An Internet Of Nosy Insects

Web Bugs, Advertisers, and You

Samuel Daniel

samuel.daniel@tufts.edu

Abstract

The growth of the advertising-based Internet economy has brought about the creation of new advertising technologies. A popular advertising scheme is the targeting of individual user through the use of Web bugs, 1x1 pixel GIFs, and other technologies that surreptitiously track an individual user's Internet browsing habits. Advertisers and other Internet-tracking entities will place HTML iframes or JavaScript snippets in a page's source code that planet cookies when a user visits a site. When the user clicks a link to travel to another site or a new page, the tracker updates its cookie with that information, effectively duplicating the user's browsing history inside the cookie. Advertisers will analyze this cookie's contents in order to display advertisements that are aligned with content a particular user regularly visits on the Internet. The use of social media creates a direct connection between a user's real-world personal information and his or her Internet presence. As the line between someone's online and offline presence blur, Internet advertisers are eager to fill in the gaps with relevant ads. This paper will examine the concepts behind contemporary web bugs, the legal issues surrounding their use, and some preventative measures for privacy-minded Netizens.

I. Introduction

The term "Web bug" has been around since the late 1990s. In the most general sense, Web bugs are snippets of HTML, Javascript, or other code in a web page that is almost always hosted by a third-party server, such as an advertiser. When the user's browser loads a page containing a third-party Web bug, it downloads the Web bug from the third-party's server, inadvertently sending information like the user's IP address and any previously set cookie values. Web bugs manipulate cookie values to uniquely identify users and create a browsing history on the third-party server that gets updated each time the user visits a website with that particular Web bug. Advertisers use this information to create profiles on an individual user's interests and Internet habits. Web bugs are often included in HTML formatted emails, especially in mass commercial emails. Whenever the recipient opens the email, the email client loads the HTML and executes the Web bug, thus telling the sender that the recipient has indeed opened the email. (SANS)

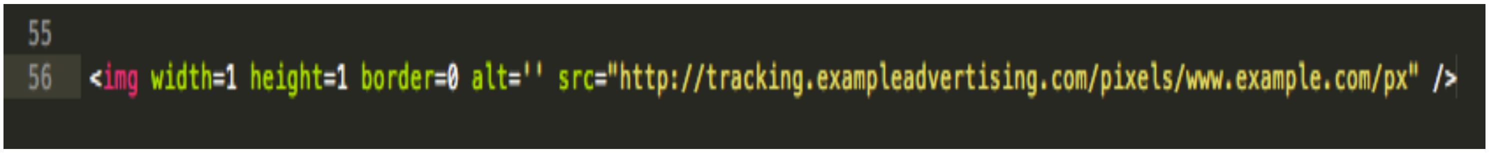
II. Technologies and Techniques

Web bugs can take many forms. The canonical Web bug is a 1 pixel by 1 pixel transparent GIF image, hosted on a third-party webserver, and placed in an <img> tag on a web page. Other forms of Web bugs are scripts written in PHP or JavaScript that are also hosted by third-party servers and then executed as soon as the user loads the page.

A) 1x1 Tracking GIF

A Web bug can easily be added to a Web page simply by including an image hosted on a third-party server. In practice, these images are transparent 1 pixel by 1 pixel GIFs hosted by an advertiser. These GIFs are given unique paths and filenames on the host server so that the advertiser can easily narrow down which of its many Web bugs has been triggered. Transparent GIFs are used because transparency in GIFs is more widely supported by different (especially older) browsers.

According to the definition in the previous paragraph, the following situation describes a simple Web bug. The website www.example.com wants to include a Web bug from Example Advertising Inc. Example Advertising sends www.example.com's webmaster a link to a unique tracking pixel and instructs him or her to include it in www.example.com's source:



```

<img width=1 height=1 border=0 alt='' src="http://tracking.exampleadvertising.com/pixels/www.example.com/px" />
```

When a user visits www.example.com, the browser receives the source code for www.example.com. When the browser renders the source code, it will make an HTTP GET request to tracking.exampleadvertising.com in order to display that <img> tag.

The process of the user's browser downloading the tracking pixel happens swiftly and without the user's knowledge. When the server receives the user's HTTP request, it can parse and log all of the information contained in the request, such as:

