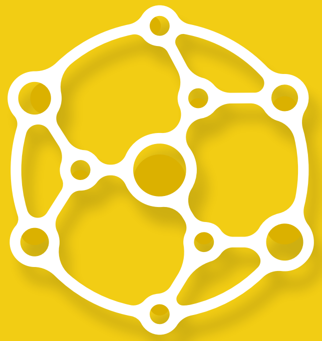
ObservePoint

Bridging Internal Website Privacy Gaps



Over the past couple of years, ObservePoint's annual **Digital Governance Reports** have shown that if you're part of an enterprise-level organization, it's often difficult to know who's in charge of website privacy, let alone what's actually being done about it.

Part of the issue is that privacy compliance demands interdepartmental cooperation from teams with conflicting interests, which can sometimes create a desire to not poke the bear.

For example, the **legal department** feels pressure to keep as much risk off of the website, but they also might not have a thorough understanding of how tags and cookies work and how valuable they are. They're worried about privacy but aren't sure how to execute it because they're not involved operationally.

Marketing or data analysts are under pressure to understand how their ad spend is affecting the bottom line, what performance looks like across marketing touchpoints, and how to optimize their personalization, conversion rates, and purchase journeys, so they want as much information about their customers as possible. They'll want to avoid talking to legal about privacy issues because it might mean that they'll get asked to do more work they see as a nuisance.

Does any of that sound familiar? Ideally, your organization has a department dedicated to data protection that can act as a translator between these two teams, but the responsibility can be assigned anywhere from the legal department to IT depending on resource scarcity. No matter where you sit in your company, this tip sheet will help you ask the right questions to the right people to get an appropriate privacy strategy in place. In addition, we'll tell you how ObservePoint can help fill in the gaps if you need a hand.

As we've seen large **GDPR and CCPA fines** play out in the news, it's no longer prudent to stick our heads in the sand. If we care about revenue and reputation, then we must adhere to a culture that also cares about customer transparency and digital rights. That starts by bridging internal gaps between teams involved in privacy compliance.

Read on to find out how you can achieve website privacy compliance with a better understanding of each other's pain points and what tools you can utilize to minimize annoying tasks and bottlenecks.

Tip 1
Agreeing on Definitions

Generally speaking, if your company has implemented privacy training, then you may have already established a communal understanding of consumer privacy so that there is a framework for handling personal information and an obligation to regulatory compliance and public expectations.

While a privacy-aware team sounds like a great place to start, you may be working without the benefit of such training sessions. With or without a cohesive privacy-centric corporate culture, when it comes to actually executing website privacy compliance efforts, we've noticed that there are some terms that differ by department, which can contribute to confusion. So, here's a handy mini thesaurus we've put together:

Legal Team's Term	Definition	Marketing/Analyst's Term
Data Collectors	Technology on a site that collects data from from visitors	Tags, cookies, JavaScript
Data Transfers	Where data is sent	Network requests
Data Discovery	Finding out what all the technologies collecting data on the site are	Tag/cookie inventory
Data Mapping	To legal, this is a broader topic encompassing more than just the website, such as financial information. For data analysts and software developers, this is going to be the complete list of tags, variables, and vendors	Tagging Plan

Tip 2
Who Should You Ask Questions?

Legal

Each organization is structured differently, but someone in the legal department should find out who is responsible for: **Tag management** - This could be members of the marketing team, an analytics team, a software development department, someone in IT, or a combination of departments. Whoever is managing tags will be a good place to start for your data discovery.

Marketing/Analytics

If marketing, analytics, dev, or ops have questions about legal policies, they should find out who is in charge of: **Data protection or privacy compliance** - This could be the legal department, a dedicated data protection office, or even IT. These are the people you want to collaborate with to get your policies sorted out.

Tip 3
What Questions Should You Ask?

Legal

While you may be concerned with privacy compliance for your company from multiple angles, we're narrowing in on the issues that surround website data privacy. The questions below are not quickly and easily answered by marketing or website managers but represent a thorough accounting of the data points you need for discovery, mapping, and compliance confirmation.

