Privacy Module

of

Watchfire® WebXM™ 4.0

REPORTS AT A GLANCE

Managing Online Privacy

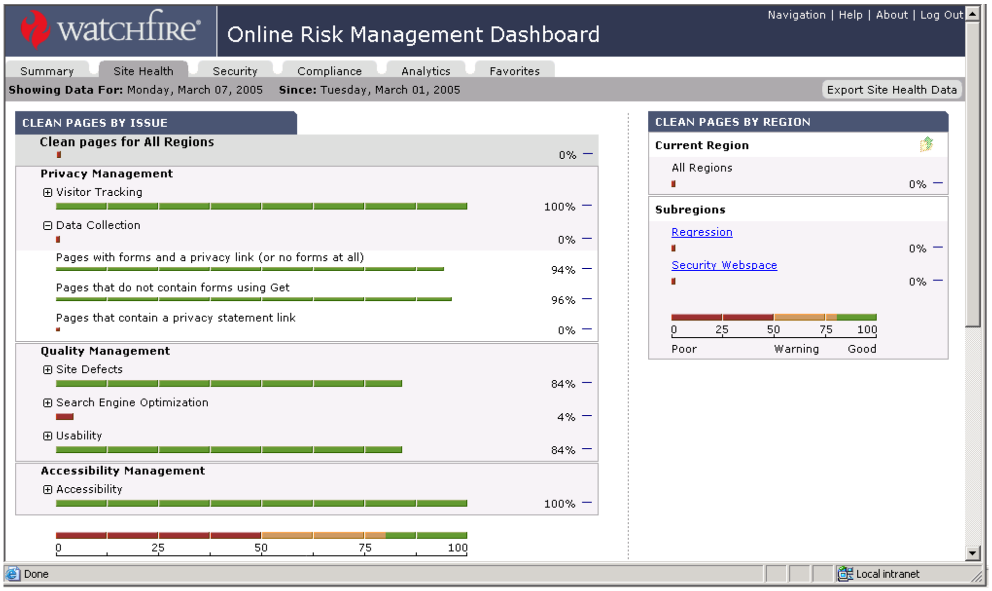
The **Privacy** module of Watchfire® WebXM™ monitors online web properties on an ongoing basis to help manage online privacy, and generates comprehensive, actionable privacy reports that provide visibility into what is occurring on a site so you can manage risk, enable compliance, and create trust. The Privacy module actively monitors your online business and provides reports so you can:

- identify brand and risk issues such as information collection, privacy policy linking (including P3P), user tracking practices, and web page security practices
- enable compliance
- create customer trust
- understand the business implications of your online practices

The Types of Reporting

THE DASHBOARD

The Dashboard lets you see the aggregate summary of the privacy of your website. This executive view allows senior stakeholders to quickly study interactive reports about the website's privacy issues.



Showing Data For: Monday, March 07, 2005 **Since:** Tuesday, March 01, 2005

CLEAN PAGES BY ISSUE

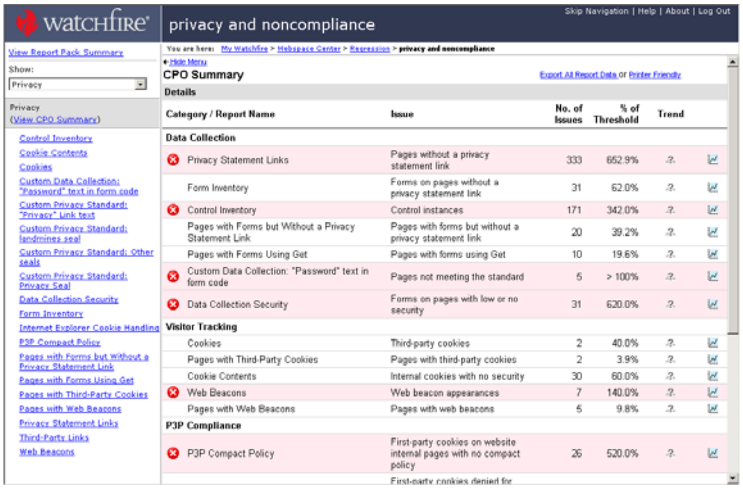
Clean pages for All Regions	0%
Privacy Management	
⊞ Visitor Tracking	100%
⊟ Data Collection	0%
Pages with forms and a privacy link (or no forms at all)	94%
Pages that do not contain forms using Get	96%
Pages that contain a privacy statement link	0%
Quality Management	
⊞ Site Defects	84%
⊞ Search Engine Optimization	4%
⊞ Usability	84%
Accessibility Management	
⊞ Accessibility	100%

