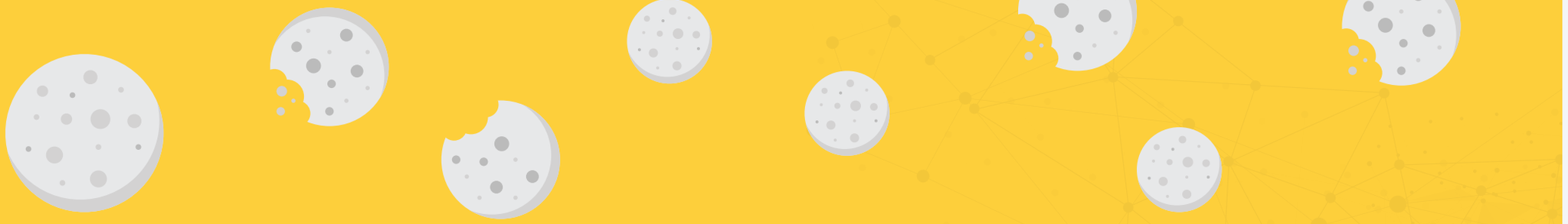
What Every Company **Should Know About Cookies**

What They Are?

Why Your Website Needs Them?

How to Avoid Legal Exposure?



Introduction

Today, nearly all companies' websites rely on cookies, and it's not hard to see why. These relatively simple tools enable your site to collect specific information about its visitors in order to offer them a more personalized experience, while providing you with valuable insights.

Because of their efficiency and usefulness, cookies are used frequently both by companies looking to optimize their websites' functionality and by third parties looking to create customer profiles for targeted marketing. But while cookies can be profitable for businesses and beneficial for consumers, they can also create privacy risks.

As a result, they have been targeted by recent legislation such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Specifically, there are increasingly strict requirements for companies to get an individual's consent before setting cookies on that individual's computer, smartphone, or other digital device. While these regulations may benefit consumers, they can create serious challenges and legal exposure among businesses.

To avoid legal risk, many companies are turning to digital technology designed to facilitate their compliance with relevant laws. Consent management platforms (CMPs) are one particularly popular type of solution helping companies avoid potentially costly infractions. But while a CMP may reliably ensure that a website will only set cookies with a user's consent, these platforms only offer limited visibility into the activities of third- and fourth-party services running on the website. As a result, a CMP alone cannot always detect when a third party discreetly uses cookies in ways that the user has not approved.

To help you ensure that your business complies with relevant laws, this eBook will explain:

- **What cookies are and how they work.**
- **What the various types of cookies are and how they differ.**
- **Why cookies are so popular and how they benefit both website owners and visitors.**
- **Why some cookies create privacy concerns for consumers.**
- **How recent laws have restricted the use of cookies.**
- **How to protect your company from legal risks, and how digital solutions can help.**

Table of Contents

CHAPTER 1

What Are Cookies?

A cookie is a small piece of textual data placed on a user's hard drive by a website that the user visits. Based on the website's instructions, some of the data stored in the cookie (specifically, the cookie's name and value) will be sent back to that site at certain points. This way, the website can recognize specific information about the user in order to offer a more personalized and user-friendly experience.

But to really understand how cookies work and what they accomplish, first it is important to understand why there is a need for cookies in the first place. A wide variety of websites need a way to keep track of visitors' personal details in order to achieve their basic goals. For example, eCommerce websites need a way to allow a user to fill a shopping cart, social media sites need a way to remember whether a user has logged in, and freemium online newspapers need a way to count the number of articles a user has viewed.

But websites do not have a built-in mechanism for storing these kinds of personal information. While some sites rely on server-side databases that can include detailed information about specific users, even these databases need a way to identify an individual user in the first place. Cookies were developed in the 1990s as **a way of enabling websites to store important details about each user** without relying exclusively on server-side storage.

Today, they are used nearly universally on major websites, and **it is common for a single website to use dozens or hundreds of cookies.**

What Is the Difference Between First-Party and Third Party Cookies?

From the user's perspective, perhaps the most important distinction is between first-party and third-party cookies.

Historically, the first cookies to be used were first-party cookies. The idea was pretty simple: When a user visited a website, the website would set a cookie to be saved on the user's hard drive that would allow the site owner to keep track of a user's activity s they moved from page to page on the in the domain. By default, first-party cookies are allowed in every web browser.

