

DATA QUALITY

and the

DIGITAL WORLD

A WEB ANALYTICS DEMYSTIFIED WHITE PAPER

April 2015

ERIC T. PETERSON

Author, Founder & Senior Partner
Web Analytics Demystified

Presented by

ObservePoint

EXECUTIVE SUMMARY

In 2015 **Web Analytics Demystified** and **ObservePoint** called attention to the need for a greater focus on data collection and accuracy in online and mobile sites and applications. Our white paper, *When More Is Not Better: Page Tags*, described the dramatic proliferation of script-based data collectors including Web Analytics, Voice of Customer, Customer Experience Management and related solutions. We detailed the risks associated with failing to pay close attention to where and how tags were deployed.

Our recommendation to assign executive responsibility for the flow of data into and out of the Enterprise, is one that companies have increasingly been following. To follow-up, ObservePoint offered to sponsor this white paper to examine the requirements for creating a trustworthy, high-value tag management practice within organizations. “It’s like an oil change on your car, an insurance policy against bigger problems down the road,” says Tim Munsell, ObservePoint customer and Web Analyst at DaveRamsey.com.

To this end, we provide ten tested tips to help you institutionalize an effort to ensure data accuracy, integrity, and trustworthiness across your entire business. Each of the tips are reasonably easy to execute, and in total they will result in a world-class program of data management in your online and mobile-connected channels.

Web Analytics Demystified has worked with clients the world over to help ensure the

utility of digital data within the Enterprise and we sincerely hope you will benefit from what we have learned. Executed properly, these tips have the potential to transform your digital measurement efforts.

According to Matt DiAntonio, Director of Business Analytics at Carbonite, "Investment in a tag auditing solution helped my teams reduce gaps in tagging over the entirety of content deployments across hundreds of sites worldwide. This was a huge victory considering the amount of content we produce and changes we were making."

We welcome comments and questions about this work.

TABLE OF CONTENTS

Executive Summary	ii
Data Quality and the Digital World	1
Inexperienced Internal Resources	2
Agencies and Other Third Parties	3
Data Leakage: The New Enterprise Concern	4
10 Tips to Create Trust in Online Data	6
Assign ownership for data quality	6
Define governance for data quality	8
Deploy a robust tag auditing platform	10
Illustration 1: Fast Results	11
Set a rhythm for scanning	11
Illustration 2: Actionable Detail	12
Audit data collection once, twice, three times	13
Create proactive alerts	15
Scan globally, act locally	16
Confirm complex integrations	17
Leverage audits for documentation	18
Illustration 3: Data Export	19
Prevent Data Leakage	20
Illustration 4: Audit Summary	21
Conclusion	23
About the Author	24
About Web Analytics Demystified	25
About ObservePoint	25

“ More than 80% of sites have improperly deployed data collectors at some point, resulting in broken web pages, loss of site traffic, and lost sales.

— Tagman

DATA QUALITY AND THE DIGITAL WORLD

The notion of data quality in the digital world is something of a boondoggle; everyone expects it, but few companies do nearly enough to work to achieve any level of completeness in data collection. Despite promises to the contrary, ensuring accuracy in an increasingly complicated digital environment – one plagued by external sites, non-standard devices, and the ebb and flow of media-driven consumer paranoia – is incredibly complex. And while companies would be well-advised to simply give up on the crazy notion of data accuracy and instead recognize the inherently sampled nature of all digitally collected data, in our experience at Web Analytics Demystified few companies are willing to take that step.

Why is data accuracy such a difficult issue? Myriad reasons, but three consistently rise above the rest and are worthy of discussion.

NEW TECHNOLOGY (AND TECHNOLOGY IN GENERAL)

Perhaps the single most insidious cause of data loss and inaccuracy is our never-ending quest for shiny new things. Social networks, mobile applications, video, ...the list appears endless at times, and while each presents a unique opportunity to connect with

consumer audiences, collectively new technology more often than not ends up breaking the traditional data collection mold and introduces even more opportunity for inaccuracy.

Given the restrictions imposed – ranging from limitations on the kind of code that can be deployed, the type of data that can be collected, and even the ability to deploy tracking code altogether – it is a small miracle that business owners are able to report meaningful data for their investment in new channels, despite the expectation of 100% accuracy in reporting.

