GOOGLE ANALYTICS: ANALYZING THE LATEST WAVE OF LEGAL CONCERNS FOR GOOGLE IN THE U.S. AND THE E.U

RAIZEL LIEBLER & KEIDRA CHANEY†

I. INTRODUCTION

Like Microsoft in the 90s, Google has been at the center of much

† Raizel Liebler, Research Services Librarian & Adjunct Professor, John Marshall Law School, J.D., DePaul University; Keidra Chaney, Social Media & Digital Analytics/Web Analytics Consultant, Google Analytics Certification, 2009. The authors would like to thank Ann Bartow, Jessica de Perio Wittman, David L. Schwartz, and Corey Yung for helpful insight, and additional thanks to Teresa Do for research assistance. This article covers developments in Google Analytics through June 2010. Additional developments in this area will be discussed on the authors' website, The Learned Fangirl (http://thelearnedfangirl.com).

high-profile Intellectual Property-related litigation (such as the Google Books Settlement and AdWords litigation) and technology-based privacy concerns (such as de-anonymizing Google search, Google Streetview, and the controversy over Google Buzz).

However, the next wave of concern regarding Google involves web analytics. Web analytics is the measurement, collection, analysis, and reporting of Internet data for the purposes of understanding and optimizing web usage.[1] The concerns of web analytics use touches on issues of online user privacy, government use of personal information, and information on website user activity. The profession of web analytics has formally existed since the early 90s and Google Analytics has been available since 2005. While Google Analytics is not the sole web analytics product on the market, it is widely used by corporate, non-profit, and government organizations. The product has been reported to have a 59% market share among web analytics vendors in a 2008 study.[2]

Web analytics technology has also recently become the focus of government review in both the U.S. and the E.U. In May 2009, the Center for Democracy & Technology (CDT) and the Electronic Frontier Foundation (EFF) released a joint paper, *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites*.[3] In the United States, as part of a larger commitment to a consistent technology policy, in July 2009, the Office of Management and Budget asked for comments regarding web-tracking technologies, such as cookies.[4] In June 2010, in response to the comments, the Office of Management and Budget released two highly influential documents relating to the collection of personally identifiable information through web tracking technologies on government websites.[5] In one of these documents, the government recognizes the clear potential benefits of web measurement and

[1] Web Analytics Association About Us, http://www.webanalyticsassociation.org/?page=aboutus (last visited Aug. 18, 2011).

[2] Stephanie Hamel, *Web Analytics Vendor Shares*, IMMERIA, Jan. 4, 2008, http://blog.immeria.net/2008/01/web-analytics-vendors-market-shares.html.

[3] CTR. FOR DEMOCRACY & TECH. ELEC. FRONTIER FOUND., OPEN RECOMMENDATIONS FOR THE USE OF WEB MEASUREMENT TOOLS ON FEDERAL GOVERNMENT WEB SITES (2009), http://www.cdt.org/files/pdfs/20090512_analytics.pdf.

[4] Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, 74 Fed. Reg. 37,062 (July 27, 2009), *available at* http://edocket.access.gpo.gov/2009/E9-17756.htm.

[5] OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR ONLINE USE OF WEB MEASUREMENT AND CUSTOMIZATION TECHNOLOGIES (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf; OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

customization technologies.[6]

In addition, the E.U. and Germany have been interested in changing the functionality of web analytics software. In October 2009, the European Union's e-Privacy Directive (2002/58/EC) was changed. Now the E.U. requires website users to opt-in to tracking cookies.[7] The edits change Article 5(3), and now requires member states to make sure "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information."[8] This change will make keeping web statistics, as through Google Analytics, more difficult. A user-based browser opt-in for use of Google Analytics at least makes the possibility of European use of Google Analytics possible. As of June 2010, the number of E.U. countries that have implemented the amended e-Privacy Directive are sparse – only Finland and Sweden are in compliance.

Web analytics programs such as Google Analytics will continue to evolve, but we hope this article will serve as a starting point for understanding both this Google product and online data collection. This article will discuss developments regarding Google Analytics and similar products through June 2010.

In this article, we discuss web analytics and Google Analytics (Part II); the privacy and legal issues involved with web analytics (Part III); the approaches taken by various countries to the privacy and technology issues involved, including the United States (especially for government websites), the European Union, and Germany (Part IV).

Finally, we conclude with our predictions for the future of Google analytics from July 2010 onward (Part V), stating that Google Analytics will continue to raise privacy concerns, especially within Europe, considering those online users do not generally take additional steps to make their online behavior anonymous. In the United States, the potential for cookies that cannot be erased by users will raise the ire of users, government regulators, and legislators and has the potential for creating regulations that will finally directly limit the use of analytics programs, such as Google Analytics.

---

6 *See, e.g.*, OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR ONLINE USE OF WEB MEASUREMENT AND CUSTOMIZATION TECHNOLOGIES; OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS.

7 Council Directive 2009/136, 2009 O.J. (L337) 11 (EC) (amending Council Directive 2002/58), *available at* http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf.

8 *Id.*

II. WEB ANALYTICS

A. What is web analytics?

The Web Analytics Association (WAA), the worldwide professional organization for web analytics, defines web analytics as "the measurement, collection, analysis and reporting of Internet data for the purposes of understanding and optimizing web usage."[9]

Web analytics involves the collection and measurement of various forms of online user data, and is traditionally used as a tool for market researchers and web professionals to measure the effectiveness of website communication. As Internet-based transactions have become a major source of revenue for companies large and small, online marketing and web communication has evolved to become more of a priority for marketing departments. By measuring and optimizing users online experiences, companies can better target and serve users. Web analytics commonly provides information on online user activity, including: web page views, number of visitors, visitor location, and referring websites. This information is then used by marketers to evaluate the effectiveness of website content.

The WAA cites the 1993 founding of web analytics software company WebTrends as the formal beginning of web analytics as an industry and a profession. In subsequent years, the founding of web analytics software companies, including: Omniture and WebSideStory, created new avenues for industry competition and prompted additional methods of data collection.[10]

There are two primary methods of data collection used by web analytics software to track user sessions on a website:

1. *Logfile analysis*. This method uses the log files stored on a website server to collect information on users' IP addresses, date/time information, and referring websites (websites that users started from to get to their present website, such as a Google Search page). A number of open source web analytics tools employ this method.

2. *Page tagging.* This method involves placing Javascript code on a webpage to notify a third-party server whenever a page is loaded in a browser, such as Microsoft Internet Explorer or Mozilla Firefox. This method is employed by Google Analytics.

Cookies, a data collection method used by most analytics software companies, tracks user sessions by placing a small piece of text onto a

9 Web Analytics Association, *supra* note 1.

10 Web Analytics Association, *supra* note 1.

user's computer when a browser loads. The use of cookies by analytics vendors, including Google Analytics, will be discussed in greater detail further in this article.

B. Cookies

An http cookie is a file that is placed on a user's computer hard disk by a web server when a user loads a webpage on their browser. Lou Montulli, an engineer at computer company Netscape, as a way to save, track, and differentiate online transactions, invented cookies in 1994.[11] Cookies are commonly employed by web servers to track and authenticate detailed information about online users based on identifying the specific computer and browser combination of the user. First-party cookies are issued by the same website domain being visited. They are commonly used by e-commerce businesses, such as Amazon.com, for user identification.

Third-party cookies are issued to track user activity among multiple websites. E-commerce companies for targeted online advertising, based on clickstream behavior, commonly use third-party cookies. While most analytics companies for data collection, including Google Analytics, use cookies, privacy concerns have prompted some users to delete cookies from their computers after use. According to a 2007 report from web analytics firm Comscore, 3 out of 10 Internet users regularly delete cookies from their computers.[12]

While cookie technology is not intended to violate consumer privacy by design, there have been instances of companies using this technology maliciously. From 2002 to 2003, thirteen lawsuits were filed against New York advertising firm, DoubleClick Inc., alleging that the company used cookies to track user behavior without obtaining clear and proper consent from users.[13]

The potential misuse of cookies in online marketing has long been a point of controversy for privacy advocates and a source of confusion among some online consumers and web-marketing practitioners. A 2006 study on consumer understanding of cookie technology showed that users remain unclear about how cookies technology is used by websites; the advantages and disadvantages of use; and the differences between cookies, viruses, and malware.[14]

---

11 Lou Montulli, http://www.montulli.org/lou (last visited Nov. 1, 2011).

12 Press Release, Comscore, Cookie-Based Counting Overstates Size of Web Site Audiences (Apr. 16, 2007), *available at* http://www.comscore.com/Press_Events/Press_Releases/2007/04/comScore_Cookie_Deletion_Report.

13 Brian Sullivan, *Privacy groups debate DoubleClick settlement*, CNN, May 24, 2002, http://archives.cnn.com/2002/TECH/internet/05/24/doubleclick.settlement.idg/.

