their personal information. Consumers want to know if brands are taking the appropriate steps to protect that data, and what actions they themselves should take to ensure their personal information isn't at risk.

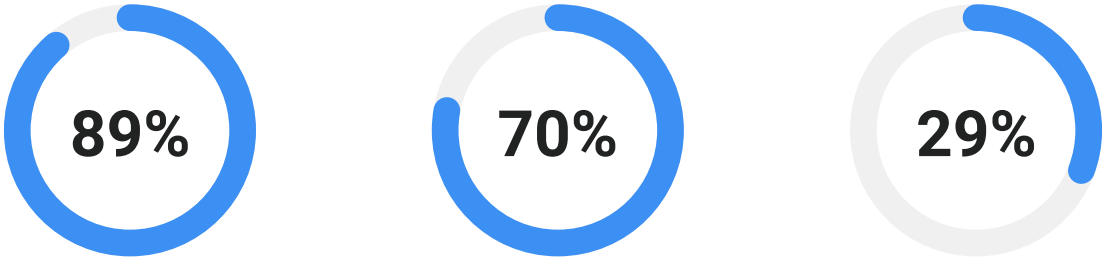
Consumers' expectation: Data privacy

Today's consumers expect data privacy, or the ability to decide for themselves how their personal information is collected, stored, used, and communicated to others. While there is no single set of guidelines for the appropriate handling of personal, confidential or financial information, recent laws and regulations throughout the world have attempted to define what steps businesses must take to respect the privacy of the individuals whose information they obtain.

Important to note: data privacy is not the same as data security. While data privacy relates to how information is collected or used, data security involves the protection of information to prevent loss, misuse, or unauthorized access. Brands must educate themselves on the differences as a first step to ensuring compliance, as 89% of surveyed consumers want more control over their data, with 70% citing data privacy as a buying factor.

Priorities and actions protecting their privacy according to consumers worldwide, June 2020

% of respondents



I care
I care about data privacy.
I care about protecting others.
I want more control.

I'm willing to act
I am willing to spend time and money to protect data.
This is a buying factor for me
I expect to pay more.

I've acted
I have switched companies or providers over their data policies or data sharing practices.

Source: Cisco, "2020 Consumer Privacy Survey"; Insider Intelligence calculations Oct 21, 2020

Privacy protection enhancements

In response to consumer privacy concerns, there's been a range of global changes that protect consumers and ensure an optimal digital experience. The central philosophy of the regulations ensure that personal data belongs to the person, not a company. Recent privacy changes include:

IDFA

An acronym for "Identifier for Advertisers", IDFA is the unique identifier for mobile devices that is used to target and measure the effectiveness of user-level ads across phones and tablets. The IDFA is used by some solutions to measure success of ad campaigns as well as provide hyper-personalized ads to individual users. In early 2021, Apple released an opt-in for individual apps requiring consent from consumers in order for apps to track mobile device activity. More than 60% of users reported that they will not permit apps to track them following IDFA notifications.

Browser Changes

ITP

Intelligent Tracking Prevention (ITP) is a feature that Apple added to Safari browsers in 2017 to curtail companies' ability to monitor user behavior via cookies. ITP and its following iterations were released to improve privacy for Safari users by preventing cross-site tracking, the default setting for all impacted browser versions. As a result, ITP effectively disables third-party cookies for domains that use data for tracking user activity.

Total Cookie Protection

A Firefox update that partitions cookies to each website the consumer visits, isolating tracking cookies to the individual site on which they were created and preventing tracking (including performance marketing tracking) from tracking consumers' browsing activity across the web.

Chrome's cookie phase out

Seeking to develop new web technologies that can both protect privacy and allow the growth of digital businesses, Google launched its Privacy Sandbox initiative in 2019. As part of this initiative, Google announced that it is working to phase out all third-party cookies in its Chrome browser by 2023.

GDPR

The General Data Protection Regulation (GDPR) is a legal framework out of the European Union (EU) regulating the collection and processing of personal information for individuals in the EU. The GDPR was created to replace the EU Data Privacy Protection Direction (1995) and aimed to take data privacy protection into the digital age. The GDPR definition of personal data is considerably broader than some previous definitions, including not only direct identifiers but also indirect identifiers, or information that does not identify a person in isolation but can do so when combined with other information. After Brexit, the United Kingdom also continues to operate under its own version of the GDPR (the "UK GDPR"). Taking steps to comply with GDPR—which affects everyone, in or out of the EU—is critical. **Here's why:**

01

If you're in the business of designing products or services (even features) that harvest consumers' personal data (think mobile apps), you need to put consumer data privacy at the forefront at the very start.

02

Data privacy is the new default and it will be the consumer's choice whether they wish to turn privacy off within these apps.

03

Data breaches must be reported significantly faster. In fact, GDPR requires many data breaches to be reported to the proper authority within 72 hours.

04

The consumer has the "right" to take their data with them, should they switch to another provider of service—a practice known as "data portability". Consumers can also simply request that data be erased, provided certain criteria for erasure is met.

If you're in the business of designing products or services (even features) that harvest consumers' personal data (think mobile apps), you need to put consumer data privacy at the forefront at the very start.

Data breaches must be reported significantly faster. In fact, GDPR requires many data breaches to be reported to the proper authority within 72 hours.