This is not to say that measuring web sites in itself is easy – far from it. Given the rapid growth of Internet usage around the world, coupled with the ceaseless influx of new measurement and optimization platforms, it should come as no surprise that web-based data collection often fails. What's more, according to a study produced by tag management system vendor TagMan, more than 80% of sites have improperly deployed data collectors at some point resulting in broken web pages (36%), loss of site traffic (31%), and lost sales (28%).¹ These data are validated by work done by BPA Worldwide who shockingly found that 95% of 250 sites surveyed had holes in their data collection plan on an average of 20% of their pages.²

INEXPERIENCED INTERNAL RESOURCES

Technology is not the only culprit when it comes to sources of inaccuracy. Within enterprise information technology (IT) groups, there is an interesting phenomenon when it comes to tag-based data collection technology – the job often falls on the least qualified and least experienced person possible. Perhaps it is because analytics is boring, perhaps because page tags are banal, or possibly because IT is simply too busy to help marketers gather data. Likely, these groups don't understand the data's value to the business. I am honestly not sure, but it is exceedingly common

1 <http://www.tagman.com/tag-management-survey/>

2 <http://www.observepoint.com/blog/tag-audit-study-reveals-shocking-statistics>

to hear that some aspect of tag deployment went sideways, resulting in incomplete data (or worse – widespread data corruption), simply because unsuitable resources were assigned to the work.

Now this is clearly not the case in all instances, but it happens often enough that we called this issue out in our earlier work with ObservePoint, and the problem persists. In our 2010 paper, *When More Is Not Better: Page Tags*, we identified this problem and called for the creation of a Chief Data Officer role to clarify governance and business process for data collection across the business. And while we are not yet aware of any company that has created such a C-level position, we do know many that have taken our advice to heart and paid closer attention to ensure that qualified and senior resources are tasked with caring for their digital data collection infrastructure.

AGENCIES AND OTHER THIRD PARTIES

Unfortunately, getting things straight inside the business is sometimes not enough, especially within large, complex, and global organizations. It is common to find agencies and third parties taking responsibility for building web sites and applications and, more often than not, responsibility for deploying data collectors as part of their deliverables.

While it is hardly fair to throw all agencies and external developers under the proverbial bus, in our experience the agency model rarely rewards the type of attention that most script-based data collectors require. Instead, they prefer the on-time delivery of exquisitely crafted user interfaces, edgy campaigns, and otherwise brilliant content (that will sadly not be measured properly or accurately).

The only ways we have found to counteract this occurrence is to pay careful attention to deliverables, closely manage how data collection is implemented, or have your own team implement data collection. Even then, last-minute changes can break data collection and, in the worst case scenario, result in a bunch of people sitting uncomfortably around

a table having to admit that they're really not sure how effective the exquisite, edgy, and otherwise brilliant creative was at driving traffic and generating revenue.

DATA LEAKAGE: THE NEW ENTERPRISE CONCERN

During the research and conversations for this white paper, something new came up that frankly, we didn't expect: the threat of data leakage. Given the sheer number of tag-based data collectors out there, coupled with relatively junior resources, agencies, and the general fragmentation of modern web sites, it should not come as a surprise that sometimes tag-based data collectors are being deployed without permission, against policy, and in ways that potentially puts valuable business data at risk.

One company interviewed for this research, thanks to their use of ObservePoint, found both Google Analytics and Quantcast tags – very much disallowed by the company's Privacy Practices group responsible for consumer data privacy across the entire global business.

The threat of data leakage certainly depends on your business and the relative importance of your online channels. Small, centralized companies and those companies that generate only a small amount of revenue digitally are likely unconcerned about this potential risk.

But consider the case of publicly traded, Internet only companies like Amazon.com and Expedia.com where a data leak potentially divulges information that could be used to illegally evaluate company performance and thus impact shareholder value. Even if you're not a publicly held Internet pure-play, common sense dictates that you would want to protect your online data the same way you do all of your business, financial, and employee records – but to protect your data you first need to know what is deployed and who has access.

Do you?

TEN TIPS TO CREATE TRUST IN ONLINE DATA

Today's business leaders are looking to their marketing and digital analytics teams to provide actionable insights based on reasonably accurate, trustworthy data. Delivering on this expectation is no easy feat and requires a combination of people, process, and technology coupled with accountability that sadly too few companies have been able to muster.

Still, at Web Analytics Demystified we have helped many clients meet their leaders expectations of their digital measurement, analysis, and reporting efforts. We offer the following "ten tips" to create a more trustworthy, valuable, and actionable data environment to serve as a basis for all of your analytical efforts.