14 FARAH AL SHAAR, VICKI HA, LINA HDEIB, KORI INKPEN, CHI, AN EXAMINATION OF

Both the Electronic Privacy Information Center (EFF) and the Better Business Bureau have worked to educate consumers on the use of cookies by e-commerce and marketing companies and the consumers' options in maintaining online privacy.[15]

C. Do Government Websites Need Web Analytics?

Web measurement provides federal website managers with valuable data about the usage and effectiveness of their websites. Whereas corporate websites use commercial metrics, such as sales, to determine the success of their websites, the vast majority of government websites do not aim to make a profit. Thus, federal website managers utilize other metrics to measure a return on investment in their sites. Web measurement tools provide these website managers with the capacity to prove that their sites are achieving a certain level of user traffic and participation, which is vital to securing additional funding to support increased transparency and more services on agency sites. In essence, website managers need to be able to measure the success of their sites in order to justify additional spending on additional improvements.[16]

D. Google Analytics

In 2005, Google acquired Urchin, an enterprise web analytics software provider, and Google began offering a modified version of Urchin's software for free. Offering a free analytics program was previously unheard of in the web analytics industry. Until this point, web analytics vendors charged hundreds or thousands of dollars for their software. By offering comparatively sophisticated software to companies for free, Google cut into the market of enterprise-level web analytics vendors, including Omniture and WebTrends, and created new markets of small business and non-profits that would otherwise not have the budget for such software. According to a study by online analytics expert Stephane Hamel, as of 2009, Google Analytics had 59% of overall web analytics market share.[17] A licensed version of the Urchin software is still available for purchase through Google.

The market viability of Google Analytics has also prompted a rise in

USER PERCEPTION AND MISCONCEPTION OF INTERNET, http://portal.acm.org/ft_gateway.cfm?id=1125615
&type=pdf&coll=GUIDE&dl=GUIDE&CFID=82274247&CFTOKEN=87863850.

15 Better Business Bureau, *Understanding Cookies*, BBB ONLINE, http://www.bbbonline.org/understandingprivacy/toolbox/cookies.asp.

16 Ctr. for Democracy & Tech. & Elec. Frontier Found., *supra* note 3, at 8.

17 Hamel, *supra* note 2.

similar open source analytics software options, including Mint Web Analytics, Clicky Web Analytics, and Piwik Web Analytics. Google Analytics (GA) collects data through a combination of first-party cookies and javascript page tagging. GA does not collect personally identifiable information but does log user activity and identify unique visitors through the use of several types of cookies. The two most commonly referred to are:

> Session based cookies are executed when a user views a page on a site. Google Analytics Javascript code attempts to update this cookie. If no cookie is found, a new one is written and a new session is established. Session based cookies are updated to expire in 30 minutes, so a single session is logged as a 30-minute interval.
>
> Persistent cookies are used to identify a unique visitor to a website, this cookie is written to the browser upon a users' first visit to your a particular web browser. This cookie is stamped with a unique user ID and updated to expire in 2 years, so that returning visitors to a web site can be identified.[18]

Google employs persistent cookies for many of its services, including Gmail, to authenticate users. Privacy advocates have criticized this policy for the potential of leaving personal user data exposed to hackers and other security vulnerabilities.[19]

Also, the use of Google Analytics for government websites was historically delayed due to Google's use of persistent cookies, based on a policy issued by memorandum M-00-13 of the Federal Office of Management and Budget (OMB):

> Particular privacy concerns may be raised when uses of web technology can track the activities of users over time and across different web

[18] *Cookies & Google Analytics*, http://code.google.com/apis/analytics/docs/concepts/gaConceptsCookies.html (last visited Nov. 2, 2011).

[19] Liam Tung, *Gmail cookie vulnerability exposes user's privacy*, CNET, Sept. 27, 2007, http://news.cnet.com/Gmail-cookie-vulnerability-exposes-users-privacy/2100-1002_3-6210353.htm.

> sites. These concerns are especially great where individuals who have come to government web sites do not have clear and conspicuous notice of any such tracking activities.[20]

The government information issues will be discussed in section B below.

Unlike many of the Google-branded products that have prompted criticism of the company, such as Streetview and Google Books, Google Analytics is installed within a website's source code where the default is to not have a public notification of this product's use.

E. Specific concerns with analytics products

Web managers do not need all of the personally identifiable information that is collected by Google Analytics for commercial use. If there is no user transaction, such as a sale, then the collected individual information may not immediately benefit the user, though the user behavior information that is collected may be used to optimize the website for improved user experience in the future. As one commenter states:

> [for the] Google Analytics program, only some of the information collected is actually necessary for the program's operation. Interestingly enough, it turns out that even privacy-sensitive e-consumers appreciate the value these services provide and concede that most of the [personally identifying information] collection is a small price to pay in return for the benefits provided.[21]

Google Analytics is not generally used to identify individual users, like a "digital dossier" of information, but it could potentially be used as a tool to do so.[22] The ability to create a digital dossier using an analytics program increases if the user of the website has created an account or if the

---

[20] OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: PRIVACY POLICIES AND DATA COLLECTION ON FEDERAL WEB SITES (June 22, 2000), *available at* http://www.whitehouse.gov/omb/memoranda_m00-13/.

[21] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 571-72 (2007)

[22] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1-10 (Jack M. Balkin & Beth Simone Noveck eds., 2004) (created the term "digital dossiers" to describe the intersection of information collection and privacy)

website has placed a cookie on the browser. Some analytics software programs such as Clicky make it possible to individually track an individual online session, using a combination of personalized online information, including an IP address and URL.

As of June 2010, Google is working on methods for web developers and administrators in Europe, as well as government agencies, to address the issues discussed in detail below. There has been a major change in recent months that reflects both Google's acknowledgement of the privacy standards in Europe and the United States government, and a financial need to retain the majority market share.

According to a statement of the Google Analytics blog by Amy Chang, Group Product Manager, Google Analytics:

> As an enterprise-class web analytics solution, Google Analytics not only provides site owners with information on their website traffic and marketing effectiveness, it also does so with high regard for protecting user data privacy. Over the past year, we have been exploring ways to offer users more choice on how their data is collected by Google Analytics. We concluded that the best approach would be to develop a global browser based plug-in to allow users to opt out of being tracked by Google Analytics.[23]

While this browser opt-in is situated as a great step forward, it is not likely to be used much. Most people use the default web browser that is pre-installed on their computer or mobile device without making changes, such as limiting the collection of cookies. This allows Google to claim that it has made changes that will protect users, while not having to change the true backend aspect of Google Analytics.

Also, how would one characterize this change? Is it an opt-out (of tracking by Google Analytics)? Or is it an opt-in (because it is an addition to browsers that users have to specifically add)? Perhaps the best way to characterize this option is opting-in to opting-out!

[23] Posting of Amy Chang to Google Analytics Blog, http://analytics.blogspot.com/2010/03/more-choice-for-users-browser-based-opt.html (Mar. 18, 2010, 11:22 EST).

III. WHAT ARE THE GENERALIZED PRIVACY AND LEGAL ISSUES INVOLVED WITH GOOGLE ANALYTICS?

The issue of privacy is very large, but even larger when it comes to information disclosure online. Considering others have discussed many of these issues in detail, we will limit our discussion to those issues that specifically relate to Google Analytics.

According to Bennett and Raab, there are generalized principles involving the use of information that are contained in the laws and treaties covering the United States, Canada, and the European Union.

The principles or norms for the "collection, retention, use, and disclosure of personal information" for any organization—whether public or private—and thereby including anybody that would use Google Analytics:

> must be accountable for all the personal information in its possession; should identify the purposes for which information is processed at or before the time of collection; should only collect personal information with the knowledge and consent of the individual (except under specified circumstances); should not use or disclose personal information for purposes other than those identified, except with the consent of the individual (the finality principle); should retain information only as long as necessary; should ensure that personal information is kept accurate, complete, and up-to-date; should protect personal information with appropriate security safeguards; should be open about its policies and practices and maintain no secret information systems; should allow data subjects access to their personal information, with an ability to amend it if it is inaccurate, incomplete, or obsolete.[24]

[24] COLIN J. BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 12-13 (Ashgate Publ'g Ltd. 2006) (2003); *see also* LEE BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 57 (P. Brent Hugenholtz et al. eds., Kluwer Law Int'l 2002) (describing these same principles as "fair and lawful processing," "minimality," "purpose specification," "information quality," "data subject participation and control," "disclosure limitation," "information security, and "sensitivity").

Expanding the analysis beyond laws and policies, the real world implications of use of web analytics programs is based on how people actually work with their own personally identifiable information and the information of others. While laws and policies are concerned with personal information disclosure and retention of personal information (as well as disagreements about what is "personal information"), people make choices to share information, both knowingly and unknowingly. However, most users don't actively make efforts towards protecting their privacy by changing browser settings, they use whatever default settings are selected for the browser out of the box. If it takes extra effort to know that most websites, especially commercial ones, use analytics, then the default of having information shared will continue.