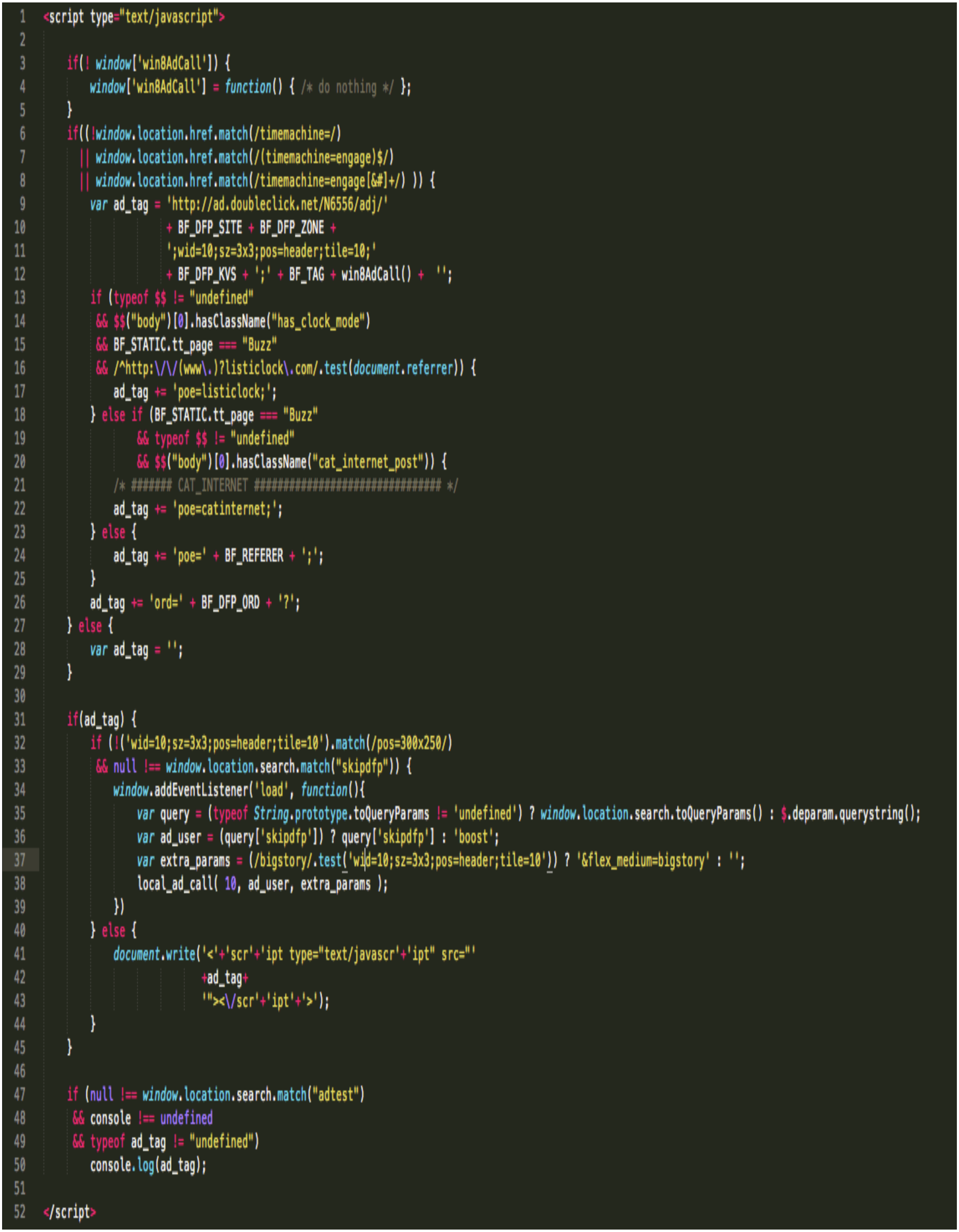
- the user's IP address
- the URL of the page containing the Web bug
- the URL of the Web bug itself
- the time that the user loaded the page (and subsequently triggered the Web bug)
- the user's browser
- any previously set cookies that belong to track.exampleadvertising.com

This type of Web bug is especially useful in HTML email messages. Web bugs help organizations running large-scale email campaigns to measure how many people have viewed a particular email, detect if someone is not reading an email at all, and to match a Web browser cookie with an email address. This last use is important to a lot of Web sites because it allows them to narrow down the identity of visitors. (Smith)

B) JavaScript and PHP

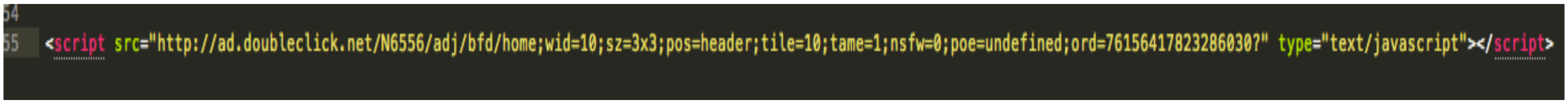
The simple model of the tracking GIF can easily be enhanced with the addition of JavaScript or PHP. When a website includes a link to a third-party's JavaScript or PHP code, a user's browser will execute this code when the page is loaded. These executable Web bugs are sometimes called Trojans because they will execute arbitrary code that the user has no knowledge of and did not intend to execute. Intelytics, a group of web analytics specialists, demonstrated an example of a malicious executable Web bug in front of a group of U.S. Congressmen. The Web bug stole the email address book from the computer that visited a bugged website. (Nichols)

A common use of PHP or JavaScript is to dynamically build up query parameters for the URL of a tracking pixel. Then, when the user's browser downloads the tracking pixel, it uses a URL that has been loaded with information from cookies or other sources. For example, consider the following JavaScript snippets from BuzzFeed.com.