TIP**1**

ASSIGN OWNERSHIP FOR DATA QUALITY

The key to data quality is having someone in your organization take responsibility for ensuring data quality. As pedantic as this may sound, we are too often surprised at the wide gap between the number of companies expressing the desire for accurate and trustworthy data and the number of companies actually doing something to create accuracy and trustworthiness.

While the title and role of the owner will vary depending on the current maturity of your organization, we typically recommend assigning the responsibility of data stewardship to someone with the following characteristics and qualifications:

- 1 Has a technical background.** A strong background in technology is a requirement. Hopefully this is obvious, but let us accentuate. Javascript is a must, as is Flash ActionScript if you do any work in Flash, plus enough familiarity with the platform your sites are built on and any mobile platforms you may be building for today or in the future.
- 2 Understands the value of data to the business.** Technological sophistication is only a small part of the data steward's job; the bigger picture is communicating the value of the collected data back to the business. Remember: you're not collecting data for data's sake, you're collecting data for the business sake.
- 3 Is reasonably senior.** Far too often, the job of data steward is given to someone too junior in the organization to actually cause change when change is necessary. By assigning responsibility for data quality to someone more senior, you improve the odds that identified issues will be resolved, challenges will be overcome, and the overall quality of your digitally collected data will improve.
- 4 Actually uses the data in their job.** Rather than assign the role of data stewardship to a mechanic trained to look for broken code, at Web Analytics Demystified we recommend assigning the work to someone who will actually recognize problems in the data as they manifest. It goes without saying, but there are profound differences between a variable being populated and a variable being populated correctly.

Once someone is assigned responsibility for your company's data, the next step is to create organizational process and governance to ensure ongoing quality and handle exceptions as they occur.

TIP

2

DEFINE GOVERNANCE FOR DATA QUALITY

High quality data does not just organically appear, especially in a complex enterprise. Data quality happens because the organization agrees that having accurate, trustworthy data is important and because business stakeholders are willing to change internal process and behavior as necessary to facilitate data quality.

While the comprehensive requirements of data collection best practices are beyond the scope of this white paper, our decade of experience helping companies build and refine governance around digital measurement, analysis, and optimization reveal three key processes:

- 1 Add new data collection devices.** Data collection is a key process in any business, but one especially important in complex, distributed, or multi-brand businesses where an array of resources are developing and deploying measurable content. All too often web analytics is considered an afterthought during the design and deployment process and, typically at the eleventh hour, code is slapped on the page without regard for proper deployment and variable setting. Creating a clear and consistent business process for adding data collection that is integrated into development and content deployment processes is critical to your success in creating actionable and trustworthy data.
- 2 Verify proper functioning of data collection devices.** Just deploying data collector code to your pages and applications isn't enough. You will need a process to confirm that variables are set properly and that the code functions as expected

under a variety of conditions. Given the still changing browser landscape, coupled with the emergence of mobile devices (with additional limitations), verifying proper coding is more important than ever.

While there is likely some temptation to assign this responsibility to your normal developmental quality assurance (QA) staff, at Web Analytics Demystified we recommend resisting that temptation and keeping the data confirmation processes within your digital measurement group. Keep in mind that it's not enough for data to simply be populated – the data has to be correctly populated. A combination of knowledge about data collectors, analytics systems, and the systems generating the data is critical. While proper functioning can be verified using simple technology found in a number of QA tools, such as ObservePoint's browser plug-in,³ there is no substitute for knowing why the data is being collected and how the data collected will be used in a business context.

3 Conduct a data collection device audit. Once you believe that data collectors have been correctly deployed, you then need a process to confirm the deployments are maintained over time. While it may seem odd – the need to confirm that deployed code has stayed deployed – in our experience most modern web sites have enough moving parts and enough people touching code that failing data collectors are surprisingly common. Fortunately this process is easily facilitated thanks to tag auditing and management platforms.

A new product category has emerged in the past few years that, like tag auditing solutions, is designed to help the enterprise improve the overall accuracy and utility of tag-based data collection. Dubbed Tag Management Systems (TMS) by Web Analytics Demystified in our 2010 work titled *The Myth of the Universal Tag*⁴, these systems similarly help mitigate common challenges associated with digital data collection.