1. What data do we already have on our customers?
2. Are we collecting only the data that is necessary for our revenue teams to conduct business?
3. Can we explain what data we're collecting, for what purpose, and how we're using that data?
4. Do we have a method for tracking down and deleting records if a user requests to be forgotten?
5. Do we have a complete list of every technology that collects data, what data they're collecting, and where they're sending it?
6. Who are the third parties that are receiving our data? (This is a concern for GDPR, since those partners would be considered data processors.)
7. Are our website privacy policies clear, transparent, and accessible from every entry point into the website?
8. Is the "Do Not Sell/Share" link for CCPA compliance accessible from all appropriate parts of the website?
9. Do we have a Consent Management Platform (CMP)? (This is third-party software like One Trust that collects and manages user consent on a website via cookie banners and consent profiles.)
10. Is the consent banner present on all pages? (This is the banner that pops open a modal for users to specify their consent preferences.)
11. Does the CMP effectively respect all possible consent profiles, blocking or allowing specific cookies and tags per user-specified consent preferences?
    a. Accept all
    b. Reject all
    c. Individual permutations of specific categories opted in or out
12. Are the cookie classifications that our web developers/analyst teams use accurate?
13. Is there a way to monitor new cookies and tags that show up on our website, so we can account for them and classify them on an ongoing basis?
14. Are there any network requests coming from countries/regions or specific domains that we should not be sending data to?
15. Have there been any notable changes in JavaScript file sizes that could indicate a potential data privacy concern? (JavaScript is the code that makes the website work.)
16. Are there rogue or piggybacking tags loading outside of a Tag Management System which are therefore not under the CMP's control?
17. Where on our site can personally identifiable information (PII) be entered by users?
18. Where are the PII values being captured, stored, and passed?
19. Do we have a process by which we encrypt and protect PII?

Marketing/Analytics

1. How do we write a privacy policy that would satisfy regulatory requirements for clarity and transparency?
2. Is there guidance on how we classify cookies (as strictly necessary, for functionality, for advertising, etc.) for GDPR, CCPA, or other privacy regulations?
3. To what countries should we not be sending data?
4. Do we have a process of notifying regulatory authorities if there is a data breach?
5. How should we communicate with our third-party vendors when we need to discuss privacy concerns?

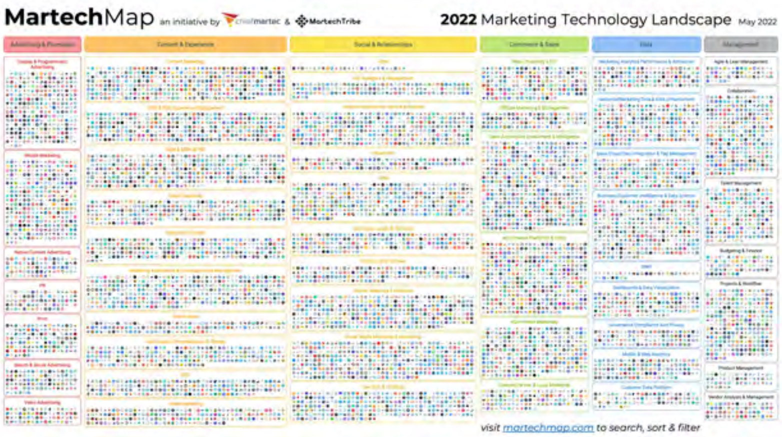
As you can tell from the number of questions, it often falls on the operational departments to provide answers to a legal department whose main function is advisory. However, that's not to say that marketing is not already participating in self-regulatory measures, such as the principles established by the Digital Advertising Alliance (DAA).

> *"Since 2009, Digital Advertising Alliance Principles have existed to extend meaningful privacy safguards and controls to consumers while enabling a more relevant advertising experience, and facilitating a thriving, competitive digital economy that serves thousands of businesses and millions of consumers"*
>
> *– DAA "In Defense of Tailored Advertising: Key Trade Groups Rally Around Responsible Data Collection to Serve Relevant Ads and Engage Consumers"*

Tip 4
Be Understanding of Why Data Discovery Might Be Difficult

Legal

A corporate website is often unwieldy with many moving parts and multiple teams touching the code. Business objectives can change, marketing campaigns launched, and new technologies added, resulting in a dynamic site that is constantly in flux. The pace at which these departments are under pressure to work to generate revenue means that many governance and maintenance tasks are not their top priority. Tagging plans, or the documentation of all the tags, cookies, and variables, are often outdated and can seem overwhelming to maintain. In addition, attributing revenue to the right sources and measuring marketing campaigns are extremely challenging anyway, so there are compelling reasons to try and capture as much data as possible instead of being choosy about it.



Marketing/Analytics

The legal department knows that regional data privacy laws should be a priority, but it's hard to know where to start when you're not involved in the day-to-day operations. Taking the time to educate the privacy team on why you want to track visitors and campaigns, how you're accomplishing it, and being open to adjustments will be important to make measured, strategic compliance plans that mitigate risk, increase customer trust, and get you the information you need to make decisions and produce results. If you feel overwhelmed by the amount of information other teams need, read on for automated solutions built to solve these very problems.