CLEAN PAGES BY REGION

Current Region	
All Regions	0%
Subregions	
Regression	0%
Security Webspace	0%

SUMMARY REPORT

The CPO Summary report allows you to monitor your organization's website privacy management practices, and to track the progression of implemented privacy practices.


watchfire®
Skip Navigation | Help | About | Log Out
View Report Pack Summary
Show:
Privacy
Privacy
(View CPO Summary)
Control Inventory
Cookie Contents
Cookies
Custom Data Collection: "Password" text in form code
Custom Privacy Standard: "Privacy" Link text
Custom Privacy Standard: landmines seal
Custom Privacy Standard: Other seals
Custom Privacy Standard: Privacy Seal
Data Collection Security
Form Inventory
Internet Explorer Cookie Handling
P3P Compact Policy
Pages with Forms but Without a Privacy Statement Link
Pages with Forms Using Get
Pages with Third-Party Cookies
Pages with Web Beacons
Privacy Statement Links
Third-Party Links
Web Beacons
Hide Menu
Export All Report Data or Printer Friendly

privacy and noncompliance

You are here: My Watchfire > Webspace Center > Regression > privacy and noncompliance

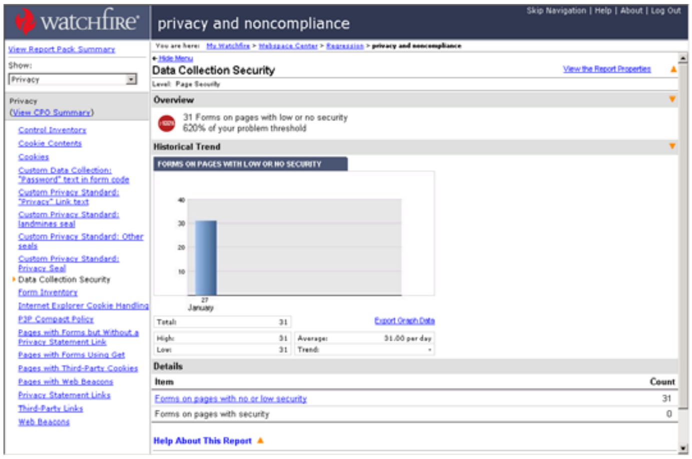
CPO Summary

Details

Category / Report Name	Issue	No. of Issues	% of Threshold	Trend
Data Collection				
Privacy Statement Links	Pages without a privacy statement link	333	652.9%	-?-
Form Inventory	Forms on pages without a privacy statement link	31	62.0%	-?-
Control Inventory	Control instances	171	342.0%	-?-
Pages with Forms but Without a Privacy Statement Link	Pages with forms but without a privacy statement link	20	39.2%	-?-
Pages with Forms Using Get	Pages with forms using Get	10	19.6%	-?-
Custom Data Collection: "Password" text in form code	Pages not meeting the standard	5	> 100%	-?-
Data Collection Security	Forms on pages with low or no security	31	620.0%	-?-
Visitor Tracking				
Cookies	Third-party cookies	2	40.0%	-?-
Pages with Third-Party Cookies	Pages with third-party cookies	2	3.9%	-?-
Cookie Contents	Internal cookies with no security	30	60.0%	-?-
Web Beacons	Web beacon appearances	7	140.0%	-?-
Pages with Web Beacons	Pages with web beacons	5	9.8%	-?-
P3P Compliance				
P3P Compact Policy	First-party cookies on website internal pages with no compact policy	26	520.0%	-?-
	First-party cookies denied for			