Over ten years ago, Laurence Lessig, in *Code*, said the following about the additional step for users in blocking cookies, an essential aspect integrated in analytics programs.

> With one click, you can disable the deposit of cookies [b]ut this privacy comes at a cost. Users who choose this option are either unable to use [websites] where cookies are required or forced constantly to choose whether a cookie will be deposited. Most find the hassle too great and simply accept cookies on their machine. [25]

More recently in 2006, in *Code: 2.0*, Lessig describes the ubiquity of tracking services online and how the public generally does not care about this sharing. "The traceability of IP addresses and cookies is the default on the Internet now. Again, steps can be taken to avoid this traceability, but the vast majority of us don't take them. Fortunately, for society and for most of us, what we do [online] doesn't really concern anyone."[26] But what counts as "concerning" varies based on the viewpoint of the one viewing the information, and it is likely that some people do not know about the types of information shared through analytics programs or that they even exist.

Rather, it is likely that very few people will continue to take what Laurence Lessig calls "extraordinary steps" to protect their information:

> Unless you've taken extraordinary steps—installing privacy software on your computer,

[25] LAURENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 41-42 (Basic Books 1999).

[26] LAWRENCE LESSIG, CODE: VERSION 2.0 49 (Basic Books 2006).

> or disabling cookies, etc.—there's no reason you should expect that the fact that you visited certain sites, or ran certain searches, isn't knowable by someone. It is. The layers of technology designed to identify "the customer [or user]" have produced endless layers of data that can be traced back to you.[27]

That is not to say that those that want to prevent sharing of their information through web analytics cannot take steps to do so, through deleting cookies and through "anonymous" browser settings.

Generally, people are unaware of the type of information being tracked via cookies online. However, there are relatively simple means of becoming more informed, such as the browser add-on Ghostery. Originally starting as a warning list, Ghostery now is a browser add-on for most frequently used browsers, allowing users to see all of the analytics programs or malware that track user's online information.

Dr. danah boyd has described the means by which people are willing to share their potentially personal information:

> Privacy is about having control over how information flows. It's about being able to understand the social setting in order to behave appropriately. To do so, people must trust their interpretation of the context, including the people in the room and the architecture that defines the setting. When they feel as though control has been taken away from them or when they lack the control they need to do the right thing, they scream privacy foul. . . .
>
> Wanting privacy is not about needing something to hide. It's about wanting to maintain control. Often, privacy isn't about hiding; it's about creating space to open up. If you remember that privacy is about maintaining a sense of control, you can understand why Privacy is Not Dead. [28]

---

27 *Id*. at 203-04.

28 danah boyd, Keynote at SXSW: Making Sense of Privacy and Publicity (Mar. 13, 2010) (transcript available at http://www.danah.org/papers/talks/2010/SXSW2010.html).

Dr. boyd also divides up personal information in a unique way, applicable to how people view most of the information shared via web analytics programs:

> If you've spent any time thinking about privacy, you've probably heard of PII - "Personally Identifiable Information." All too often, we assume that when people make PII available publicly that they don't care about privacy. While some folks are deeply concerned about PII, PII isn't the whole privacy story. What many people are concerned about is PEI - "Personally Embarrassing Information." This is what they're brokering, battling over, and trying to make sense of.[29]

The opt-in versus opt-out issue for information disclosure by users demonstrates Google Analytics's problematic conflation of actual behavior with idealized, legally expected behavior. When people use websites they do not usually read the terms of service. Websites do not open with pop-ups including terms of service that must be accepted before entering the site. Once one has had a website open it is too late to avoid having a cookie or another tracking service.

A 2010 *New York Times* article even disparages the conceptual model of consent for sharing private information with websites:

> One prime candidate for the digital dustbin, it seems, is the current approach to protecting privacy on the Internet. It is an artifact of the 1990s, intended as a light-touch policy to nurture innovation in an emerging industry. And its central concept is "notice and choice," in which Web [sic] sites post notices of their privacy policies and users can then make choices about sites they frequent and the levels of privacy they prefer. [30]

[29] boyd, *supra* note 28.

[30] Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. TIMES, Feb. 27, 2010 at BU4.

IV. APPROACHES TO WEB ANALYTICS AND GOOGLE ANALYTICS

A. Are Web Analytics Being Considered in Discussions of Technology and Privacy?

The analysis of web analytics programs within U.S. law has been minimal thus far. Very few treatises or articles on privacy or technology mention it at all. A typical mention reads much like the one in *Successful Partnering Between Inside and Outside Counsel*: "There are various analytics programs available. For example, Google offers a free program to gather these numbers: Google Analytics**.** While it is capable of complex analyses, its simplest implementation involves only adding a few lines of code to a website's template."[31] There is no mention of privacy concerns or how potential clients might respond to their information being used by the firm that installed Google Analytics on its website.

However, according to our search on Lexis, Westlaw, and other databases, at present, this treatise has the longest mention of web analytics in any legal treatise. [32]

As discussed by others, it is often difficult to determine exactly what laws would directly cover the use of Google Analytics in the United States. A commenter states:

> [i]nvisible third-party services, such as edge caching and visitor tracking [such as Google Analytics] run on thousands of websites, often without visitors' knowledge. For each of these types of services, it is difficult to classify users as customers or subscribers. Thus, it is unclear whether these relationships fall under [Title II of the Stored Communications Act (SCA),

---

31 Louis J. Briskman et al., *Marketing to Potential Corporate Clients*, *in* SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL § 6:16 (2010).

32 *Id*.

The entirety of the section on analytics within this treatise is: "*Analytics*--The raw statistic that 60,000 unique visitors entered a web site in a month is not particularly useful without analysis of the practical implications of the numbers. The numbers provided by analytics packages can allow a site owner to determine what visitors are doing once they enter a site. If a web site is designed and maintained with a clear purpose, then analytics can help its owner determine whether visitors are indeed using the site and the information contained therein for its intended purposes. Getting a visitor to perform a desired action is known as 'conversion.' For example, on a consumer site, a conversion would occur if a customer entered the site, searched for a product, and made a purchase. Determining the success of a web site using conversion rates, however, is challenging for a law firm since clients do not typically purchase legal services online. Instead, a possible conversion may occur if a visitor came to the site, read an article, clicked on the biography of an attorney mentioned therein, and then e-mailed that attorney. More simply, a conversion could occur every time a visitor clicked the link to e-mail an attorney at the firm or accessed a news item or publication."

> which covers communications in electronic storage]'s current framework.[33]

Google Analytics and web analytics have only minimally been mentioned in case law. Google Analytics was mentioned in a case where a Google Analytics contract did not establish minimum personal contacts for jurisdictional purposes:

> [i]f a person's use of Google Analytics–or the Google.com search engine, which has the same forum selection and choice of law clauses–were sufficient to subject her to the jurisdiction of a California court for a dispute that is unrelated to Google, the limits on specific jurisdiction would be meaningless and California courts would be overwhelmed.[34]

Google Analytics has also been mentioned in trade secrets and trademark cases. In a trade secrets case based in California law, the court held that a former employee's unauthorized access to a Google Analytics account did not destroy the trade secret.[35] In *Shoemoney Media Group, Inc. v. Farrell*, the defendant was accused of violating the Lanham Act because he placed a registered trademark in the text of ads on his website; visits to the site by users imputing this registered trademark as a search term were verified by Google Analytics.[36] Other mentions of Google Analytics vary, but none so far relate directly to the legality of aspects of actually using Google Analytics or other web analytics programs. [37]

B. Web Analytics and Government Information

While the issues related to web analytics are broader than government information, most policy concerns and potential changes have been limited

---

33 Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1948-49 (2009).

34 *Life Alert Emergency Response, Inc. v. Lifealert Sec., Inc.*, No. CV 08-3226 AHM, 2008 WL 5412431, at *4 n.2 (C.D. Cal. Dec. 29, 2008).

35 *Vinyl Interactive LLC v. Guarino*, 91 U.S.P.Q.2d 1771 (N.D. Cal. 2009).

36 *Shoemoney Media Group, Inc. v. Farrell*, No. 8:09CV131, 2009 WL 1383281 (D. Neb. May 14, 2009).

37 *See, e.g.*, *Columbia Pictures Indus., Inc. v. Bunnell*, No. CV 06-1093, 2007 WL 4916964 (C.D. Cal. May 7, 2007) (granting plaintiff's motion to compel defendant to produce Google Analytics report); *Coremetrics, Inc. v. Atomic Park.com, LLC*, 370 F. Supp. 2d 1013 (N.D. Cal. 2005) (denying defendant's motion to dismiss where plaintiff is a company that provides web analytics, and defendant is a client who is being sued for breach of contract).

to web analytics regarding government information. It is not surprising that potential changes to information shared on government websites, started with the Obama administration, considering the frequent and effective use of technology during the Obama Presidential campaign, and the Obama Administration's interest in a Chief Technology Officer.