However, as websites started to incorporate more third-party services, it became more common for these services to place their own cookies on users' hard drives. In some cases, these embedded services would only set cookies that were really designed to enhance the user experience. In other cases, a single service embedded into a wide variety of websites—for example, a series of online ads—would place cookies via many different sites. Then, these services would use cookies to track individuals' browsing behaviors, build customer profiles, and use these profiles to drive behavioral advertising.

First-Party Cookies	Third-Party Cookies
Can be set by the publisher's web server or any JavaScript loaded on the website.	Can be set by a third-party server (e.g. adserver) via requests made by the user's browser to that server.
Only accessible via the domain that created it.	Accessible to the third-party vendor on any website that loads the third-party server's code.
Improves user experience.	Tracks user behavior across different websites.
Saves settings/preferences/preferred language.	Enables the third-party to create unique user profiles.
Optimizes website for each individual visitor.	Enables many methods of online marketing (tracking, retargeting).
Publisher held responsible for data usage/abuse.	Publisher held responsible for data usage/abuse.
Supported by all browsers and can be blocked and deleted by the user, but doing so may provide a bad user experience.	Supported by all browsers, but many are now blocking the creation of third party cookies by default. Many users also delete third-party cookies on a regular basis.

CHAPTER 2

How Do Cookies Create Privacy Risks?

While cookies offer benefits to both website owners and visitors, they can also create concerns over individual privacy. It is typically possible for an end user to view and delete the cookies stored on their own hard drive, but many consumers are largely unaware of the information contained in them.

While much of the data stored in cookies is useful and relatively safe, **they can also store personally identifiable information (PII).**

Recent years have seen increasing concern over the amount of information about consumers that can be gathered by third-party cookies. Not only can these cookies track individuals' behavior across multiple sites, but they may discreetly gather this information on behalf of companies that the end users are not even familiar with. As a result, some major browsers have started blocking third-party cookies.

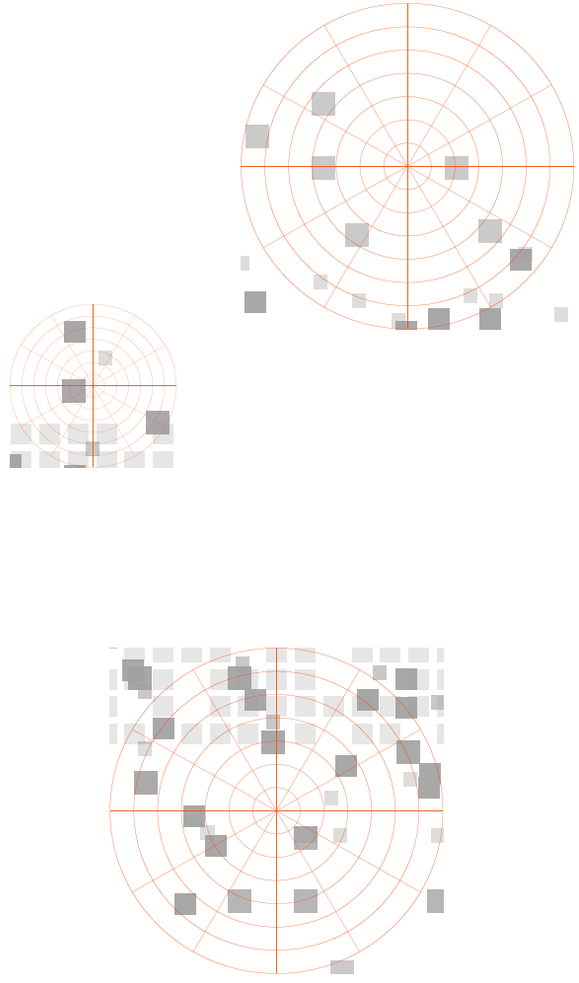
But even if third-party cookies are blocked, there is another way third-party services can use cookies—creating a privacy risk for they website.

How Can Third-Party Services Use First-Party Cookies?

Today's websites tend to rely heavily on third-party services. In addition, many of these third-party services themselves rely on external software embedded into their code. As a result, it is common for websites to rely on third-party software, and third-party services to rely on fourth-party services. In fact, **the data that we at Namogoo have gathered indicates that roughly 40% of all embedded services come from fourth parties.**

By default, when a webpage relies on third- and fourth-party services, those services can view any first-party cookies that are not http-only or secured accessed by that page. For example, if your website's homepage checks for a cookie containing each visitor's first name and last name, any third- or fourth-party service embedded into this page could have access to that information. Should you expose any more sensitive customer details in cookies that other services have access to, your website could create a major privacy risk.