DETAILED REPORTS

The detailed reports give you page-by-page analysis of all of the pages with privacy issues.


watchfire®
Skip Navigation | Help | About | Log Out
View Report Pack Summary
Show:
Privacy
Privacy
(View CPO Summary)
Control Inventory
Cookie Contents
Cookies
Custom Data Collection: "Password" text in form code
Custom Privacy Standard: "Privacy" Link text
Custom Privacy Standard: landmines seal
Custom Privacy Standard: Other seals
Custom Privacy Standard: Privacy Seal
Data Collection Security
Form Inventory
Internet Explorer Cookie Handling
P3P Compact Policy
Pages with Forms but Without a Privacy Statement Link
Pages with Forms Using Get
Pages with Third-Party Cookies
Pages with Web Beacons
Privacy Statement Links
Third-Party Links
Web Beacons
Hide Menu
View the Report Properties
FORMS ON PAGES WITH LOW OR NO SECURITY
40
30
20
10
27
January
Export Graph Data
Help About This Report

privacy and noncompliance

You are here: My Watchfire > Webspace Center > Regression > privacy and noncompliance

Data Collection Security

Level: Page Security

Overview

31 Forms on pages with low or no security
620% of your problem threshold

Historical Trend

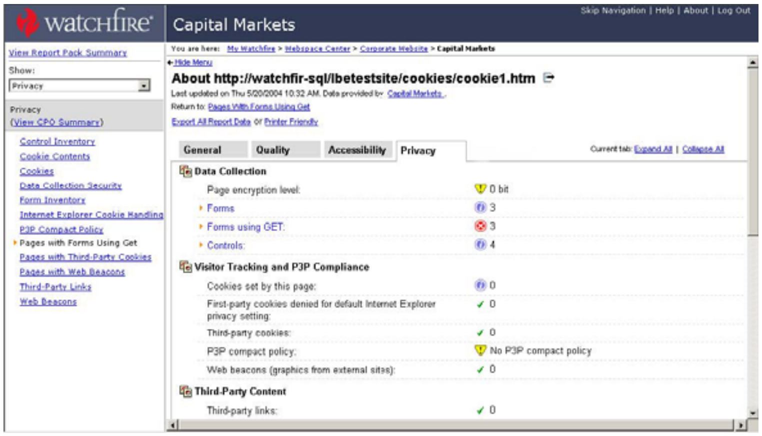
Total:	31		
High:	31	Average:	31.00 per day
Low:	31	Trend:	-

Details

Item	Count
Forms on pages with no or low security	31
Forms on pages with security	0

ABOUT THIS PAGE REPORTS

The 'About this page' report is a summary of the issues found on a single page, including privacy issues. This enables you to monitor and fix all of the privacy issues and other issues on a page at once.



Capital Markets

You are here: My Watchfire > Webspace Center > Corporate Website > Capital Markets

About http://watchfir-sql/ibetestsite/cookies/cookie1.htm

Last updated on Thu 5/20/2004 10:32 AM. Data provided by: Capital Markets .

Return to: Pages With Forms Using Get

Data Collection

Page encryption level:	0 bit
Forms	3
Forms using GET:	3
Controls:	4

Visitor Tracking and P3P Compliance

Cookies set by this page:	0
First-party cookies denied for default Internet Explorer privacy setting:	✓ 0
Third-party cookies:	✓ 0
P3P compact policy:	No P3P compact policy
Web beacons (graphics from external sites):	✓ 0