Data privacy is the new default and it will be the consumer's choice whether they wish to turn privacy off within these apps.

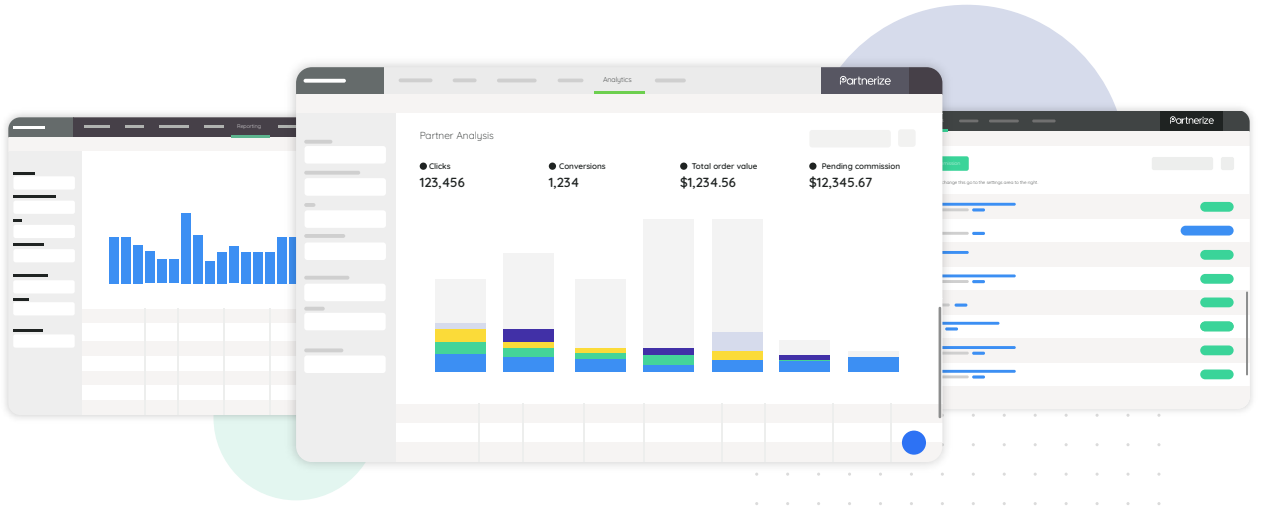
The consumer has the "right" to take their data with them, should they switch to another provider of service—a practice known as "data portability". Consumers can also simply request that data be erased, provided certain criteria for erasure is met.

CCPA

The California Consumer Privacy Act (CCPA) provides California residents with control over the personal information that businesses collect about them, and arms them with the rights to:

- Know the personal details that are being collected
- Delete personal information that is collected
- Opt out of the sale or dissemination of their personal information
- Non-discrimination for exercising their CCPA rights

For marketers, ensuring compliance with these changes is critical not only to adhere to the applicable law, but also to ensure persistent performance program tracking.



The marketer's challenge: Optimizing amidst privacy protection updates

While these privacy measures provide consumers with the protection they deserve, they also pose challenges for some of the traditional tracking found in performance marketing campaigns. These tracking inconsistencies and data limitations precipitated by privacy changes impact the way that partnerships are managed and bring about restrictions for brands seeking to provide a customized experience at a time when it's demanded by the same consumers these rules protect.

Many marketers are also not aware of how the changes impact their partner programs. In fact, the IAB UK Buyside Survey uncovered that more than half of surveyed marketers indicated third-party cookies as the number one most relied on mechanism for tracking. Another 21% of affiliate marketers didn't know their tracking method. Without consistent tracking amidst ever-changing privacy regulations, it's impossible for marketers to drive profitable growth.

Key takeaways

Get educated.
Whether you're in the know about evolving privacy regulations or learning about them for the first time, one thing is for certain: they are constantly changing. Marketers must stay up to date on how they should protect the privacy of their consumers and be clear on the necessary steps to remain compliant.

Talk to providers across your tech stack.
Even if your business is not maintaining user data, don't overlook your partners. Talk to your vendors and integrated partners to ensure that they are also in compliance with applicable data protection law.

Know your performance marketing tracking type.
If you're one of the 21% of marketers that don't know your tracking type, dig into your infrastructure to ensure that your marketing programs are futureproofed and set up for success.

Involve your tech team.
Keep your tech team in the loop to help weigh the best tracking solutions for your business. They'll be a key component in making sure that your tracking is consistent and providing clear, accurate data that powers equitable rewards to your partners.

Leverage solutions across the technology ecosystem.
Integrate with providers that specialize in supporting mobile and in-app events, dynamic personalization and regulated retargeting. These solutions will ensure that you maintain accurate tracking regardless of device type and can provide the personalized experience demanded by consumers regardless of data limitations. It's important to note that not all MMPs track across mobile devices with IDFA changes and associated opt-outs, so be sure to confirm with your providers that persistent tracking is in place.

Fulfill transparency requirements.
Brands are required to notify users if they collect cookies. Comply with this regulation and put consumers' minds at ease by implementing a pop up or notification on your site alerting them to cookies or other collected information.

For more information on how Partnerize powers marketers to drive profitable growth amidst evolving privacy regulations, get in touch at contact@partnerize.com.