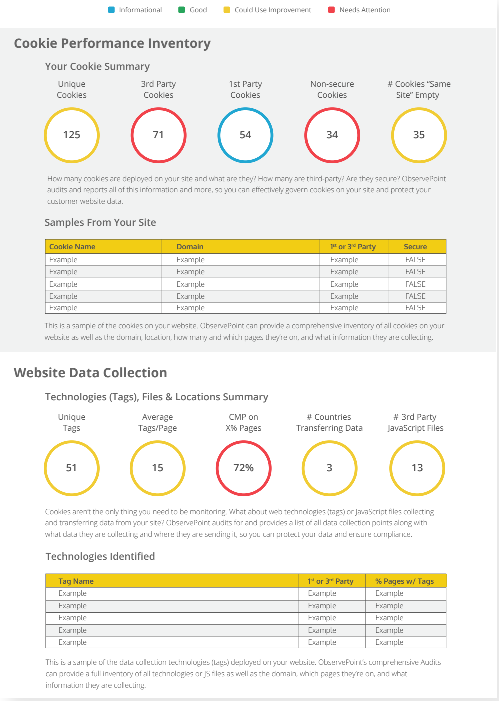
> *"Familiarizing an organization with the concept of data minimization...can provide guidance to the staff about when it is appropriate to collect personal information... Trained team members become more sensitive as to what to ask and how to ask it. They also become more knowledgeable as to why any requested information is needed... A privacy-aware organization can rely on employees to address some privacy concerns independently."*
>
> *– IAPP "Six Ways Privacy Awareness Training Will Transform Your Staff"*

Tip 5
Use Tool to Make Things Easier

ObservePoint can sit between each team and facilitate data discovery as well as ongoing monitoring by helping to answer many of the technical questions the legal or data privacy teams might have.

The legal department can use automated audits for data discovery, and marketing/analytics can treat them as ground zero for an updated tagging plan. ObservePoint can take the heavy lifting of data discovery and compliance monitoring off your plate.

- ☑ Set up comprehensive audits for a complete inventory of the current state of your site.
- ☑ Validate the presence of privacy policies, "Do Not Sell/Share" links, cookie consent banners, and every tag or cookie whether new, approved, or rogue.
- ☑ Enhance CMP limitations, like their tendency to only list a cookie once, even if they are on multiple pages, or their inability to spot piggy backing tags, with drill-down reporting and visual maps.
- ☑ Create custom audits mimicking different user consent preferences to make sure that cookies are being dropped only after consent has been given.



🟦 Informational 🟩 Good 🟨 Could Use Improvement 🟥 Needs Attention

Cookie Performance Inventory

Your Cookie Summary

Unique Cookies	3rd Party Cookies	1st Party Cookies	Non-secure Cookies	# Cookies "Same Site" Empty
125	71	54	34	35

How many cookies are deployed on your site and what are they? How many are third-party? Are they secure? ObservePoint audits and reports all of this information and more, so you can effectively govern cookies on your site and protect your customer website data.

Samples From Your Site

Cookie Name	Domain	1st or 3rd Party	Secure
Example	Example	Example	FALSE
Example	Example	Example	FALSE
Example	Example	Example	FALSE
Example	Example	Example	FALSE
Example	Example	Example	FALSE

This is a sample of the cookies on your website. ObservePoint can provide a comprehensive inventory of all cookies on your website as well as the domain, location, how many and which pages they're on, and what information they are collecting.

Website Data Collection

Technologies (Tags), Files & Locations Summary

Unique Tags	Average Tags/Page	CMP on X% Pages	# Countries Transferring Data	# 3rd Party JavaScript Files
51	15	72%	3	13

Cookies aren't the only thing you need to be monitoring. What about web technologies (tags) or JavaScript files collecting and transferring data from your site? ObservePoint audits for and provides a list of all data collection points along with what data they are collecting and where they are sending it, so you can protect your data and ensure compliance.

Technologies Identified

Tag Name	1st or 3rd Party	% Pages w/ Tags
Example	Example	Example
Example	Example	Example
Example	Example	Example
Example	Example	Example
Example	Example	Example

This is a sample of the data collection technologies (tags) deployed on your website. ObservePoint's comprehensive Audits can provide a full inventory of all technologies or JS files as well as the domain, which pages they're on, and what information they are collecting.

How compliant is your website? **Get a 100-page audit** and see how your privacy stacks up.

START YOUR PRIVACY AUDIT