Third-Party Content

Third-party links:	✓ 0

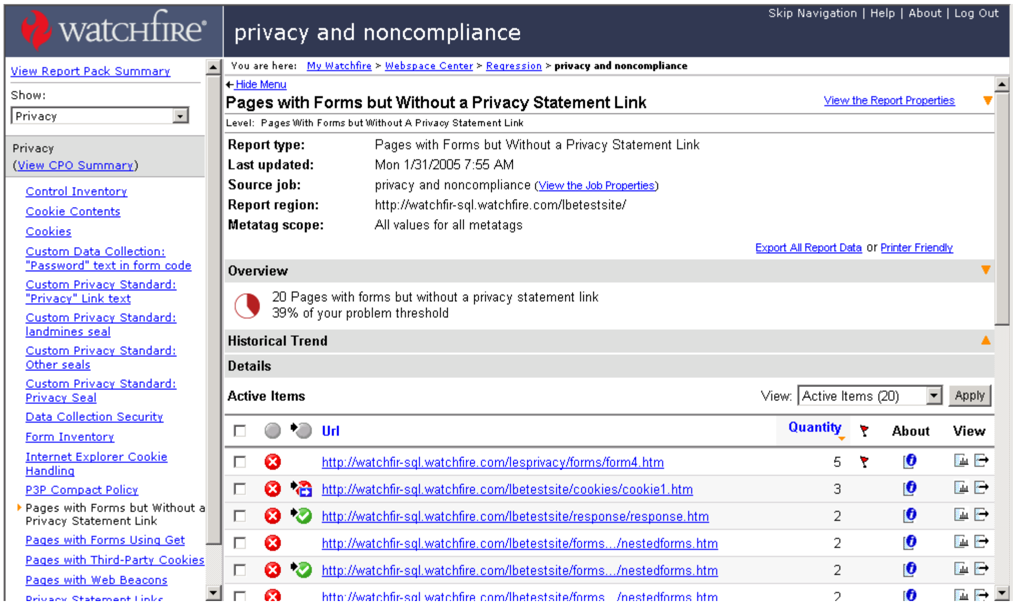
CRITICAL PAGES

The classification engine allows you to select an issue and classify it as open, in progress, noise, or fixed. WebXM remembers the classification from scan to scan so that issues that are either fixed or marked as unimportant are not reported again. This lets you track progress and reduce confusion in the reports. WebXM lets you define how critical pages are determined. This functionality lets you assign criticality to those that are most important to your organization.

You can define criticality by:

- Type of Issue: certain issues may be deemed more important than others so you can label these as most important, such as changing a Warning check into "noise" or "passed"
- Traffic to the Page: you risk exposure may be higher if more users are going to that issue
- Region of the website: certain websites or sections are more important for driving your business

Once you have defined how WebXM should determine criticality it will be highlighted in the report. You can sort the reports by criticality, enabling you to address the items that are most important.


watchfire
privacy and noncompliance
Skip Navigation | Help | About | Log Out
You are here: My Watchfire > Webspace Center > Regression > privacy and noncompliance
View Report Pack Summary
Show:
Privacy
Privacy
(View CPO Summary)
Control Inventory
Cookie Contents
Cookies
Custom Data Collection: "Password" text in form code
Custom Privacy Standard: "Privacy" Link text
Custom Privacy Standard: landmines seal
Custom Privacy Standard: Other seals
Custom Privacy Standard: Privacy Seal
Data Collection Security
Form Inventory
Internet Explorer Cookie Handling
P3P Compact Policy
Pages with Forms but Without a Privacy Statement Link
Pages with Forms Using Get
Pages with Third-Party Cookies
Pages with Web Beacons
Privacy Statement Links
Hide Menu
View the Report Properties
Export All Report Data or Printer Friendly
View: Active Items (20)
Apply

Pages with Forms but Without a Privacy Statement Link

Level: Pages With Forms but Without A Privacy Statement Link

Report type: Pages with Forms but Without a Privacy Statement Link
Last updated: Mon 1/31/2005 7:55 AM
Source job: privacy and noncompliance (View the Job Properties)
Report region: http://watchfir-sql.watchfire.com/lbetestsite/
Metatag scope: All values for all metatags