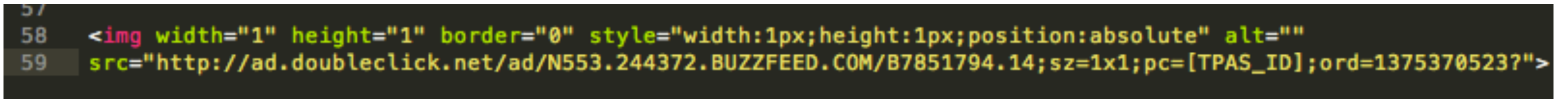
```
<script type="text/javascript">

    if(! window['win8AdCall']) {
        window['win8AdCall'] = function() { /* do nothing */ };
    }
    if((!window.location.href.match(/timemachine=/)
      || window.location.href.match(/(timemachine=engage)$/)
      || window.location.href.match(/timemachine=engage[&#]+/) )) {
        var ad_tag = 'http://ad.doubleclick.net/N6556/adj/'
                     + BF_DFP_SITE + BF_DFP_ZONE +
                     ';wid=10;sz=3x3;pos=header;tile=10;'
                     + BF_DFP_KVS + ';' + BF_TAG + win8AdCall() +  '';
        if (typeof $$ != "undefined"
         && $$("body")[0].hasClassName("has_clock_mode")
         && BF_STATIC.tt_page === "Buzz"
         && /^http:\/\/(www\.)?listiclock\.com/.test(document.referrer)) {
            ad_tag += 'poe=listiclock;';
        } else if (BF_STATIC.tt_page === "Buzz"
                && typeof $$ != "undefined"
                && $$("body")[0].hasClassName("cat_internet_post")) {
            /* ####### CAT_INTERNET ################################ */
            ad_tag += 'poe=catinternet;';
        } else {
            ad_tag += 'poe=' + BF_REFERER + ';';
        }
        ad_tag += 'ord=' + BF_DFP_ORD + '?';
    } else {
        var ad_tag = '';
    }

    if(ad_tag) {
        if (!('wid=10;sz=3x3;pos=header;tile=10').match(/pos=300x250/)
         && null !== window.location.search.match("skipdfp")) {
            window.addEventListener('load', function(){
                var query = (typeof String.prototype.toQueryParams != 'undefined') ? window.location.search.toQueryParams() : $.deparam.querystring();
                var ad_user = (query['skipdfp']) ? query['skipdfp'] : 'boost';
                var extra_params = (/bigstory/.test('wid=10;sz=3x3;pos=header;tile=10')) ? '&flex_medium=bigstory' : '';
                local_ad_call( 10, ad_user, extra_params );
            })
        } else {
            document.write('<'+'scr'+'ipt type="text/javascr'+'ipt" src="'
                           +ad_tag+
                           '"><\/scr'+'ipt'+'>');
        }
    }

    if (null !== window.location.search.match("adtest")
     && console !== undefined
     && typeof ad_tag != "undefined")
        console.log(ad_tag);

</script>
```

The above code uses global variables ("BF_DFP_SITE", "BF_STATIC", etc.) defined elsewhere in order to generate the following <script> tag:



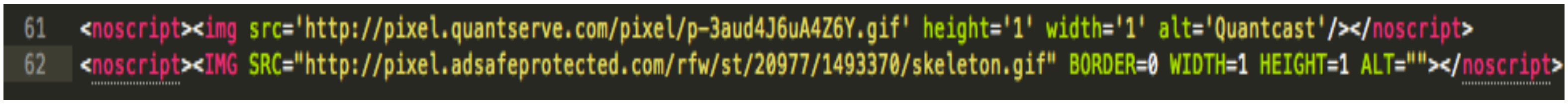
```html
<script src="http://ad.doubleclick.net/N6556/adj/bfd/home;wid=10;sz=3x3;pos=header;tile=10;tame=1;nsfw=0;poe=undefined;ord=7615641782328603?" type="text/javascript"></script>
```

This dynamically loads more JavaScript and ultimately results in a transparent 1 pixel by 1 pixel Web bug:



```html
<img width="1" height="1" border="0" style="width:1px;height:1px;position:absolute" alt=""
src="http://ad.doubleclick.net/ad/N553.244372.BUZZFEED.COM/B7851794.14;sz=1x1;pc=[TPAS_ID];ord=1375370523?">
```

The BuzzFeed.com source also contained these two tracking pixels:



```html
<noscript><img src='http://pixel.quantserve.com/pixel/p-3aud4J6uA4Z6Y.gif' height='1' width='1' alt='Quantcast'/></noscript>
<noscript><IMG SRC="http://pixel.adsafeprotected.com/rfw/st/20977/1493370/skeleton.gif" BORDER=0 WIDTH=1 HEIGHT=1 ALT=""></noscript>
```