3 <http://www.observepoint.com/form-validation-and-analytics-analysis-plugin>

4 <http://www.ensighten.com/whitepapers>

While TMS is very much a step in the right direction, these platforms also require care and consideration in their deployment. According to Patrick Foster, Senior Director of Analytics and Messaging Systems at Turner Broadcasting Systems, “If there was some way to guarantee that our tag management system was deployed correctly every single time we wouldn’t need something like ObservePoint but, at least today, we don’t have a tool to confirm the accuracy of our TMS deployed tags and, even if we did, we believe the human element will always necessitate validation.”

TIP 3

DEPLOY A ROBUST TAG AUDITING PLATFORM

Unless you are the smallest of small businesses or have an extraordinarily simple web site and deployment, Web Analytics Demystified strongly recommends the use of a robust tag auditing solution. Designed to census your entire web site to confirm the presence (or absence) of various of digital measurement solutions, the best auditing solutions on the market today take scanning a step further and offer solution-specific data confirmation services, complex tag verification, and proactive alerting.

Fast Results

An email alert showing that a site scan is complete. The alert shows the number of pages found, tags found, and pages missing tags.



Given that digital measurement solutions are only as good as the data they process, a tag auditing solution can be the difference between having data and having accurate, actionable, and trustworthy data. According to Tim Munsell from DaveRamsey.com, “Having a tag auditing solution has improved how we go about tagging our pages and how we think about what we are tracking and why.”

Especially in complex environments where content changes frequently or when a large number of resources are deploying content, the likelihood that your data steward can oversee data collection without an auditing solution and QA automation is quite low. Given the relatively low cost of currently available auditing solutions juxtaposed against the value of having trustworthy data, at Web Analytics Demystified we consider tag auditing solutions to be a requirement.

SET A RHYTHM FOR SCANNING



Once you have assigned an owner, developed governance, and deployed a tag auditing solution, the next step is to develop an ongoing reporting rhythm for scanning and auditing. Developing a rhythm will ensure that the regular verification and validation of your data collection environment becomes part of your organization’s digital DNA. We recommend two ongoing scanning rhythms:

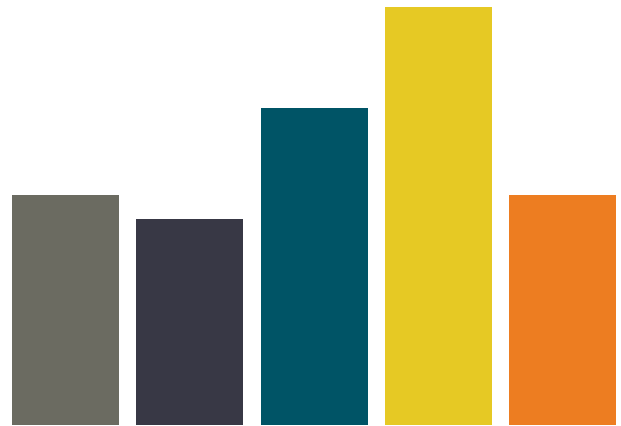
- 1 Perform weekly “difference” scans to determine what, if anything, has changed.** On most complex sites a lot is changing on a weekly basis. Rather than try and wade through your entire site and confirm each and every page, Web Analytics Demystified recommends looking only at the pages on your site that have changed. How you do this will depend on the service you use, but if you have good documentation on your site’s deployment (perhaps via a version control system) you can simply feed your auditing solution changed URLs to confirm that

they are tagged properly.

- 2 **Perform monthly “full” scans to ensure complete and accurate data collection.** Regardless of how often your site changes, Web Analytics Demystified recommends doing a monthly complete scan of your site or sites to confirm data collection is occurring as planned and, if not, create a priority list of pages that need to be corrected. Depending on the relative stability of your site, the results can be either easily read or overwhelming; fortunately the best tag auditing services help you very quickly identify areas that need attention, all the way down to the level of the URL and variable needing attention.

Actionable Detail

solution-specific data confirmation, complex tag verification, and proactive alerting for all digital marketing channels and content types.



TIP 5

AUDIT DATA COLLECTION ONCE, TWICE, THREE TIMES

Web Analytics Demystified recommends a three-fold auditing strategy whenever new content or functionality is being deployed. Ideally, you are able to pass data collected during the development and testing process into a “dummy” or throwaway account, just in case data collection doesn’t go exactly as planned.

Test frequently during the development process.