Overview

20 Pages with forms but without a privacy statement link
39% of your problem threshold

Historical Trend

Details

Active Items

☐	●	●	Url	Quantity	⚑	About	View
☐	✖		http://watchfir-sql.watchfire.com/lesprivacy/forms/form4.htm	5	⚑	ⓘ	
☐	✖		http://watchfir-sql.watchfire.com/lbetestsite/cookies/cookie1.htm	3		ⓘ	
☐	✖	✓	http://watchfir-sql.watchfire.com/lbetestsite/response/response.htm	2		ⓘ	
☐	✖		http://watchfir-sql.watchfire.com/lbetestsite/forms.../nestedforms.htm	2		ⓘ	
☐	✖	✓	http://watchfir-sql.watchfire.com/lbetestsite/forms.../nestedforms.htm	2		ⓘ	
☐	✖		http://watchfir-sql.watchfire.com/lbetestsite/forms.../nestedforms.htm	2		ⓘ	

Data Collection Reports

PRIVACY STATEMENT LINKS

This report lists pages with or without links to the privacy statement. This report is particularly useful if your organization requires privacy statements be placed on certain pages of your website.

Why it's useful:

Most websites now display a privacy statement explaining what information the organization collects from website users and what it does with that information. Given that some degree of information collection continuously occurs as a visitor navigates a website, many organizations want to ensure that a link to the statement is included on every page. Other organizations require that every page that collects personal information from users include a link to the privacy statement. This report will help you identify where your site does and does not contain links to your privacy statement.

FORM INVENTORY

This report lists pages that contain forms. The Form Inventory report consists of the following levels:

- **All Forms:** This report displays a list of all the forms used on your web pages. For each form encountered, the form name, URL, data collection method, level of security, and age is displayed, as well as an indication of the presence or absence of a privacy statement link.
- **Forms on Pages without a Privacy Statement Link**: This report displays information on pages that don't match defined privacy statement rules. Fair information practices prescribe that users be informed of an organization's privacy practices at or before the point at which personal information is collected. Therefore, many organizations have a policy to provide a link to their privacy statement on every web page with data collection forms. If your organization has such a policy, this report will allow you to assess whether your site adheres to the policy.
- **Forms on Pages with a Privacy Statement Link**: This report displays a list of the forms used on web pages that match your privacy statement link rules.
- **Forms Using GET**: When the source page is delivered in response to a page or form that uses the "GET" method, certain information (including data that the end user entered into the form) may be inadvertently transmitted to the receiving server. Litigation and adverse publicity has resulted from the use of the GET method, therefore organizations should review their site to verify that they are not inadvertently transmitting personal user data to

third parties. This report displays a list of the forms on your website that use the GET method to collect visitor information. For each form encountered, the form name, URL, level of security, and age is displayed, as well as an indication of the presence or absence of a privacy statement link.

- **Forms Using Post** With the POST method, form data is sent via the requested header and is not visible in the URL. The submitted data is only sent to the server delivering the page content. This report displays a list of the forms on your website that use the Post method to collect visitor information. For each form encountered, the form name, URL, level of security, and age is displayed, as well as an indication of the presence or absence of a privacy statement link.

Why it's useful:

This report allows you to analyze data collection practices and identify forms that could potentially be inconsistent with privacy policies or lead to information leaks, and is critical to understanding the type of notice given to users when they provide information about themselves.

CONTROL INVENTORY

The Control Inventory report provides summary information about the type of form controls used on your website and the number of pages that contain each type of control. A form control is a component of a form such as a data collection field. The features of this report and its levels are as follows:

- **All Form Controls:** Many websites grant users the ability to express their privacy preferences with user choice components such as checkboxes and radio buttons. If your website displays user choice components to grant users the ability to opt-in/opt-out, this report will identify when these components appear on the same page as a form. This report displays a list of the form controls used to collect visitor data. For each form encountered, the form name, URL, control name, and control type is displayed, as well as an indication of whether the control is pre-populated.
- **Form Controls that are Pre-populated** report displays a list of the forms whose controls are pre-populated with data. For each form encountered, the form name, URL, control name, and control type is displayed.
- **Form Controls that are Not Pre-populated** report displays a list of the forms whose controls are not pre-populated with data. For each form encountered, the form name, URL, control name, and control type is displayed.