The content within the <noscript> tags is rendered when a user's browser has JavaScript disabled. (Kyrnin) The first tracker from pixel.quantserve.com belongs to Quantcast, a marketing analytics company. The second tracker appears in Google's Safe Browsing diagnostic page for adsafeprotect.com, Google's testing found a "malicious trojan" at that domain which was "downloaded and installed without user consent". (“Google Safe Browsing…”)

C) Advertising Networks and Third-Party Cookies

The JavaScript code and tracking pixel from BuzzFeed.com make reference to "ad.doubleclick.net", a subdomain of Google's DoubleClick advertising network. DoubleClick provides a variety of services. It lets publishers display advertisements on their website while simultaneously allowing the advertisers to control how often an ad is shown. DoubleClick also facilitates targeted advertising within one website or across an entire advertising network using Google's Adsense service. Adsense lets different publishers combine user data collected through third-party cookies scattered throughout the Internet. (Geary)

In 2012, Google's advertising revenues totaled $43.7 billion. (“2013 Financial Tables…”) The success of Google's advertising services can be attributed mostly to one thing: sheer scope. An advertising network's Web bugs are only useful if they are placed in as many websites as possible so that users will activate them over and over on as many sites as possible. This is what enables advertisers and marketers to build up profiles about individual people’s Internet browsing habits and then specifically target them with ads. By accumulating a history of the different ads that a user has seen, advertisers and marketers can correlate specific online purchases with ads that that user has been shown in the past. (Nichols) It is worth noting that, as of this writing, Amazon.com is hosting a DoubleClick Web bug.

The key technology that enables the continued success of Internet advertising networks is the third-party cookie. According to the HTTP cookie standard, a cookie can only be read by the server that set the cookie: cookies set by BuzzFeed.com when a user visits the page can only ever be accessed by BuzzFeed.com's servers. But third-party cookies are set by "trusted partners" of the websites that a user visits: when a user goes to BuzzFeed.com, DoubleClick's JavaScript code is allowed to set and read DoubleClick cookies on that user’s browser. When that same user goes to a different website hosting another DoubleClick Web bug, the Web bug can update the DoubleClick cookie to include the details of the user's visit to this new site. (“FAQ on Mozilla’s…”)

In December of 2012, Jonathan Mayer, a graduate student at Stanford, proposed a patch to Mozilla Firefox that would change the browser's default cookie policy to accept all first-party cookies and to only accept third-party cookies if that third-party already has at least one cookie set on the browser. This change would make Firefox's cookie policy the same as Safari's and Internet Explorer's. (Mayer; Santos) By not accepting third-party cookies, most Web bugs would be rendered useless. News of this change immediately upset Internet advertisers and marketers. The senior vice president and general counsel of the Interactive Advertising Bureau even went as far as to say that this represented a "nuclear first strike against the ad industry". (Stampler) But by May, 2013, Mozilla had decided to delay the cookie-blocking patch, citing the need for "more data". (Albanesius, “Mozilla Delays…”)

III. Law and Order

In the past decade, there have been a number of lawsuits regarding misuse of information garnered from Internet users. And as of this writing, there have been recent major developments in attempts to pass legislation and create standards about Internet tracking and privacy. The issues at the heart of the lawsuits and legislation mentioned below all stem from how Web bugs track users as they surf the Internet and what information Web bugs record and send to advertisers.

A) Previous Lawsuits

i) Facebook Beacon

In November, 2007, Facebook launched Beacon, a kind of Web bug that would allow Facebook users to share online purchases made on Beacon's affiliate websites, such as Overstock.com and Fandango.com. Users took issue with the service when they realized that it was opt-out, not opt-in, and that they were inadvertently sharing information on Facebook that they might have preferred not to share. In 2008, a class-action lawsuit was filed in California against Facebook as well as several of Facebook’s Beacon partners. Eventually a settlement was reached: Facebook was required to end the Beacon service as well as donate $9.5 million towards the creation of a foundation to promote online privacy. (Metz)

ii) Google Tracking Safari Users

The same Jonathan Mayer who developed the cookie-blocking patch for Firefox released a report in early 2012 accusing Google and three other ad networks of subverting the privacy settings on the Safari web browser to track iPhone and Mac users without their permission or knowledge. Google stated that Mayer's report "mischaracterizes" what the company is doing with its tracking, however, the company admitted that Google cookies were accidentally being set on Safari and vowed to fix the bug. The Federal Trade Commission, in its largest civil penalty ever, fined Google $22.5 million for violating a previous agreement: in March 2011, Google had agreed to implement privacy protections, submit to regular privacy audits, and to no longer misrepresent its privacy policies. (Albanesius, “Court Approves…”, “Google Accused…”)

B) Legislative Efforts

Lawsuits against Internet corporations and criticism from Internet privacy advocates have piled up in the past ten years and there have been governmental responses at both the federal and state levels.