1. Pre-Obama Administration

But a government concern with the type of information that can be tracked via web analytics started in 2000 with the first official full government statement regarding website government data collection and cookies. Also, the use of Google Analytics for government websites was historically delayed due to Google's use of persistent cookies, as mentioned in the *Memorandum for the Heads of Executive Departments and Agencies: Privacy Policies and Data Collection on Federal Web Sites*.[38] There are also additional follow-up letters to clarify the meaning of the official memorandum, although they ultimately hold less force than the memorandum itself. [39]

These statements from 2000, despite not having the imprimatur of being a federal regulation, because it is a document regulating agencies, plays an important role in understanding how federal agencies have been concerned about privacy issues on government websites. The memorandum states not only that privacy policies need to be prominently displayed on government websites, but it also states:

> [p]articular privacy concerns may be raised when uses of web technology can track the activities of users over time and across different web sites. These concerns are especially great where individuals who have come to government web sites do not have clear and conspicuous notice of any such tracking activities. 'Cookies'—small bits of software that are placed on a web user's hard drive—are a principal example of current web technology that can be used in this wayFalse[A]gencies

[38] *Cookies & Google Analytics*, *supra* note 18.

[39] Letter from Roger W. Baker, CIO, Dep't of Commerce, to John T. Spotila, Chair, CIO Council, Ofc. of Info. & Regulatory Affairs (July 28, 2000), *available at* http://www.whitehouse.gov/omb/inforeg_cookies_letter72800/; Letter from John T. Spotila, Adm'r, Ofc. of Info. & Regulatory Affairs, to Roger Baker, Chief Info. Officer, (Sept. 5, 2000), *available at* http://www.whitehouse.gov/omb/inforeg_cookies_letter90500/; Letter from Roger Baker to John Spotila on Fed. agency use of Web cookies (July 28, 2000), *available at* http://www.whitehouse.gov/omb/inforeg_cookies_letter72800.

> could only use 'cookies' or other automatic means of collecting information if they gave clear notice of those activities.
>
> Because of the unique laws and traditions about government access to citizens' personal information, the presumption should be that 'cookies' will not be used at Federal web sites. Under this new Federal policy, 'cookies' should not be used at Federal web sites, or by contractors when operating web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from 'cookies'; and personal approval by the head of the agency. In addition, it is federal policy that all Federal web sites and contractors when operating on behalf of agencies shall comply with the standards set forth in the Children's Online Privacy Protection Act of 1998 with respect to the collection of personal information online at web sites directed to children.[40]

Note that there is no specific mention of web analytics programs within this memorandum. Instead, the focus is solely on the use of cookies. While this memorandum strongly discouraged the use of web analytics by preventing the use of persistent cookies, those who wanted to use web analytics programs were stymied.

The next step by the federal government regarding the use of web analytics took place in 2003, where the prevention of web analytics by government agencies was further implemented, once again, based around preventing the use of persistent cookies or any other technology that track visitors beyond a single session.[41]

Therefore, between 2003 and 2010, federal websites were prohibited from using persistent tracking technologies, as used by web analytics

---

40 *Cookies & Google Analytics*, *supra* note 18.

41 Joshua Bolten, Memorandum for Heads of Executive Departments and Agencies: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda_m03-22.

programs, like Google Analytics, unless the agency head gives permission after demonstrating compelling need and does all of the following:

- includes within the privacy policy "the nature of the information collected; the purpose and use for the information; whether and to whom the information will be disclosed; and the privacy safeguards applied to the information collected";
- there is a "compelling need" to use "persistent tracking technology"; and
- the creation and public disclosure of privacy safeguards for the information collected (called a Privacy Impact Assessment).[42]

2. Recommendations for Change

Based on the likely difficulty of receiving agency director approval, this means that in effect, government agencies could not use Google Analytics. In response to many years of web analytics not being used on government websites, in May 2009, the Center for Democracy & Technology (CDT) and the Electronic Frontier Foundation (EFF) released a joint paper, *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites*.[43]

Their recommendations include requiring the following of any government agency that uses web measurement, such as Google Analytics: "[u]se data only for measurement . . . . [p]rominently disclose [the privacy policy]. . . . [o]ffer choice [an opt-out choice]. . . . [l]imit data retention [regarding individuals to 90 days]. . . . [l]imit cross-session measurement [and]. . . . [o]btain third-party verification. [44]

The recommendations also "suggest that the current federal policy on the use of persistent tracking technologies be updated to allow Web [sic] managers to use persistent tracking technologies for Web [sic] measurement purposes if and only if the above six conditions . . . ."[45]

One of the issues discussed in the recommendations was the idea of an opt-out for tracking via web analytics. This idea is similar to Google's opt-in or opt-out browser plug-in, though the recommendations foresee even more transparency when it comes to showing visitors to government websites whether their information is being compiled.

42 *Id.;* 14 Elec. Com. & L. Rep. (BNA) 115 (Jan. 28, 2009).

43 Ctr. for Democracy & Tech. & the Elec. Frontier Found., *supra* note 16.

44 *Id.* at 2.

45 *Id.*

> Site visitors should be offered choices about having their data collected for cross-session measurement. The choice mechanism(s) and the visitor's choice status should be clearly visible on every page of the agency site. For example, an agency could provide a simple on/off switch on each page of its site, with one option highlighted to indicate the user's current status and the other option provided as a link to allow the user to switch his or her status at any time.
>
> Site visitors should be given detailed information about how the choice mechanisms work and other means to stop persistent tracking, such as links to descriptions about how to use cookie blocking and deletion tools.[46]

3. Obama Administration Policy Regarding Web Analytics

Generally, the Obama Administration's pledge for open government has included concerns regarding privacy protections within technology.[47] Also, the federal cookie policy was mentioned in the press release that announced the Open Government Initiative.[48] The issue of cookies and other tracking systems has frequently been mentioned on the official White House blog. For example, the Federal Register comment period on the proposed changes was promoted on the White House blog,[49] and on the same day there was a guest post by Bev Godwin, Executive Sponsor of the Federal Web Managers Council and Director of USA.gov, discussing the need for a change in policy, stating:

> [t]he 'cookie policy' has been the topic of frequent discussion among federal web

46 *Id.* at 11-12.

47 The White House, Open Government Initiative, http://www.whitehouse.gov/open (last visited Nov. 5, 2011).

48 Press Release, The White House, Administration Launches Comprehensive Open Government Plan (Dec. 8, 2009), *available at* http://www.whitehouse.gov/the-press-office/administration-launches-comprehensive-open-government-plan.

49 Posting of Michael Fitzpatrick & Vivek Kundra to the White House blog, http://www.whitehouse.gov/blog/2009/07/24/federal-websites-cookie-policy (July 24, 2009, 10:25 EST).

> managers over the years as we strive to provide the best customer service online while protecting individual privacy. We want to use cookies for good, not evil. As part of the Obama Administration's efforts to create a more open and innovative government, OMB wants public input to determine how to best update the cookie policy to meet these goals.[50]

Interestingly, one such agency that did waive the ban on tracking before the 2010 OMB change was Whitehouse.gov.[51] The Whitehouse.gov privacy policy in May 2010 states:

> [c]ookies: A cookie is a tiny piece of data stored by a user's browser that helps a web site or service recognize that user's unique computer. You can remove or block cookies by changing the settings of your browser.
>
> Session specific cookies may be used on WhiteHouse.gov to improve the user experience and for basic web metrics. These cookies expire in a very short time frame or when a browser window closes and are permitted by current federal guidelines.
>
> The federal government has guidelines for the use of persistent cookies. The goals of the guidelines are to enable the useful functioning of federal websites while protecting individual privacy.
>
> For videos that are visible on WhiteHouse.gov, a 'persistent cookie' is set by third party providers when you click to play a video. (. . . *We intend, however, to fully enforce the above provisions as soon as possible. If you are experiencing any difficulties, please contact*

[50] Posting of Bev Godwin to the White House blog, http://www.whitehouse.gov/blog/2009/07/24/cookies-anyone-http-kind (July 24, 2009, 14:07 EST).

[51] 14 Elec. Com. & L. Rep. (BNA) 115 (Jan. 28, 2009).

us.)

> This persistent cookie is used by some third party providers to help maintain the integrity of video statistics. A waiver has been issued by the White House Counsel's office to allow for the use of this persistent cookie.[52]

Two White House blog posts are indicative of the impact of the Obama administration and agencies behind the proposed changes. The change in cookie policy is discussed as part of the way the administration is incorporating more Web 2.0 technologies by "updating existing practices and how these tools can be used to break down barriers to communication and information."[53]

They state:

> [i]n the nine years since [the federal cookie policy] was put in place, website cookies have become more mainstream as users want sites to recognize their preferences or keep track of the items in their online shopping carts. We've heard a lot of feedback on this area. One person put it all together. "Persistent cookies are very useful as an indirect feedback mechanism for measuring effectiveness of government web sites . . . Cookies allow a greater level of accuracy in measuring unique visitors . . . Being able to look at returning visitors allows us to see what content is important to our citizens. We can use that data to improve the content and navigation of our sitesFalse There is a tough balance to find between citizen privacy and the benefits of persistent cookies, and we would welcome your thoughts on how

52 The White House, Our Online Privacy Policy, http://www.whitehouse.gov/privacy/ (last visited Nov. 5, 2011) ("Browser information collected on the web site: We log IP addresses, which are the locations of computers or networks on the Internet, and analyze them in order to improve the value of our site. We also collect aggregate numbers of page hits in order to track the popularity of certain pages and improve the value of our site. We do not gather, request, record, require, collect or track any Internet users' Personal Information through these processes.").