In order to instill resources throughout your company with data collection best practices,

we recommend running a tag audit multiple times during any large-scale deployment effort and, when appropriate, sharing those results with developers and project managers. By sharing results, especially if you are able to go into detail regarding what is working (and what needs additional attention), you are subtly training internal resources to start thinking about the data collection process as part of larger design efforts. Consider making tag auditing results part of each regular build meeting and you'll be well on your way to creating a culture where trustworthy data is the rule, not the exception.

Test weekly during quality assurance and testing phases.

After your development project has passed into your QA environment, the time is ideal to closely monitor the data being passed to your digital measurement systems. If your company is particularly good at testing and likely to generate a wide range of sample data, the combination of a tag audit and a regular review of key variables being populated should give you a reasonably good sense of what "real world" results should look like.

Test immediately following deployment to confirm data is being collected as planned.

Most companies are used to completing this step – confirmation that data collection has successfully migrated from the development and testing environment to live. That said, the mistake that companies commonly make is delaying corrections when problems are identified. The best practice is to assign resources to post-deployment efforts tasked with ensuring that data collection is correct, that any found bugs are cleared, and that reporting from the newly deployed pages or content will help validate the value of the deployment.

Ideally, your deployment process is not considered complete until all aspects of the code are deemed functional in a production environment – including data collection code. Companies that are committed to data accuracy and utility within the broader enterprise

are never satisfied with asterisks next to their numbers indicating additional context is necessary (when that context is an explanation about why data collection challenges existed when the code was deployed live).

“We have 40 or 50 developers dedicated to the web site and we roll code twice a week,” says Tim Munsell, Lead Web Analyst at DaveRamsey.com. “Up until now, we didn’t have an easy process to validate page tagging on such a frequent basis. I needed to hand check new or altered pages with each rollout, which could easily lead to missed errors in the tags.” Now, Mr. Munsell uses ObservePoint as a part of an efficient process for working with his developers to continually validate code during the development and deployment process.

TIP

6

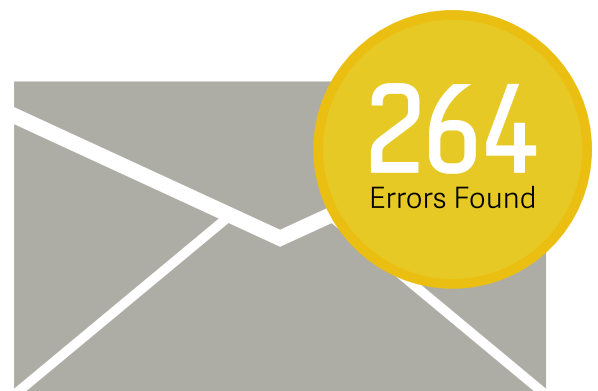
CREATE PROACTIVE ALERTS

Given the general complexity of most site and application deployments in this age of mash-ups, +1 buttons, and quickly evolving web standards, it should come as no surprise that sometimes things simply break for no foreseeable reason. Unfortunately, unless you are auditing your site constantly there is no way to know when something breaks until either, a) bad data appears in your analytics platform at high enough volumes to be noticeable, or, b) your next monthly audit occurs, highlighting the broken code.

That is, unless you have proactive alerting.

Proactive alerts

Receive notifications instantly when a page loses a tag.



Proactive alerting is exactly what it sounds like – your tag auditing solution’s ability to process your sites in the background and sending you a message when something goes wrong.

Ideally you are able to generate an alert whenever a new tag is added to a page, a tag is removed (or absent) from a page, or when a pre-determined variable doesn’t appear to be populating correctly. Additionally it would be useful to know whether your tags are taking an inordinate amount of time to run or respond – a possible indication of problems at your data collection service provider or application. Vendors in the space each provide a different level of alerting functionality so we recommend you explore their capabilities closely if you’re making a buying decision.

SCAN GLOBALLY, ACT LOCALLY



While we definitely recommend having a single data steward within your organization who takes responsibility for overall data quality, it is important to recognize that no one person can manage this effort on their own. Because of this we advocate for a scan globally, act locally approach in which the entire organization works together to ensure data accuracy and trustworthiness.

One such strategy that we have seen work effectively is to establish an enterprise-wide Data Quality Working Group which would draw on resources from across the organization, ideally from each functional group having a vested interest in the company’s online efforts. Led by the assigned data steward, this working group should meet on a monthly basis (or as frequently as you are conducting full site scans using your tag auditing technology) and assign tasks based on problems discovered during the scanning process. Each group member is then responsible to the larger working group to ensure that problems are corrected within a reasonable time frame.