i) California's Ad Disclosure Law

In September 2013, the governor of California signed a bill into law requiring Internet companies that collect personal information to publicly declare their policy regarding Do Not Track requests in an attempt to force such corporations to be more transparent. Since Internet trackers can ignore Do Not Track requests at will, the bill hopes to shame companies into changing their policies. While the passage of this new bill has a "lack of usual hyperbole about the bill bringing down the online economy", the bill is still an important first step towards a more privacy-conscious Internet experience. Jonathan Mayer criticized the bill for not thoroughly defining "do not track". (Temple)

ii) Do Not Track

In April 2013, the Senate Commerce Committee held a hearing about the status of the Do Not Track privacy standard. During the hearing, the Commerce Committee Chairman, Senator Jay Rockefeller, criticized the Internet advertising industry, accusing it of "dragging its feet" in development of the Do Not Track standard called for by the Federal Trade Commission. Senator Rockefeller was making reference to stalled negotiations between the World Wide Web Consortium and the ad industry, represented by the Digital Advertising Alliance (DAA).

The DAA proposed its "Ad Choices" program, which it claimed, would allow a user to opt out of data collection. But some critics claimed the program only blocked targeted ads rather than actually stopping user tracking. The W3C, on the other hand, had created a Tracking Protection Group at the behest of the White House and FTC two years prior, but the group had not produced any concrete proposals and missed a number of deadlines. By September 2013, discussions between the W3C and the DAA had completely collapsed. The DAA seemed to believe that the W3C was incapable of codifying the standard. Though the W3C does not require the DAA to finish its task, people involved in the process are still worried that the creation of a Do Not Track standard will drag on for some time. (Ingraham; Kaye)

IV. To The Community

The goal of this paper is two-fold: to inform curious readers about how exactly Internet advertisers track users and to raise awareness about the privacy issues that arise when companies engage in tracking programs of the massive scope and scale that can be seen today. While the technology used in most Web bugs is over two decades old, they still go relatively unnoticed. As Internet advertising networks continue to grow, it is becoming exceedingly important for Internet users as well as developers throughout the industry to take action.

Anyone and everyone should urge their representatives at both state and federal levels of government to propose and pass legislation protecting Internet users' privacy and data from abuse. Developers are in a unique position to encourage their employers to take an initiative to be more transparent and obvious about Internet tracking. Web bugs have been such wildly successful tools because most people do not know that they exist. In an ideal world, people visiting a website with Web bugs in place would be greeted with an obvious message stating very plainly that they are going to be tracked, who is tracking them, what information is being recorded, how that information will be used, and that they have the option to opt-out entirely of such tracking.

A) Preventative Measures

Until a Do Not Track standard can be devised and enforced, the best option that concerned Netizens have is to turn to a wide variety of browser extensions that help subvert Web bugs and other forms of Internet tracking.

The most important browser extension that this writer can recommend is Ghostery. Available on every browser as well as iOS and Android, Ghostery blocks over 1700 Internet trackers, cookies, Web bugs, pixels, and beacons. When a page loads, Ghostery will block whatever trackers it can find that the user has disabled. Ghostery allows the user to specify which Web bugs he or she would like to block. DoNotTrackMe and Disconnect are other browser extensions, available for multiple platforms, that perform a nearly identical function to Ghostery.

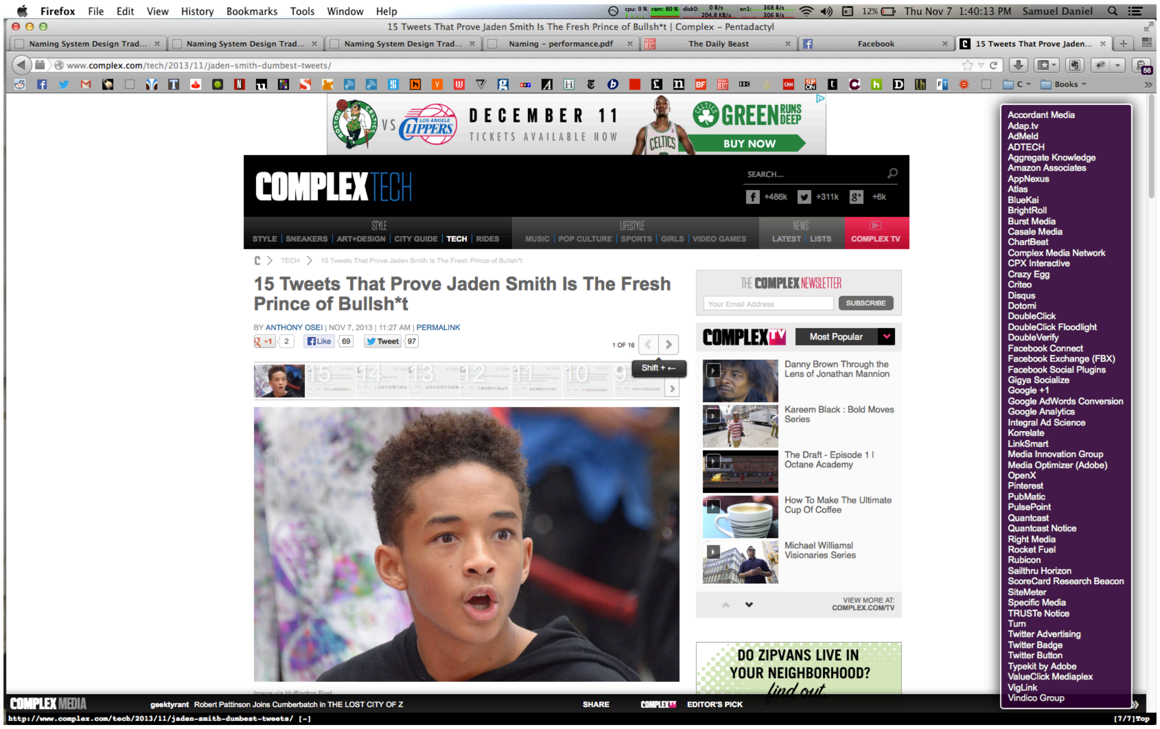
RequestPolicy is a Firefox extension that gives the user control over the cross-site requests that his or her browser makes when visiting a web page. The default setting for this extension is to deny any and all cross-site requests. This is useful in blocking both Web bugs and trackers and also preventing cross-site request forgery attacks. NoScript is another Firefox-exclusive extension that performs a similar function as RequestPolicy.