53 Fitzpatrick & Kundra, *supra* note 49.

best to strike it.[54]

The proposed change was also discussed in detail on the White House blog after the comment period opened, with additional discussion of the Obama administration's reasoning for the proposed changes, including a post by Michael Fitzpatrick, the Associate Administrator, OMB Office of Information and Regulatory Affairs and Vivek Kundra, Federal CIO. As demonstrated through this blog post, the administration wants this policy to change greatly, allowing government websites to follow the overall web standards that are now acceptable, including the use of web analytics, to help government agencies analyze how to better serve the public. They state:

> [o]ur main goal in revisiting the ban on using persistent cookies on Federal websites is to bring the federal government into the 21st century. Consistent with this Administration's commitment to making government more open and participatory, we want federal agencies to be able to provide the same user-friendly, dynamic, and citizen-centric websites that people have grown accustomed to using when they shop or get news online or communicate through social media networks, while also protecting people's privacy.[55]
>
> It is clear that protecting the privacy of citizens who visit government websites must be one of the top considerations in any new policy. This is why we've taken such a cautious approach going forward and why we felt it so important to get feedback and hear from people on this. While we wanted to get people's ideas for improving our policy, we also needed to hear any concerns so that we could understand better where potential pitfalls might lie.
>
> This privacy issue has recently received some attention in the media. We want to make it clear that the current policy on Federal

54 *Id.*
55 *Id.*

> agencies' use of cookies has not changed. Moreover, the policy won't change until we've read the public comments that have been submitted to ensure that we're considering all sides of the issue and are addressing privacy concerns appropriately.[56]
>
> We would also like to take this opportunity to address a potential misperception. Some articles have hinted that the government is creating special exemptions for third-parties from existing privacy rules, with the result that there wouldn't be adequate protection of people's personal information. This is not true. The current policy in place on persistent cookies continues to apply to all Federal agencies and to those agencies' use of third-party applications, whenever personal information is collected on the agency's behalf.
>
> Once again, we appreciate everyone's contribution to this topic and are grateful for the time and energy devoted by those who provided such useful insight on this issue.[57]

This language mirrors that of the *Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites*:

> [w]eb measurement holds much promise for federal Web managers seeking to optimize user experiences on their Web sites. The insight that Web measurement provides could be a crucial tool for federal agencies as they seek to justify increased investments in their Web sites, which in turn could lead to increased government transparency and services on the Web.[58]

In response to the CDT & EFF joint recommendations and the concerns of others, in July 2009, the Office of Management and Budget

56 *Id.*
57 *Id.*
58 Ctr. for Democracy & Tech. & Elec. Frontier Found., *supra* note 3.

asked for comments through official rulemaking procedures regarding web tracking services, like cookies. [59]

The Federal Register statement stated:

> [d]uring the past nine years (since a ban on tracking applications federal agency websites went into effect), web tracking technologies have become a staple on most commercial web sites with widespread public acceptance of their use. Technologies such as persistent cookies enable Web sites to remember a visitor's preferences and settings, allowing for a more personalized, user-friendly experience.[60]

This proposal would allow federal agencies to use online tracking technologies on their websites, after posting "clear and conspicuous" notifications and opt-outs. The plan would also include a three-tiered system for notifications based on the level of potentially identifying information retained.[61]

Under the OMB's proposed policy:

> any federal agency using online tracking technologies would be required to: adhere to all existing laws and policies governing data collection, use, retention, and safeguards; post clear and conspicuous notices regarding use of tracking technologies; provide a clear and understandable means for a user to opt-out; and not discriminate, in terms of information access, against users who opt-out.[62]

The OMB has also suggested a three-tiered system, for the types of information that would likely be used in web analytics programs and would be subject to additional restrictions. The first tier would be single-session cookies that track users over a single session. The second would include "multi-session technologies for use in web analytics [that] track users over multiple sessions purely to gather data to analyze Web [sic] traffic

---

59 Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, *supra* note 4.

60 *Id*. at 37,063.

61 *Id.*

62 *Id.*

statistics."[63] The third tier would include "multi-session technologies for use as persistent identifiers [that] track users over multiple visits with the intent of remembering data, settings, or preferences unique to that visitor for purposes beyond what is needed for Web [sic] analytics ."[64] The idea of three tiers for the collection of information from the public was integrated into the present policy, as discussed below.

The official comments to the proposal were mixed, with government agencies, such as the Internal Revenue Service, the National Institutes of Health, and the Department of Energy, supporting the changes. However, several advocacy groups did not support the proposed changes, including: the Center for Digital Democracy, the Electronic Privacy Information Center, and the American Civil Liberties Union. Earlier, other groups stated their objections to the proposed changes, including: Lillie Coney, associate director of the Electronic Privacy Information Center. She stated that "[p]ersistent cookies are not necessary for Web 2.0 services to function. [] Commercial marketers use cookies to track online activity of users to profile consumers without their knowledge. Government does not need to track users of agency information to provide services."

Some of the comments were very interesting with their suggestions that an overall technology policy needs to be created to understand the larger issues involved. For example, the U.S. Public Policy Council of the Association for Computing Machinery recommends:

> that any new policy not be limited to today's technologies, but be written to encompass tracking technologies generally. . . .Tracking should be done openly and transparently. Until a newer, not yet envisioned technology [that will enable users to detect other tracking mechanisms] is available, tracking across websites should be limited to HTTP cookies.[65]

The supporters of an overall technology policy, included industry groups like The Future of Privacy Forum, which stated:

> [p]ersonalizing site content for users who wish

---

63 *Id.*

64 *Id.*

65 U.S. PUB. POLICY COUNCIL OF THE ASS'N FOR COMPUTING MACH., COMMENTS ON PROPOSED REVISION OF THE POLICY ON WEB TRACKING TECHNOLOGIES FOR FEDERAL WEB SITES (Aug. 10, 2009), http://usacm.acm.org/privsec/details.cfm?type=Testimony&id=13&cat=7&Privacy%20and%20Security.

> to have a setting remembered, enabling long term shopping carts and capturing analytics information over time to improve[ ] site usage are key to providing the public the best possible web experience. . . . We are deeply cognizant of the privacy issues raised by the use of cookies, when the public sector is involved.[66]

In response to the Federal Register, the Office of Management and Budget released two sister Memoranda on June 25, 2010 – *Guidance for Agency Use of Third-Party Websites and Applications* and *Guidance for Online Use of Web Measurement and Customization Technologies*.[67] Both of these Memoranda do not specifically discuss Google Analytics by name, but they do have implications for its use. There are sections of this new policy that now specifically allow for use of web analytics, as long as privacy protections are in place.

In the *Guidance for Online Use of Web Measurement and Customization Technologies Memoranda*, the government recognizes the "clear [] potential benefits of web measurement and customization technologies."[68] To balance the benefits, the goal of the new procedures is:

> to respect and safeguard the privacy of the American public while also increasing the Federal Government's ability to serve the public by improving and modernizing its activities online. Any use of such technologies must be respectful of privacy, open, and transparent, and solely for the purposes of improving the Federal Government's services and activities online.[69]

---

66 Jules Polonetsky & Christopher Wolf, *FPF's Reply Comments to the Federal Websites Cookie Policy*, FUTURE OF PRIVACY FORUM, Aug. 08, 2010, http://www.futureofprivacy.org/2009/08/10/fpfs-reply-comments-to-the-federal-websites-cookie-policy/.

67 OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR ONLINE USE OF WEB MEASUREMENT AND CUSTOMIZATION TECHNOLOGIES (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf; OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR AGENCY USE OF THIRD-PARTY WEBSITES AND APPLICATIONS (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

68 OFC. OF MGMT. & BUDGET, EXEC. OFFICE. OF THE PRESIDENT, GUIDANCE FOR ONLINE USE OF WEB MEASUREMENT AND CUSTOMIZATION TECHNOLOGIES (June 25, 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

69 *Id*.

The memorandum places the importance of privacy above all possible collection activities: "Any [uses of web measurement technologies, such as web analytics] must not compromise or invade personal privacy. It is important to provide clear, firm, and unambiguous protection against any uses that would compromise or invade personal privacy."[70] The new policy followed the three tiers suggested in the Federal Register, with the first tier regarding a single session, the second tier with multi-session without personally identifiable information, and the third tier with personally indefinable information. Based on most government websites and services provided, only tiers 1 and 2 will likely be used, while tier three requires opt-in to collect data.[71] Therefore, government websites that collect personally identifying information are required to have users opt-in to the collection of their information.