Because most of the data stored in cookies is not encrypted– approximate 89.9%, it would be relatively easy for an unscrupulous third-party service provider to take advantage of this information. The risk increases when you consider the fourth-party services that your company's web developers may not even be aware of. And even if one of your service providers has no ulterior motives for gathering sensitive information from your customers, **there is always the risk of a cyber-attack on that service provider's website, which could give hackers access to any exposed customer details.**



CHAPTER 3

How Do Recent Laws Raise the Stakes?

As concerns over online consumer privacy have grown in recent years, there has been an international trend toward stricter regulation of companies' collection and use of consumer information, including through cookies. In particular, new laws have focused on the individual's right to know about the information being gathered about them and their right to opt in or out of this data collection.

This epicenter of this legislative trend is in Europe, where **the European Union passed the General Data Protection Regulation (GDPR) in 2016 and began implementing it in 2018.**

Also in 2018, the State of California passed the California Consumer Privacy Act (CCPA), which is due to come into effect on January 1, 2020. The GDPR has also inspired similar legislation in a number of other countries, and the CCPA has inspired similar laws in a number of other U.S. states.

While there are some differences between these laws, both the GDPR and the CCPA regulate the use of cookies. Although the GDPR makes clear that its regulations apply to the use of personal information stored in cookies, businesses within the European Union are also obligated to use cookies in line with the ePrivacy Directive, an older law.

Taken together, the GDPR and the ePrivacy Directive require companies to:

- Receive the user's consent before setting non-essential cookies on their hard drive.
- Before receiving this consent, provide the user with an accurate, specific, and easily understood description of the data that will be collected by cookies and the purpose of its collection.
- Keep track of this consent.
- Let the user access a website even if they decline to offer this consent.
- Allow the user to withdraw their consent as easily as they provided it.

Similarly, the CCPA makes clear that it applies to personally identifiable information (PII) stored in cookies just as it does to other types of PII. As a result, the rights that it guarantees to all users apply to personal details stored in cookies.

These rights include:

- The right to know what personal information about them is being collected by a business.
- The right to have their personal data deleted.
- The right to know if their personal information is sold or disclosed.
- The right to say no to the sale of their personal data.
- The right to know what types of personal data will be collected from them before the information is collected.
- The right to know the purposes of collecting their personal data.
- The right to know whom their personal data may be shared with.
- The right to know the sources from which their personal information is acquired.
- An opt-in mandate for the sale of information belonging to minors (persons under the age of 16), with a requirement that a parent or guardian opt in on behalf of a child under the age of 13.
- The right to not be discriminated against for exercising one's rights under the CCPA (although a later amendment added an exception for cases in which "the differential treatment is reasonably related to value provided to the business by the consumer's data").
- The private right of action against a company in the case of a breach of personal data.

Still, it remains to be seen how the CCPA will be applied in the real world once it goes into effect in 2020. In contrast, we have already seen how European courts have begun enforcing the GDPR.

Notably, a recent European case ruling clarified that **users must knowingly and actively provide consent before cookies can be set.** Not only does this ruling forbid the use of pre-checked boxes requesting consent, but **it also requires website publishers to inform visitors in advance about how long a cookie will last and whom its information will be shared with.**

Taken together, relatively recent laws in Europe and California point to increasingly strict requirements for informed consent before cookies can be used. And with similar laws expected in other parts of the world—as well as a new ePrivacy Regulation expected to replace the European Union's ePrivacy Directive—it seems that legal compliance will become a more pressing concern for websites' use of cookies in the future.

Perhaps most importantly, so far it looks like these laws have real teeth.

For violating the GDPR, an organization can be fined up to 4% of its global annual turnover, or 20 million euros—whichever is higher. We have already seen British Airways fined $229 million after suffering from a data breach via a third-party service embedded into its website. And while the CCPA only allows for penalties of up to $2,500 for each unintentional violation and up to $7,500 for each intentional violation, it also allows consumers to sue companies either individually or in a class-action lawsuit. As a result, the CCPA's penalties could reach from $100 to $750 (or the cost of actual damages, should it exceed $750) for each individual violation—potentially resulting in a sum large enough to destroy a small or midsize business.