Why it's useful:

The Control Inventory report shows you the number of pre-populated form controls to help determine where privacy choices are being offered (opt-in or opt-out).

PAGES WITH FORMS BUT WITHOUT A PRIVACY STATEMENT

This report displays a list of the forms used on web pages that do not match any rule defined for privacy statement links. This provides a list of pages that should, at a minimum, be reviewed to determine if the data being collected could be perceived as personal by a website visitor. For those pages that do collect personal information, a link to a privacy statement should be provided on the page that is requesting the information.

Why it's useful:

It is important that a website visitor can easily determine how data is going to be used when a website asks for information. A website's privacy policy will describe why data is being collected, who will be given access to the data and what types of rights the website visitor has regarding that data once it is submitted. Providing a link from a page that contains a form collecting personal data to the privacy policy governing that data is the best way of providing information to the user when they need it.

PAGES WITH FORMS USING GET

The Pages With Forms Using GET report lists pages that contain forms that are using the GET method of form submission. This provides a list of pages that need to be reviewed to determine if the data being submitted is sensitive. For those pages that do contain information that needs to be protected, the submission method should be changed to use the POST method.

Why it's useful:

When a form is submitted using the GET method, data can be inadvertently transmitted to a third-party website and contravene the website privacy policy. Essentially, the data is passed from the website visitor's computer to the website server via a URL (a web page address line). The items entered into the form are contained within this URL in plain text, exposing the information to anyone who has access to the URL. In many cases the sharing of this information is unintentional. However, this can still lead to serious breach of privacy and its associated brand erosion and costly litigation. The risk is especially high when the region of the website where the form is located contains elements from third parties (e.g. an ad banner or a web beacon).

CUSTOM DATA COLLECTION

The Custom Data Collection report allows for the identification of pages collecting specific items of PII. The resulting list of pages with forms collecting PII can then be used to ensure that they reach minimum standards, such as a link to a privacy statement, proper encryption level of submitted data and the opportunity for the website visitor to opt in or out where appropriate. This report can also be used to determine pages that are not in compliance; for example, forms that request information from a child but do not consider parental consent, or forms that collect Social Security Number but do not provide a secure connection.

Why it's useful

It's important to know where personally identifiable information (PII) is being collected on a website. Not only is this important for the maintenance of corporate standards and good website management, but it can also help ensure compliance with legislation. Many countries have governing legislation that includes corporations' obligations regarding PII (e.g. The European Data Protection Directive, GLBA for US financial data, HIPAA for US health information and COPPA for protecting children's privacy in the US). Knowing where PII is being collected on corporate websites is the first step in achieving compliance.

DATA COLLECTION SECURITY

When users submit information over the Internet, they expect their information to remain secure. This report displays the type and level of security used on web pages containing forms. This report helps you verify that an adequate level of security is provided on pages that collect user information, and can help you identify those pages that do not meet your organization's security standards.

Why it's useful:

Personal information cannot be considered private if it is not collected, stored, and transmitted securely. Therefore, it is important to track the level of security on pages that collect information from users. It is the policy of many organizations to provide a certain level of security for all forms to protect the information entered by users. This report alerts you to instances when forms are not provided with certain security protections, i.e. SSL encryption. Website visitors are increasingly expecting to see a security symbol (e.g. an icon that looks like a lock) at the bottom of their browsers when accessing or submitting sensitive information. If the visitor does not see the icon, they may assume that the data submission method is not secure.

Visitor Tracking Reports

COOKIES REPORT

Cookies are digital identifiers, placed by a web server that allow for advanced personalization of websites. Privacy concerns arise when cookies are used for long-term data collection. This report lists first and third-party cookies found on a website. The information in this report helps you evaluate if cookie use is in accordance with your privacy policy.