The *Memoranda on the Guidance for Agency Use of Third-Party Websites and Applications* has much less impact on the use of Google Analytics, especially considering its sister memo discusses analytics in greater detail, but it will impact the use of web analytics programs on third-party websites.

While the Federal Trade Commission is conducting hearings and will likely prepare statements and reports in response to the call for legislation regarding online privacy, we fully predict that there will be additional changes in the federal policy towards web analytics specifically, and the collection of cookies generally. We do not expect the changes to be limited to the collection of information on government websites, but instead will reflect of a larger shift in how the federal government views web technology within the Obama administration, as part of the open government "system of transparency, public participation, and collaboration."[72]

C. Non-Government Information in the United States

In the United States, there is no governing body for privacy issues, but it seems as if at least for online privacy, the Federal Trade Commission is slowly becoming the regulatory body for regulating Internet privacy by non-government agencies. The FTC is taking on this role primarily through its consumer protection division. As part of their role, the FTC does not use the type of information that would be used in web analytics, including

70 *Id*.

71 *Id*. at 5.

72 Memorandum on Transparency & Open Gov't, 15 Fed. Reg. 4,685 (Jan. 21, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.

stating on their website, in bold, that: "We do not use persistent cookies." [73]

The FTC has demonstrated its interest in online consumer privacy for over ten years and cookies in *Privacy Online: Fair Information Practices in the Electronic Marketplace*[74] and *Privacy Online: A Report to Congress*.[75] In 2009, the FTC released the *Self-Regulatory Principles for Online Behavioral Advertising*.[76] However, the Federal Trade Commission is poised to adopt tougher approaches to Internet privacy in response to concerns about behavioral advertising and other emerging online industry practices. David Vladeck, director of the FTC's Bureau of Consumer Protection has stated that based on the change in administration, the FTC's goals are to "inject greater transparency, accountability, and consumer control" into online practices.[77]

In 2008, Lydia B. Parnes, the director at the time of the Federal Trade Commission's bureau of consumer protection, said:

> A big question is how much consumers understand the connection between relevant advertising and tracking. If you ask people whether they want to be traced when they are online they generally say they do not. But if you ask them whether they want a free Internet, they say yes. And if you ask them if they want relevant advertising, they say yes.[78]

One large area to watch is how the FTC will respond to its privacy hearings conducted during 2009 and 2010. The FTC's explanation for these hearings stems from the difficulties in understanding online privacy, requiring the government to:

> explore the privacy challenges posed by the

---

[73] *More Information about the FTC's Privacy Practices*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/ftc/privacy_faqs.shtm#what (last visited Nov. 9, 2011).

[74] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[75] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[76] FED. TRADE COMM'N, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.*

[77] *FTC Seen as Moving Toward Major Shift in Online Privacy Policy*, 9 PVLR 155 (2010). .

[78] Posting of Saul Hansell to Bits Blog, http://bits.blogs.nytimes.com/2008/07/21/the-ftcs-bully-pulpit-on-privacy/ (July 21, 2008, 14:14 EST).

> vast array of 21st century technology and business practices that collect and use consumer data. Such practices include social networking, cloud computing, online behavioral advertising, mobile marketing, and the collection and use of information by retailers, data brokers, third-party applications, and other diverse businesses. The goal of the roundtables is to determine how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation.[79]

Technically, the roundtables are not rulemaking, so there will be at least additional guidelines for online behavior proposed, if not legislation. If the FTC does release guidelines, they will likely include references to cookies and web analytics, thus reflecting how the government is planning to collect information on government websites, as discussed above.

At the final hearing, held on March 17, in addition to stating that any new "framework" suggested by the FTC will take time, Jessica Rich, deputy director of Federal Trade Commission Bureau of Consumer Protection, stated:

> [w]e want consumers to have greater control, recognizing that they really don't want to spend time reviewing privacy policies, even short ones. We want to distinguish between data uses that raise privacy concerns . . . and those that really don't and are benign uses, recognizing that privacy preferences are likely to differ across different individuals and that hard lines may be very difficult to draw. We want to accommodate the incredibly diverse business models and privacy concerns that exist today and that may be developed tomorrow: online retailing, data brokering, mobile devices, social networking, cloud computing, behavioral advertising, online medical information, identity management, location based services,

[79] Fed. Trade Comm'n, Exploring Privacy, http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml (last visited Nov. 11, 2011).

> just to name a few . . .
>
> We want a relatively simple framework so everyone can understand the norms and the expectations. Despite the clear shortcomings of privacy policies as a consumer tool they've been instrumental in promoting accountability among businesses, and many of us remember, it wasn't long ago at all when there were no privacy policies and no commitments made about how information would be used, and so we want to preserve and somehow harness that accountability while figuring out a better way to communicate with consumers about the kinds of uses and choices they have. The discussion at these roundtables. . . told us loud and clear that the dominant models really haven't kept pace with the wide range of business models and data practices that are in today's marketplace and which is evolving every day.[80]

What will happen is uncertain, but we at least know that the present standard of the practice of hiding user notification within subpages of websites as the baseline for privacy online will not remain the default privacy standard. At least two members of the Federal Trade Commission, Pamela Jones Harbour and Jon Leibowitz, have released statements saying while they appreciate the present steps taken by the FTC, that they would like further regulation and possibly legislation on the issue.[81] Current FTC Chair Leibowitz stated, "[w]e all agree that consumers don't read privacy policies" and the notice and choice regime hasn't "worked quite as well as we would like."[82] Considering that most users of websites are unaware of web analytics, this is a step in the right direction, in understanding how

---

[80] *Id*.

[81] *See, e.g.*, PAMELA JONES HARBOUR, CONCURRING STATEMENT CONCURRING STATEMENT OF COMMISSIONER PAMELA JONES HARBOUR, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf; JON LEIBOWITZ, CONCURRING STATEMENT OF COMMISSIONER JON LEIBOWITZ, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.

[82] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at FTC Privacy Roundtable 3 (Dec. 7, 2009), *available at*, http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

people actually share information online.

At least one aspect that affects the use of web analytics, like Google Analytics, has been made during the 2009 and 2010 hearings. The FTC rejected the generally accepted industry standard that if a website does not collect personally identifiable information, there are no privacy concerns for users. The FTC is concerned about cookies and they are concerned about tracking IP addresses, so it is possible that analytics programs may be at risk. But this is not likely to be the focus of the FTC privacy-directed actions.

We predict that the FTC will create a broad policy framework designed to provide guidance to both Congress and industry insiders. If the FTC follows the overall direction of the roundtable, the FTC will propose a system designed to promote consumer privacy by simplifying privacy options and increasing the transparency of data collection practices. This solution may follow the three-tiered system as discussed above, with more relaxed policies for analytics that tracks cookies over a single session, and without the ability to connect personally identifiable information. However, if as predicted, Internet users are not able to fully delete cookies even if they use all means at their disposal, the ability for all users of analytics programs to collect relevant statistics may be stymied in the future due to over-regulation in response to a few bad actors.

D. Other Possibilities in the U.S.

There are stirrings about the possibility of increased federal legislation, but as of May 2010 no legislation has been passed.[83] There are murmurings regarding future Congressional actions that will address potential Do-Not-Track legislation and whether it would be feasible to establish an "opt-out" browser feature, which would enable Internet users the option to block data-gathering firms from tracking their on-line activity. Potential legislation will likely limit the collection or storage of data regarding online activity, such as those that can be tracked via cookies and analytics programs.

If legislation is to be forward thinking, it will also require regulation through the FTC, which will require all websites to disclose their data collection practices and how that information is used. Further, an option will be required for consumers, at any point, to opt-out of having their information tracked and collected. In addition, it would allow consumers to access the information collected during their visit to a webpage, as well as the data retention and security policies.

---

[83] Posting of Saul Hansell, to Bits Blog, http://bits.blogs.nytimes.com/2009/03/13/a-call-to-legislate-internet-privacy/ (Mar. 13, 2009, 18:17 EST).

The chance of these legislative changes being enacted soon is slim. As one article states, "federal privacy and data security legislation has largely stalled over the last several years, as privacy advocates press for a legislative solution, while businesses promote self-regulation."[84] However, if there are extensive data leaks or breaches that are publicized, there may be an increased push for a legislative solution, rather than leaving businesses that collect personally identifying information to "regulate" themselves.