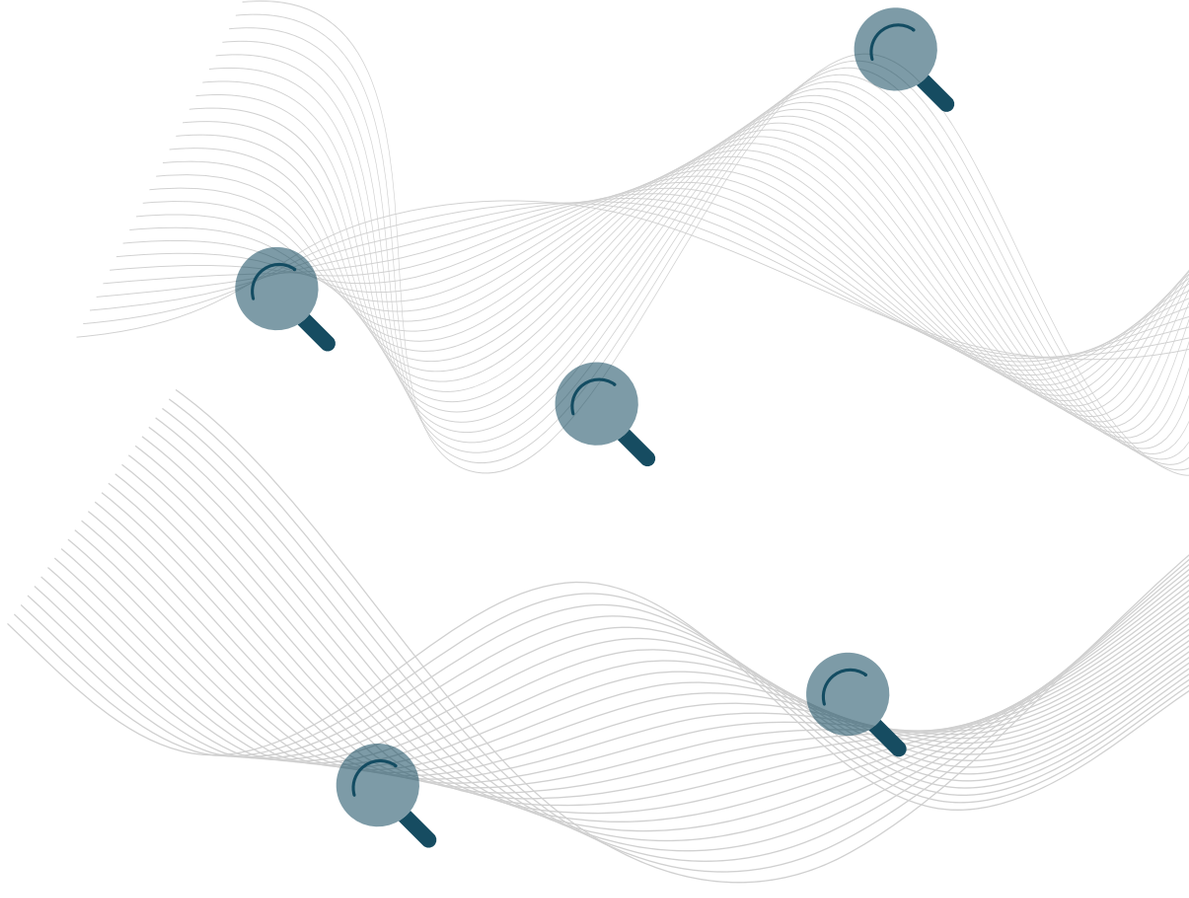
CHAPTER 4

How Can Your Company Avoid Legal Risk?

Given the international legal trends of recent years, today failure to comply with consumer privacy laws can create serious risks for companies. Not only could they face significant fines for noncompliance, but their brand reputations could also suffer as a result.

To efficiently and reliably ensure their adherence to the latest privacy laws, **many companies have started turning to digital solutions.** One of the most common types of products used to address consent requirements is the consent management platform (CMP), a solution that can be integrated into a website to streamline its approach to legal compliance. While every CMP is different, they generally keep track of users' consent and enable businesses to make sure that the use of cookies and the gathering of data take place only in line with this consent.

It is common for CMPs to have some visibility into the activities of third-party services integrated into a website. They achieve this visibility by **using crawlers that can check periodically to see whether a certain service is placing its own (third-party) cookies** or accessing the website's (first-party) cookies.



However, **Namogoo's Customer Privacy Protection (CPP) solution offers companies a far more thorough look at what their websites' third-party services are up to** and what information they have access to—complementing a CMP by filling in key gaps in transparency.