This strategy works, especially in the large enterprise, because of the often distributed nature of web development and deployment. According to Matt DiAntonio, Director of Business Analytics at Carbonite and an ObservePoint customer responsible for a worldwide web analytics practice in a previous role, “our legal group in both the U.S. and Europe really appreciated that we were keeping an eye on things (with ObservePoint) and keeping a clean house.”

By assigning corrective actions to individuals who actually report to the organization where problems are identified, you will dramatically increase the likelihood of success. The converse approach – having a single, centralized resource responsible for driving corrective action across the broader business – rarely seems to work given the siloed nature of most organizations, a generalized lack of knowledge about data collection requirements, and oftentimes a lack of urgency regarding analytics.

TIP**8**

CONFIRM COMPLEX INTEGRATIONS

One advantage tag auditing technology confers, assuming it is robust and provides granularity to the level of individual variables, the verification of complex integrations through rules-based filtering and automation. For example, if you have a set of variables that need to be populated a specific way based on how a web page is accessed, robust tag auditing tools can allow you to confirm the population of those variables on an ongoing basis. Especially given the somewhat awkward requirements imposed by many of the most popular web analytics platforms, this type of confirmation can be a tremendous time-saver.

According to ObservePoint customer Tim Munsell, Lead Web Analyst at DaveRamsey.com, “In order to control Adobe-related costs, we limit the number of Vista rules and Discover licenses we have active at any time, but we still want to enable complex reporting

on paths, tracking codes, and the like for our business analysts. One of our strategies to this end is to be very selective about what data is sent to each of our report suites. Given the complexity of this task, ObservePoint is critical to our ongoing success, constantly monitoring that the right data is being populated into Adobe's data collectors. Now, instead of having to pay for additional data collection, instead we are able to execute on a logical strategy that relies on a small number of events and eVars which simultaneously save us time and better facilitate the analysis process."

LEVERAGE AUDITS FOR DOCUMENTATION



Related to the confirmation of complex implementations is the notion of using audit results as a basis for your internal documentation for web-based data collection. Typically, documentation for digital measurement efforts involves maintaining your original Strategic Requirements and Design (SRD) document, often provided by your systems vendor or implementation consulting firm. The best practice is a quarterly review of the document with updating as necessary to maintain an accurate reflection of which data is being collected where (and why.)

When it comes to documenting web-based data collection, the reality for most companies is far from optimal. Companies often spend a great deal of time developing lengthy SRD documents on the front-end of a data collection deployment, only to have those documents end up on the shelf, collecting dust. Then, when someone has a valid question about why or how data is being collected, the document is out-of-date and unless the original developer can be found, getting answers is an exercise in futility.

There is, however, a better way that can be powered by a robust tag auditing solution. According to Tim Munsell, Lead Web Analyst at DaveRamsey.com, "The report we get from ObservePoint is a more useful and accurate reflection of our implementation than

our original documentation. We are able to export our audit to Excel and essentially work backwards, making sure that the data collected on each page on our site matches our business requirements.”

TIP**10**

PREVENT DATA LEAKAGE

Given the relative ease with which tag-based data collectors can be added to a web site, combined with the fragmented approach companies take to digital measurement, analysis, and optimization, it should be no surprise companies have started to leak data. There are perfectly good reasons that companies have deployed a multitude of data collection devices, but unless those reasons have been elucidated through proper channels and permission for deployment has been given, the business is potentially at risk.

Data leakage can create problems in a few scenarios:

- 1 An employee leaves the company to work for a direct competitor but maintains access to traffic and revenue data through the unknown deployment of a tag-based data collector;
- 2 An agency deploys a tag-based data collector which is under scrutiny over the type of personally identifiable information (PII) the system collects, thereby exposing the company to the same examination;
- 3 The information technology group has made a significant investment in a tag management system, designed to confer control and oversight of tag-based data collection across the enterprise, yet other groups continue to circumvent the tag management process to meet their own needs;
- 4 A third-party vendor has deployed a tracking technology known to sell data to other third-parties, potentially exposing your site data to direct competitors;

- 5 The management team has concerns about a specific analytics solution and has banned it from all sites, yet the tag continues to appear on pages.

Depending on your business model and the data you collect online, data leakage can vary from a minor annoyance to a major catastrophe. Few would argue that it is okay to have random data collection systems deployed to the site without a clear plan for maintaining the accuracy, validity, and security of the collected data. Bottom line: without some type of auditing plan and the organization to support it, your business might be leaking data.