Why it's useful

Use of certain cookie technology has resulted in several class-action lawsuits. At issue is whether the company's use of "cookies" to track a user's surfing habits and personal information is an invasion of privacy. Privacy advocates and class-action lawyers have argued that the use of cookie technology constitutes a form of surveillance (akin to wire tapping) that monitors and stalks users without their knowledge.

Excessive and/or unexplained use of cookies (particularly those served by third parties) may be considered deceptive data collection techniques and may even cause users to leave your site. Most web browsers can be set to detect and alert when cookies are encountered when browsing a website. Generally accepted industry standards recommend that companies disclose their cookie use and, in particular, the practice of online profiling by third-party ad servers and provide users with the ability to opt out of receiving third-party cookies. Online consumers may be more willing to interact with a website if they are made aware of their choices, and the company's practices as they pertain to the use of cookies.

COOKIE CONTENTS

The Cookie Contents report displays information about the content and security of each cookie that is found on a website -- a list of pages on which the cookie is set, the particular element that sets the cookie, whether it is a first-party or third-party cookie, the domain the data is returned to, and if it contains a compact policy.

Why it's useful:

Because cookies can contain personally identifiable information, it is important for protecting customer information that you know the security encryption level of the cookies your site sets.

PAGES WITH THIRD-PARTY COOKIES

This report provides a detailed inventory of all cookies found during a scan. Since the websites to which your site links may impose reputation risks for your organization, you should monitor this list. You can use this report to ensure that all the linked sites meet your organization's policies for linked sites.

Why it's useful:

Of all cookie types, third-party cookies are the highest risk to a corporation. Third-party cookies contain and provide information to a third-party that is collected from your company's website visitors. The combination of a third-party cookie with a third-party element can enable a user to be tracked as they browse (the most common example of this is a web beacon). Most website visitors will browse a website and provide information based on their level of trust they have with the company (brand) that owns the website -- they can feel betrayed if a third-party is collecting information and benefiting from this trust.

It is very important to determine the necessity of all third-party cookies on a website. The data stored and collected using that cookie is controlled by a third-party. If third-party cookies are being used, it is important to disclose their use and purpose in the corporate privacy statement. Cookies are often set without the website visitor's knowledge. Web browsers now provide the ability for users to be warned about, or automatically block, third-party cookies. These browser generated alerts, combined with the general perception of most internet users that all cookies are a threat to privacy, can negatively impact a users level of trust.

WEB BEACON

Web beacons (also referred to as web bugs, clear GIFs, or pixel tags) are typically used by third-party service providers to capture information about user behavior on a website. In recent years, website collection of information from Internet users without their knowledge has garnered media scrutiny and legislative attention. The use of web beacons has been especially criticized. As such, their use on your website imposes privacy considerations of which you should be aware. This report displays information about any web beacons that are on the pages in your website. The information in this report helps you to properly disclose to your website visitors how your company is using web beacons and the information they collect.

Why it's useful:

There is potential risk exposure for a website if unauthorized tracking devices are present, if authorized tracking devices are capturing inappropriate data, or if captured data is being used inappropriately. This report can help you determine when new web beacons have been added to your website. It will also allow you to identify old web beacons that should be removed. Web beacons are considered controversial because they are invisible, and monitor online users without their knowledge. As a result, companies that choose to use web beacons should include the use of this technology in their privacy policies. Best practices advocate against using web beacons on "sensitive" sites, such as those sites that target children, or may indicate a user's financial status, health, or sexual orientation.

PAGES WITH WEB BEACONS

The Pages with Web Beacons report provides a list of pages that contain web beacons and displays information about the following:

- all images that originate outside of the website
- the size, with the smallest first by default since very small images are the most suspicious
- which beacons set cookies and are therefore more likely to be legitimate beacons

- external images that do not set cookies. Because they are from an external site, they could become web beacons if whoever controls the external site decides to add a cookie to the image

Why it's useful:

The purpose of web beacons is for a third-party to track a user as they navigate a website. It is also possible to track a user across several websites. This information is sometimes used to provide advertising that targets a user based on the pages and, possibly, various websites that they visit. In general a web beacon collects the information anonymously. However, should the user being tracked ever provide personal information to that third-party, either inadvertently or not, the entire history of that user can be mapped to that individual. Web beacons can cause trust to be eroded and lead to the exposure of sensitive information.