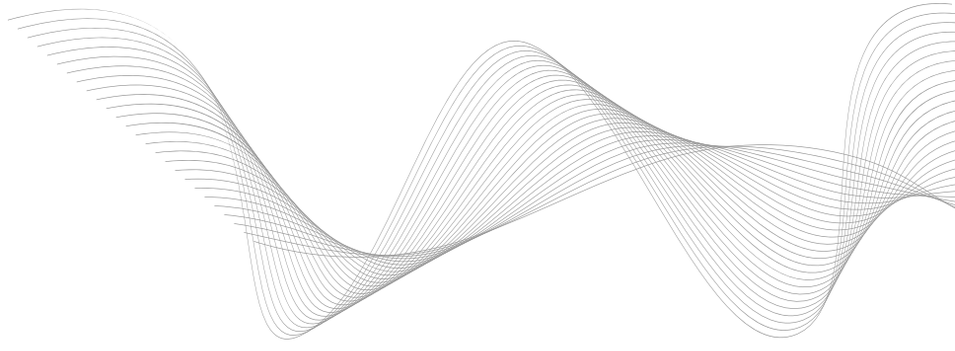
How Does CPP Help Companies Comply with Cookie-Related Laws?

Namogoo's Customer Privacy Protection solution offers you full visibility into the data collected from your website by third- and fourth-party service providers, including data stored in first- or third-party cookies. Specifically, **CPP gives you insight both into the data these service providers actually collect and into any sensitive data that your website would enable them to collect.**

Unlike CMPs, our CPP solution continuously monitors your website's first- and third-party cookies. Whereas CMPs rely on crawlers that run when called into action, CPP offers real-time protection around the clock. In case of suspicious data collection by third or fourth parties, our solution provides you with an immediate alert including the details you need to mitigate any risk and resolve any underlying vulnerabilities. And to help you resolve such incidents quickly, our CPP platform automatically ranks incidents by their priority level based on severity and impact.

Additionally, CPP provides you with a detailed breakdown of the data a given vendor collects from your website, as compared to the data that vendor collects from other websites—providing benchmarks to highlight any suspicious anomalies.

By combining the capabilities of a CMP with the comprehensive, real-time insights offered by our CPP solution, a company can make sure that its use of cookies complies with legal requirements for informed consumer consent. In a world of increasingly strict privacy laws—and growing public awareness of major violations of these laws—using the two types of digital solutions together can prevent significant legal liability and negative press coverage



Conclusion

Among today's websites, the use of cookies is virtually universal—and for good reason. Not only do cookies allow for user-friendly, personalized online experiences, but they enable businesses to gather useful insights into their customers and prospective customers. And they accomplish these goals without requiring companies to store the necessary information within their own server-side databases.

But as helpful as they can be, there is good reason for consumers to be worried about the impact of cookies on their online privacy and security. **Cookies can be used to store sensitive personal details, and many consumers are unaware of the personal information about them that is stored in cookies.** With the proliferation of third- and fourth-party services embedded into websites, it has become common for webpages to allow external companies to access their cookies. And many third- and fourth-party services create their own cookies, allowing a small number of large companies to track individuals' browsing habits in order to support targeted marketing efforts.

In the face of these privacy concerns, the last several years have seen a trend toward increasingly strict regulation of the collection, transmission, and use of consumer details gathered online, including through cookies. Since the passage of the European Union's General Data Protection Regulation (GDPR),

This trend has spread to other states and countries around the world. Both the GDPR and the California Consumer Privacy Act (CCPA) have expanded the rights of individuals to be informed regarding websites' use of cookies and to opt in or out of their use. Perhaps most importantly, these laws have significantly raised the financial risk of noncompliance.

To avoid inadvertently violating these and other privacy rules, many companies have turned to digital solutions such as **consent management platforms (CMPs), which can streamline the process of ensuring that cookies are only set on individuals' hard drives with the agreement of those individuals.**

But while CMPs can be useful tools, they offer limited visibility into the collection of data by third- and fourth-party services.

By supplementing a CMP with Namogoo's Customer Privacy Protection (CPP) solution, a company can gain full transparency into the behavior of its websites' embedded services in real time—enabling the company to ensure that these services do not cause it to unwittingly violate consumer privacy rules. This way, a business can enjoy all the benefits of cookies—the insights, the improved user experience, the monetization opportunities, and the convenience of client-side information storage—without needing to worry that it could unwittingly expose itself to the risk of privacy-related lawsuits.