Fortunately, combating data leakage is relatively simple, especially given the availability of robust tag auditing solutions such as ObservePoint. All that is required is a complete scan of your sites; the result is a list of technologies found which can then be compared to expectations.

When unexpected results are found, the action will be clear: the first level of drill-down on these reports details the exact URLs where the potentially leaking code was found. At that point all that is required is a little research into who deployed the code, why, and who has access to the resulting data.

One ObservePoint customer was able to identify such an issue: "During one of our site scans we discovered that one of our third-party advertising partners was dropping a commonly used competitive analysis solution's tags on our site without our knowledge. This was very much a problem since the solution in question sells data to our competitors and, thanks to our advertising partner, they now had direct access to our data." Armed with his site audit results, this person was able to clarify for the advertising partner that the use of this solution was disallowed and the offending code was quickly removed.

This example demonstrates an important aspect of modern web design – there are an increasing number of advertising, targeting, and optimization solutions out there that are essentially tag containers that, once deployed to the site, are able to deploy additional

technology and data collectors without the knowledge of the site's owners and operators.

Even if you are keeping a careful eye on your site, given that some of these technologies are surreptitiously deployed, you may overlook problematic exposure of confidential data to systems outside of your control. Regular monitoring and auditing can expose rogue data collectors, and we recommend discussing the idea of data leakage with your vendor to ascertain exactly how they will help you prevent leaks from occurring.

CONCLUSION

As businesses increasingly shift online and as consumers continue to show preference for whichever channels are most convenient to meet their needs, the value of digital data of data only becomes more important. To this end, we sincerely hope that the tips we've provided are helpful in your efforts to build a better, more trusted digital measurement, analysis, and optimization practice within your business. Having better knowledge of the challenges and opportunities afforded to your business offers a clear path for improving the overall quality of your digitally collected data.

One thing to keep in mind: Managing and maintaining your digital data is not easy. We have provided the tips in this document, and published our previous work with ObservePoint, in an effort to clarify the requirements for any business so that the process becomes practical enough to deliver value commensurate with the effort. After reading these white papers and discussing their ramifications both internally and externally with your analytics solution providers, you should see a dramatic improvement in the quality, utility, and value of all of your digital measurement and analysis efforts across your business.

We welcome your thoughts, comments, and observations.



ABOUT THE AUTHOR

Eric T. Peterson, CEO and Principal Consultant at Web Analytics Demystified, has worked in web analytics since the late 1990s in a variety of roles including practitioner, consultant, and analyst for several market-leading companies. He is the author of three best-selling books on the subject, *Web Analytics Demystified*, *Website Measurement Hacks*, and *The Big Book of Key Performance Indicators*, as well as one of the most popular web analytics

bloggers at www.webanalyticsdemystified.com.

Mr. Peterson has committed much of his life to the betterment of the web analytics community, so much so that Jim Sterne, President and co-founder of the Web Analytics Association says “Eric’s leadership in the industry is unparalleled, his devotion to the community is legendary and his years of experience translate immediately into strategic and tactical competitive advantage for everybody who works with him.”

ABOUT WEB ANALYTICS DEMYSTIFIED

Web Analytics Demystified, founded in 2007 by internationally known author and former Jupiter Research analyst Eric T. Peterson, provides objective strategic guidance to companies striving to realize the full potential of their investment in web analytics. By bridging the gap between measurement technology and business strategy, Web Analytics Demystified has provided guidance to hundreds of companies around the world, including many of the best known retailers, financial services institutions, and media properties on the Internet.

For more information on Eric T. Peterson and Web Analytics Demystified, please visit www.webanalyticsdemystified.com or call (503) 282-2601.

ABOUT OBSERVEPOINT

Every point of data is important. On your website, one data point is one visitor, one person learning about your company, one sale, one more chance to build a relationship. Every point in data should be carefully collected, used, and safeguarded.

ObservePoint helps data-informed companies trust their data through the application of best practices in tag management. ObservePoint pioneered automated web analytics auditing and their worldwide distributed network audits millions of pages every month to report data loss, inflation and leakage to web analytics managers and stakeholders. ObservePoint helps companies serve their customers better - and helps you trust your data.

For more information about ObservePoint or to arrange a pilot for your company, please visit

www.observepoint.com or call (801) 717-9361