Blender is a very simple Firefox-exclusive browser extension that fakes the data in an HTTP header with common parameters. It sets the user's operating system to Windows 7 64-bit, the Firefox version to 22, the language to English, and leaves the accepted charsets parameter as unspecified.

Cookie Monster is a browser extension that allows a user to manage exactly which websites can and cannot set cookies on his or her browser. It works with both first-party and third-party cookies.

These browser extensions are all very appealing to anyone concerned about their privacy on the Internet. But there are two caveats to their usage. The first is quite a few of the above extensions are for Firefox only. Second, a large portion of the Internet requires cookies and JavaScript in order to look and function correctly. Certain browser extensions, like NoScript or RequestPolicy, might prevent a website from executing JavaScript that it needs in order to render properly. Often, Ghostery or Disconnect will block some sort of external JavaScript or iframe that is responsible for loading something on the page.

For example, picture A is a screenshot of a random website loaded with Ghostery turned off. The purple box on the right is a list of all of the trackers and cookies that Ghostery is ignoring. Picture B is of the same webpage loaded with Ghostery enabled. The text in the purple box displays the trackers that Ghostery is now blocking. The list is much shorter because when Ghostery disabled the first few trackers, most of the site's content (including other Web bugs) was prevented from loading.


Firefox File Edit View History Bookmarks Tools Window Help
Thu Nov 7 1:40:13 PM Samuel Daniel
15 Tweets That Prove Jaden Smith Is The Fresh Prince of Bullsh*t | Complex – Pentadactyl
Naming System Design Trad...
Naming System Design Trad...
Naming System Design Trad...
Naming – performance.pdf
The Daily Beast
Facebook
15 Tweets That Prove Jaden...
www.complex.com/tech/2013/11/jaden-smith-dumbest-tweets/
56
C
Books
DECEMBER 11
TICKETS AVAILABLE NOW
GREEN RUNS DEEP
BUY NOW
COMPLEX TECH
SEARCH...
+486k
+311k
+6k
STYLE
STYLE | SNEAKERS | ART+DESIGN | CITY GUIDE | TECH | RIDES
LIFESTYLE
MUSIC | POP CULTURE | SPORTS | GIRLS | VIDEO GAMES
NEWS
LATEST | LISTS
COMPLEX TV
TECH
+1 2
Like 69
Tweet 97
1 OF 16
Shift + ←
THE COMPLEX NEWSLETTER
Your Email Address
SUBSCRIBE
COMPLEX TV
Most Popular
VIEW MORE AT: COMPLEX.COM/TV
DO ZIPVANS LIVE IN YOUR NEIGHBORHOOD? find out.
COMPLEX MEDIA
SHARE
COMPLEX TV
EDITOR'S PICK
[7/7]Top