V. EUROPEAN UNION

A. European Union Generally

In the EU, there are many different levels of privacy protections, but we will be focusing only on the sections that implicate analytics programs. The EU's approach to data protection has a broad scope for privacy. These laws cover all types of personal data, whether or not it is consumer data. Some of the jurisdictions moving in this direction includes: Argentina, Australia, Canada, Chile, and Japan. One commenter states that considering the number of countries moving in the direction of increased privacy protections, "[i]t would not be surprising if the majority of the developed world—with the notable exception of the United States—ultimately adopts the EU approach."[85]

Some of the EU standards include: the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, based around set principles and guidelines to streamline common privacy standards and to allow for transborder data transfer.[86] The principles include: openness, collection limitation, data quality, purpose specification, use limitation, security safeguards, and individual participation in data protection. The OECD even has a privacy policy statement generator on its website.[87]

While the OECD only includes recommended language, all EU member states must include in national law language based on the directives. Data protection directives in the EU, like 95/46/EC, require each

---

84 Mobile Device Location Data Privacy Debate Considers EU, Industry-Based Approaches, 9 PVLR 444 (Mar. 22, 2010).

85 Ruth Hill Bro, *Life in the Fast Lane: Government Enforcement and the Risks of Privacy Noncompliance*, PRIVACY & SECURITY LAW REPORT, Aug, 6, 2007.

86 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Nov. 11, 2011).

87 OECD Privacy Statement Generator, www.oecd.org/sti/privacygenerator (last visited Nov. 11, 2011).

EU country to implement privacy regulations.[88] Directive 95/46/EC directly implements the OECD principles to harmonize data protection legislation throughout Europe, and specifically states privacy is a human right. Article 7 of 95/46/EC requires data to only be used in limited circumstances after the provider has received consent from the user if data acquisition and usage goes beyond what is necessary for providing the service to the user.[89] The Directive's high standard of data privacy protection and restrictions on transfers of data to countries such as the United States, that may not meet that standard, can limit the flow of personal data, including information related to analytics.

The other major privacy directive at issue with analytics programs in the EU is the European Union Directive on Privacy and Electronic Communication (2002/58/EC). In October 2009, this Directive was modified, requiring website users to opt-in to tracking cookies.[90] Member states have eighteen months to implement this change. As of May 2010, only two countries are in compliance – Finland and Sweden – so the likelihood of all countries being able to comply within the deadline is slim to none.

The modifications change Article 5(3), requiring member states to make sure that "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information."[91]

---

88 Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

89 Council Directive 95/46, art. 7, 1995 O.J. (L 281) 31, 36 (EC) (simplifying what is allowed).

The complete language states "Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent, or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject, or

(d) processing is necessary in order to protect the vital interests of the data subject, or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

90 Council Directive 2009/136, 2009 O.J. (L337) 11 (EC).

91 *Id.*

The amendment adds in the principle of "prior consent" requiring users to "opt-in" to the use of data via cookies. Bridget C. Treacy of Hunton & Williams LLP in London supported this interpretation. She said: "If you look at the original article 5(3) and look at the new article 5(3), there is a clear difference. The old provision requires the notice and right to opt-out, the new provision refers more specifically to consent," which usually needs to be "explicit and fully informed." [92]

This move was strongly opposed by industry groups, who warned about how the change would impact user experience. For example:

> The requirement that companies provide a means for users to give explicit consent to cookies—tracking tools that can be used for behavioral advertising but are also integral to the functioning of many websites—has sparked concerns that web browsing could become cumbersome if sites begin using pop-up windows to get user permission before installing cookies or other technologies.[93]

As another example, Interactive Advertising Bureau Europe (IAB Europe), an online marketing industry group claimed that requiring previous consent for cookies "is well meant, but if you think about how many web sites you visit, it really decreases the user experience False It's not creating more or less rights for users, it's just changing the way the Internet functions." [94]

At least one attorney, Benoit Van Asbroeck of Bird & Bird, Brussels, agrees with this assessment, stating, "cookies are, even when they're legitimate, downloaded immediately [when a user visits a website]. If you need to go first through a process of accepting that . . . [it] will certainly slow down the access to the internet."[95]

This change in the Privacy Directive will complicate keeping web statistics, as through Google Analytics. However, Google's recently announced opt-out or opt-in browser addition might potentially avoid some of the privacy complications, while making data collection less accurate. The edits allow for a specific option to obtain consent from users that is

92 *New EU e-Privacy Laws Spur Confusion Over Consent Requirements for Cookies*, BNA PRIVACY LAW WATCH, Nov. 18, 2009.

93 *Id.*

94 *Online Ad Firms Object to e-Privacy Directive Cookies Plan They Say Will Hamper Web Use*, BNA PRIVACY LAW WATCH, Apr. 3, 2009.

95 *New EU e-Privacy Laws Spur Confusion Over Consent Requirements for Cookies*, BNA PRIVACY LAW WATCH, Nov. 18, 2009.

now embraced by Google to allow users to continue to use Google Analytics with the new opt-in or opt-out browser feature. The new Directive states: "Where it is technically possible and effective, in accordance with the relevant provisions of [EU Data Protection] Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[96]

Would the Google opt-in/opt-out browser option be sufficient, thus acceptable, under this new interpretation? Some commenters think it might not be enough, while others think it may be. The differential seems to be the difference between following the letter of the Directive – where having an opt-out to data collection on a browser may be sufficient versus looking at this through the perspective of user experience.

For example, "it can be argued that where the user has configured the browser in favor of cookies, the user has given consent to the use of cookies. An obvious advantage of this solution is that browsing would not be interrupted by constant questions to consent to the use of cookies." [97]

But others question whether users will actually use browser options, and whether browser options will be sufficient to protect privacy.

An argument can be made:

> that simple browser settings that just allow for a general 'yes or no' decision cannot be regarded specific enough to constitute consent. Even more problematic is the fact that some browsers only allow users to define whether cookies may be stored or not—the user does not have the option to elect whether the cookies may send some or all of the user's stored data back to a remote server once stored on the user's computer or other device.[98]

Also, Nuria Rodriguez, Senior Legal Officer at the European Consumers' Organization "reject[s] that browser settings can be considered

---

[96] Council Directive 2009/xx, http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf.

[97] Lothar Determann, *How to Ask for a Cookie: Information Technology, Data Privacy and Property Law Considerations*, BNA PRIVACY LAW WATCH, Mar. 17, 2010; *see also* Jan Dhont, *New EU e-Privacy Laws Spur Confusion Over Consent Requirements for Cookies*, BNA PRIVACY LAW WATCH, Nov. 18, 2009 (stating "valid consent might be given if browsers by default were set not to accept cookies, and users, given clear information, had to choose from the start whether to accept or partially accept cookies via tick boxes.").

[98] Determann, *supra* note 88 (stating "[a]nother problem with this solution pertains to computers that are used by multiple users. Can it be assumed that every user checks the browser settings prior to surfing the Internet?").

consent. [] Some of them are privacy friendly and some of them are not [considering] at the moment the technologies are not actually allowing the consumers to give meaningful consent."[99]

Therefore, a browser opt-in to allow for analytics use—while at this point is likely legal—does not entirely serve the interests of either (1) those that wish to protect privacy, unless a user has specifically opted in with complete knowledge; or (2) those that wish to have web analytics be as accurate as possible.

But why should companies or organizations located outside of the EU be potentially concerned with using Google Analytics, or even following EU law? Because, like the Internet itself, the EU views its jurisdictional boundaries broadly. One commenter simply puts it; "many European data protection authorities take the position that European privacy laws generally apply worldwide to companies that place cookies on European consumers' computers, thereby entering European territories."[100]

B. Germany

It is perhaps not surprising that Germany is concerned especially about information privacy and data protection considering that, according to Bennett and Raab, even our English term "data protection" derives from the German word Datenschutz.[101]

In 2001, before the birth of complex analytics programs, the National Research Council's Computer Science and Telecommunications Board released their Report, "Global Networks and Local Values: A Comparative Look at Germany and the United States." The report summarized the differences between the two countries approaches to privacy as "to the extent they provide protection, Germany puts greater emphasis on privacy and the United States favors transparency. Germany, and Europe more generally, have comprehensive systems of law and regulation to protect privacy."[102]

In Germany, Directive 95/46/EC has been included in national laws, such as the Federal Data Protection Act Bundesdatenschutzgesetz (known as the BDSG) and the German Telemedia Act (Telemediengesetz –

99 *New EU e-Privacy Laws Spur Confusion Over Consent Requirements for Cookies*, BNA PRIVACY LAW WATCH, Nov. 18, 2009.

100 Determann, *supra* note 88.

101 COLIN J. BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 8 (new ed. 2006).

102 COMPUTER SCI. AND TELECOMM. BD. OF THE NAT'L RESEARCH COUNCIL, GLOBAL NETWORKS AND LOCAL VALUES: A COMPARATIVE LOOK AT GERMANY AND THE UNITED STATES 134 (2001); *see* generally GRAHAM GREENLEAF & JAMES RULE, GERMANY, IN GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION ch. 3 (2008) (detailing the history of German privacy law).