The most sensitive web beacons are those that also set a third-party cookie. These provide the owner of the web beacon the means to track a user through a website. If they are required, their use should be clearly disclosed and explained the online privacy statement.

P3P Compliance

P3P COMPACT POLICY

A P3P compact policy is a list of three-letter codes that communicate the website privacy policy of that page to the web browser in a machine-readable format. The codes will indicate what type of information is collected and to whom the information is distributed. This report lists all compact policies found on website pages where cookies are being set.

Why it's useful:

The Platform for Privacy Preferences Project (P3P) is a relatively new industry standard that enables organizations to express their website privacy policies in a standardized format that can be automatically retrieved and interpreted by web browsers. The goal of P3P is to increase user trust and confidence in the Web. With P3P, users need not read the privacy policies at every site they visit; instead, key information about what data is collected by a website can be automatically conveyed to a user, and discrepancies between a site's practices and the user's preferences can be automatically flagged.

For organizations that are adopting P3P, this report serves as a valuable resource to verify that a full implementation has been achieved.

INTERNET EXPLORER COOKIE HANDLING

Internet Explorer 6, the world’s most commonly used web-browsing software, introduced a method for users to specify a personal privacy setting for managing cookies. There is a range of six privacy settings varying from Accept all Cookies to Block all Cookies. Internet Explorer will compare the P3P compact policy to the privacy setting selected by the user and manage the cookie accordingly. This report contains information on how Internet Explorer will handle cookies found during a scan.

Why it’s useful:

Internet Explorer can take four different actions on a cookie:

- A Denied cookie will not be set, meaning the information it is meant to store and pass back to the specified domain will not be available.
- A Downgraded cookie is one that the HTTP header for a page or element specifies to be persistent but that Internet Explorer treats as a session cookie.
- A Leashed cookie is a cookie that will only be accepted in a first-party context. If an attempt to set or read the cookie is made in a third-party context, the cookie will be blocked.
- An Accepted cookie is one that is accepted by Internet Explorer.

Given that cookies often support critical website functionality such as logins, shopping carts, and personalization, it is important to determine how cookies will be treated by website visitors using Internet Explorer. This report shows how each cookie found during the scan will be treated for users at each privacy setting within Internet Explorer.

Third Party Content

THIRD PARTY LINKS

This report lists pages with third-party links where your organization may be exposed to litigation and reputation risks if a linked site has questionable privacy practices. You can use this report to ensure that all the linked sites meet your organization's policies for linked sites.

Why it’s useful:

It is important to know what external websites your site links to. Your organization may bear reputation and litigation risks if a linked site has questionable privacy practices. Identifying the linked sites can help you monitor these risks. Managing your company’s data practices may also encompass a due diligence of any third parties’ links on your website. Companies should strive to assure that parties with whom they have a business relationship have adequate security and privacy policies in place. If these third parties have substandard privacy practices, an organization may want to remove the links to these sites in order to avoid privacy risks. Understanding your business affiliates' practices is as important as knowing your own.

Custom Privacy Standard

This report displays information about the pages on your website that satisfy, or do not satisfy, the custom rules that you created for the content scan. WebXM scans your site and can report on any predefined web standard such as profanity, or any other corporate standard. You can use WebXM to check for the absence or presence of any specific text, links, and tag text to help ensure compliance with corporate standards.

Why it's useful:

An educational site discovered it was linking to a pornographic site. A major financial institution found profanity on its corporate site. An insurance site uncovered links from its site to one instructing readers on how to commit suicide. Could this happen to your site? Yes. What are you doing to monitor that it does not?