15 Tweets That Prove Jaden Smith Is The Fresh Prince of Bullsh*t

BY ANTHONY OSEI | NOV 7, 2013 | 11:27 AM | PERMALINK

Image via Huffington Post

Danny Brown Through the Lens of Jonathan Mannion

Kareem Black : Bold Moves Series

The Draft - Episode 1 | Octane Academy

How To Make The Ultimate Cup Of Coffee

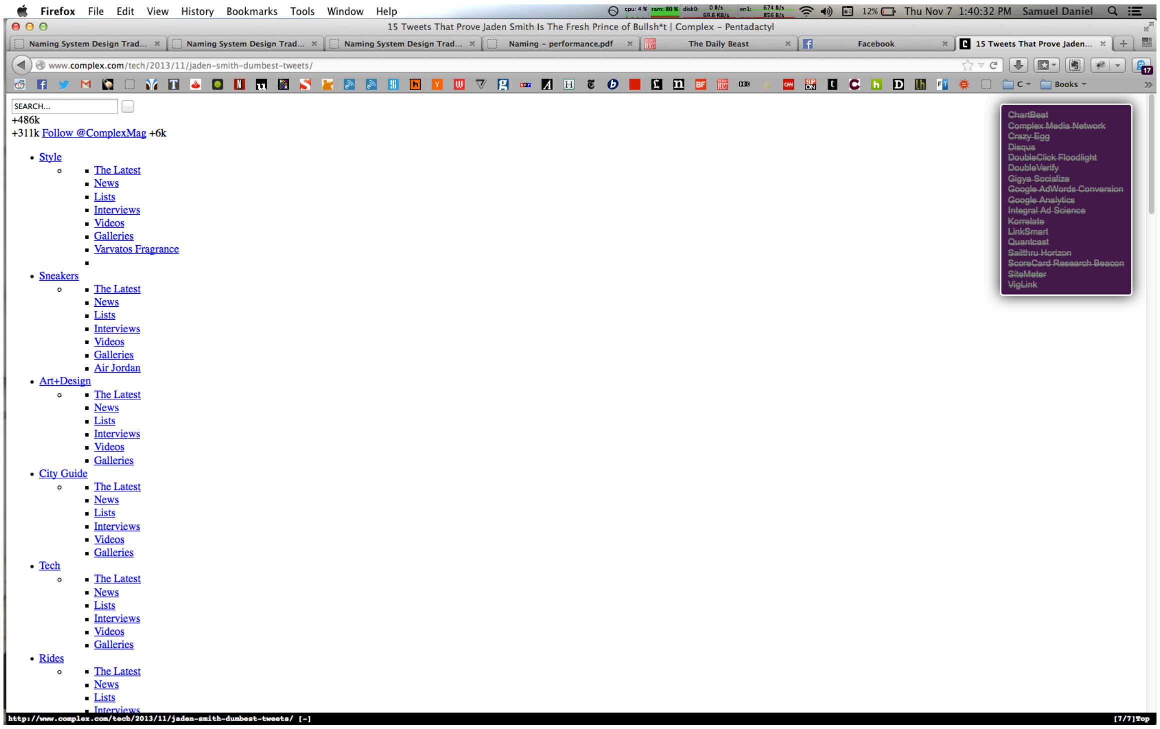
Michael Williamsl Visionaries Series

geektyrant Robert Pattinson Joins Cumberbatch in THE LOST CITY OF Z

Accordant Media
Adap.tv
AdMeld
ADTECH
Aggregate Knowledge
Amazon Associates
AppNexus
Atlas
BlueKai
BrightRoll
Burst Media
Casale Media
ChartBeat
Complex Media Network
CPX Interactive
Crazy Egg
Criteo
Disqus
Dotomi
DoubleClick
DoubleClick Floodlight
DoubleVerify
Facebook Connect
Facebook Exchange (FBX)
Facebook Social Plugins
Gigya Socialize
Google +1
Google AdWords Conversion
Google Analytics
Integral Ad Science
Korrelate
LinkSmart
Media Innovation Group
Media Optimizer (Adobe)
OpenX
Pinterest
PubMatic
PulsePoint
Quantcast
Quantcast Notice
Right Media
Rocket Fuel
Rubicon
Sailthru Horizon
ScoreCard Research Beacon
SiteMeter
Specific Media
TRUSTe Notice
Turn
Twitter Advertising
Twitter Badge
Twitter Button
Typekit by Adobe
ValueClick Mediaplex
VigLink
Vindico Group

```
http://www.complex.com/tech/2013/11/jaden-smith-dumbest-tweets/ [-]
```

Picture A


Firefox File Edit View History Bookmarks Tools Window Help
Thu Nov 7 1:40:32 PM Samuel Daniel
15 Tweets That Prove Jaden Smith Is The Fresh Prince of Bullsh*t | Complex – Pentadactyl
Naming System Design Trad...
Naming System Design Trad...
Naming System Design Trad...
Naming – performance.pdf
The Daily Beast
Facebook
15 Tweets That Prove Jaden...
www.complex.com/tech/2013/11/jaden-smith-dumbest-tweets/
17
C
Books
[7/7]Top

SEARCH...
+486k
+311k Follow @ComplexMag +6k

- Style
  - The Latest
  - News
  - Lists
  - Interviews
  - Videos
  - Galleries
  - Varvatos Fragrance
  -
- Sneakers
  - The Latest
  - News
  - Lists
  - Interviews
  - Videos
  - Galleries
  - Air Jordan
- Art+Design
  - The Latest
  - News
  - Lists
  - Interviews
  - Videos
  - Galleries
- City Guide
  - The Latest
  - News
  - Lists
  - Interviews
  - Videos
  - Galleries
- Tech
  - The Latest
  - News
  - Lists
  - Interviews
  - Videos
  - Galleries
- Rides
  - The Latest
  - News
  - Lists
  - Interviews