TMG).[103] TMG implements Directive 95/46/EC, and it affects all providers within Germany and over the Internet. Both of these laws require users to give voluntary and informed consent as an opt-in to data collection before personal data is collected, and users must be informed in writing if their data will be transferred outside of the EU.[104] Because the servers for the Google Analytics system are in the United States, use of Google Analytics means that user data is being transferred outside of the EU. As with EU law, providers have to give data subjects (like users of websites) an opportunity, at any point, to change how their data is collected, including deleting or correcting data.[105]

However, users of websites are not usually aware that Google Analytics or other web analytics programs are running and collecting data, let alone thinking about opting in to the data collection. Despite Germany's role in promoting privacy, the use of analytics programs, specifically Google Analytics, are widespread in Germany. According to one article, about 13% of German website owners (sites that end with .de) currently use Google Analytics, including major businesses, media, drug companies and political parties.[106] One German-based study looked at 655,000 German web pages by 14,000 website providers to determine whether "a provider uses a statistics service like Google Analytics and declares this properly."[107]

In a February 18, 2010 statement by Germany's federal data protection agency, German federal data protection officer, Peter Schaar, informed health insurance companies that they are not permitted to use any web analytics program, thus, prompting about 100 health insurance companies to immediately stop using any web analytics program.[108] Using "web analytics software violates German privacy law if the information on an individual's Internet activities is conducted without the subject's consent." [109] Schaar stated: "This result of our surveillance processes clearly show the importance of data protection audits and consultation."[110]

---

103 Felix Wittern, *Germany, in* DATA PROTECTION LAWS OF THE WORLD (Christopher Millard, Mark Ford & Marcus Turle eds., 2009)

104 *Id.*

105 *See, e.g.,* Bundesdatenschutzgesetz [Data Protection Act], Dec. 20, 1990, BGBl. l at § 34 (F.R.G.); Council Directive 95/46/EC, Art. 12; Witten, *supra* note 94.

106 *Datenschützer wollen Einsatz von Analytics verhindern*, ZEIT ONLINE, Nov. 24 2009, *available at* http://www.zeit.de/digital/datenschutz/2009-11/google-analytics-datenschutz.

107 Thorben Burghardt, Klemens Bo¨hm, Erik Buchmann, Ju¨rgen Ku¨hling, & Anastasios Sivridis, *A Study on the Lack of Enforcement of Data Protection Acts*, 2010, *available at* http://dbis.ipd.uni-karlsruhe.de/download/bu09edemocracy.pdf.

108 *EU Data Protection: German DPA: User Must Consent to Web Analysis*, BNA PRIVACY LAW WATCH, Feb. 22, 2010.

109 *Id.*

110 *Id.*

Google Analytics's browser plug-in, while ostensibly a response to privacy critics, is highly unlikely to be used by the majority of online consumers.

One concern that this proposal does solve is the need for different systems for different privacy models, as discussed by Bennett & Raab: "The value of personal information for a [] firm is probably a greater incentive to seek the lowest possible standard. If it has to design its systems to allow an opt-in in Germany, and an opt-out in the United States, so be it."[111] If very few users use the opt-out, Germany, and the rest of the EU, will likely press Google to adapt the software again in the future. Perhaps European privacy enforcers will require extreme measures, such of the destruction of already collected data. Considering the importance of privacy for German data protection authorities, it is likely that Google Analytics will still be viewed as illegal without the consent of the person being tracked, even with an opt-out feature available to German Internet users.[112]

More than the rest of Europe, Google's opt-out browser option is likely to be met with skepticism by government officials due to the likelihood of it being used by very few users. But on the other hand, considering the importance of Google Analytics generally and its present market share, those who use analytics program will see this option as the means to avoid implementing other changes.

Otherwise, deleting all existing user data will be the only means to comply with the data retention standards. We predict that Google Analytics (and other analytics programs) will also create versions of their programs that will allow for all data to be retained within the EU, thereby avoiding some of the more strenuous privacy protections.

VI. WHAT IS THE FUTURE OF GOOGLE ANALYTICS?

As the web analytics industry enters adolescence, the tension between the demand for behavioral-targeted marketing and online privacy concerns have become more of a priority for consumers. Individuals and consumer organizations have actively contributed to an increased dialogue about online companies' privacy policies. Google's introduction of real time social networking platform Google Buzz, as a part of Gmail in February of 2010, prompted a wide consumer backlash among online users and a formal

111 COLIN J. BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 218 (2006)

112 There are additional functionality-based options; one includes an experimental program at Carnegie Mellon which notifies online users to more carefully consider privacy when online, and a means of giving uses a "visceral notice" of sharing of private information, and lastly, to change generally how web browsers work. Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. Times, February 27, 2010

complaint with the Federal Trade Commission (FTC) on the part of advocacy group Electronic Privacy Information Center (EPIC), and a public statement by the Electronic Frontier foundation. EPIC's argument, that Google's access to personally identifiable user information through products such as Gmail, violates privacy and gives Google an unfair competitive advantage.[113] German government officials in their critique of Google Analytics used a similar argument.[114]

While Google Analytics collects user information anonymously, Google's unique position, as a multi-channel information technology corporation, makes the company's free analytics service open to a higher level of scrutiny than its competitors in the web analytics software marketplace. Even so, some server-hosted web analytics software companies do collect enough online information to track a user individually, such as Clicky Web Analytics, which makes it possible for a user to track the individual session data of a website visitor. In addition, Google's Urchin product, the licensed alternative to Google Analytics hosted on an organization's own servers, can report on individual visitor clickpaths. With that said, the major criticism of Google Analytics is that it is hosted on Google's own server, which also hosts the private information of millions of online users.

Amidst this criticism, in March 2010, Google announced the development of a browser-based opt-out option for Google Analytics users, which would allow online visitors to GA installed website a choice in allowing their behavior to be tracked by the software.[115] This development, while ostensibly a response to criticism from EU governments, may also have been a response to Google Analytics's developing relationship with U.S. government departments. In February 2010, Google Analytics was approved for use on the apps.gov website, a resource for U.S. government approved cloud computing applications.[116]

The June 2010 changes in government policy, regarding the collection of potentially personally identifying information on government websites, is a huge shift. Whether this will lead to changes in policy regarding

---

113 Ryan Paul, *EPIC fail: Google faces FTC complaint over Buzz privacy*, Ars Technica, February 17, 2010, http://arstechnica.com/security/news/2010/02/epic-fail-google-faces-complaint-over-buzz-privacy-issues.ars

114 Robin Wauters, *Achtung! Google Analytics is illegal, say German government officials*, November 24, 2009, TechCrunchEU, http://eu.techcrunch.com/2009/11/24/google-analytics-illegal-germany/

115 Amy Chang, *More choice for users: browser-based opt-out for Google Analytics on the way*, Google Analytics Blog, March 18, 2010, http://analytics.blogspot.com /2010/03/more-choice-for-users-browser-based-opt.html

116 *Google Analytics, Powerful, Secure and now approved by the U.S. Government*, February 17, 2010, http://analytics.blogspot.com/2010/02/powerful-flexible-secure-and-now.html

commercial and nonprofit websites, as regulated by the FTC, or federal legislation, is too early to tell. But there is a high likelihood of additional shifts, considering both the need for return on investment for both government and industry, and the inevitability of privacy data breaches.

The future of web analytics—as a tool and as an industry—will continue to evolve as behavioral targeted marketing and social media become more commonly utilized by companies, organizations, and governments. In addition, Google Analytics's widespread use in the industry will likely continue unabated, thanks in part to its open source status and relative ease of use. But as we have discussed, privacy advocates will continue to raise concerns in the United States, the European Union, and Germany.

While the Center for Democracy & Technology (CDT) and the Electronic Frontier Foundation (EFF), Open Recommendations for the Use of Web Measurement Tools on Federal Government Web Sites are specifically intended for government websites, they may also serve as a roadmap for the web analytics industry in addressing the way that overall privacy is protected:

> But much has to change beforeFalse Web sites can take full advantage of Web measurement without harming individual user privacy. First and foremost, the providers of measurement tools must build their products to higher privacy standards than what currently exists in the commercial sector. Agencies must craft robust policies to ensure that data collected for measurement purposes is adequately safeguarded. And the [] polic[ies] on persistent tracking technologies must be adapted to continue to establish the highest levels of privacy protection while accounting for recent technological advances.[117]

Increased consumer education about how online visitor information is collected and used by web analytics software is the best way to ensure public accountability of the web analytics industry regarding privacy. This approach would be more impactful to structural policy change and a dialogue on online user privacy than Google's functionality-based

117 CENTER FOR DEMOCRACY & TECHNOLOGY & THE ELECTRONIC FRONTIER FOUNDATION, OPEN RECOMMENDATIONS FOR THE USE OF WEB MEASUREMENT TOOLS ON FEDERAL GOVERNMENT WEB SITES, May 2009, http://www.cdt.org/files/pdfs/20090512_analytics.pdf

approach; one that likely very few consumers will use. It will also be more effective than a strictly regulatory approach that may always be a step or two behind developing analytics technology.