~~ChartBeat~~
~~Complex Media Network~~
~~Crazy Egg~~
~~Disqus~~
~~DoubleClick Floodlight~~
~~DoubleVerify~~
~~Gigya Socialize~~
~~Google AdWords Conversion~~
~~Google Analytics~~
~~Integral Ad Science~~
~~Korrelate~~
~~LinkSmart~~
~~Quantcast~~
~~Sailthru Horizon~~
~~ScoreCard Research Beacon~~
~~SiteMeter~~
~~VigLink~~

```
http://www.complex.com/tech/2013/11/jaden-smith-dumbest-tweets/ [-]
```

Picture B

The best way to circumvent Web bugs in email is to prevent an email client from loading the images in an email as soon as the email is opened. This is a setting that can be changed in all major email clients. Recently, Google has announced that it will cache all of the images sent to Gmail users. This means that all of the content hosted on a third-party server will first be downloaded to Google's servers. Then Google will display the images to the user when he or she opens the message. This policy change completely defeats the purpose of including Web bugs in an email: the Web bug will trigger when Google caches the image, not when the user actually reads the email. (Amadeo)

B) Good Practice for Webmasters

Website analytics software hosted on a third-party server, like Google Analytics, is a subtle form of Web bug. Though the information that the analytics code might collect is not being used for advertising purposes, it is most likely still being logged. In order to fully protect users, the best solution is to roll one's own analytics software. Free and open source software like Open Web Analytics, Hummingbird, whereswaldo, and Piwik all allow webmasters to host and manage their own analytics software.

V. Conclusion

A) Looking Forward

Replacements for the classic cookie are already coming down the pipeline. Recently, Google has announced that it has beginning to focus on developing an anonymous identifier to possibly replace cookies called AdID. The AdID would be distributed to advertisers and advertising networks that have agreed to use Google's new system, which the an anonymous source within the company claims will give consumers more privacy and control of their data. This development is concerning to some in the advertising industry because it could shift more control of the industry to already powerful companies like Google. (Barr) "Supercookies" are a new type of cookie developed by Google and Microsoft that are capable of tracking users across every device they own: smartphones, computers, game consoles, televisions. Being able to expand tracking horizontally across devices enables much more powerful analytics and ultimate even more accurate targeted advertising. (Anthony) Supercookies differ from standard cookies in that they are stored in different locations on the user's device, like in a file used by a Flash plug-in. This makes supercookies much harder to find and delete for existing technologies. (Olsen)

B) Where do we go from here?

In the immediate short term, Web bugs are certainly not going to disappear; the advertising that they enable is too important to the economic structure of the Internet as whole. And it is not necessarily in the best interests of companies who utilize Web bugs to make their intentions obvious to users. Internet advertising is a wildly successful multi-billion dollar industry that is only going to grow; and tracking data is a vital resource that most corporations are unwilling to give up at all. The allure of targeted advertising is too great. Though government and industry bodies are attempting to standardize and regulate commercial tracking on the Internet, the technology driving the trend is changing quickly and the responsible regulatory bodies are extremely slow to catch up. If the litigious history of some Internet tracking endeavors can teach us anything, it is that self-regulation by the people doing the tracking will only go so far. Until appropriate legislation is finally signed into law and regulation codified and enforced, it will be up to individual users to protect themselves from the sting of Web bugs.

References

"2013 Financial Tables Investor Relations - Google." Google.com. Google, Inc., n.d. Web. 11 Dec. 2013. <http://investor.google.com/financial/tables.html>.

Albanesius, Chloe. "Court Approves $22.5 Million Safari Tracking Fine Against Google." PC Magazine. PC Magazine, 19 Nov. 2012. Web. 13 Dec. 2013. <http://www.pcmag.com/article2/0,2817,2412291,00.asp>.

Albanesius, Chloe. "Google Accused of Tracking Safari Usage Without Permission." PC Magazine. PC Magazine, 17 Feb. 2012. Web. 13 Dec. 2013. <http://www.pcmag.com/article2/0,2817,2400413,00.asp>.

Albanesius, Chloe. "Mozilla Delays Cookie-Blocking by Default in Firefox." PC Magazine. PC Magazine, 17 May 2013. Web. 13 Dec. 2013. <http://www.pcmag.com/article2/0,2817,2419140,00.asp>.

Amadeo, Ron. "Gmail Blows up E-mail Marketing by Caching All Images on Google Servers." Ars Technica. Condé Nast, 12 Dec. 2013. Web. 13 Dec. 2013. <http://arstechnica.com/information-technology/2013/12/gmail-blows-up-e-mail-marketing-by-caching-all-images-on-google-servers/>.

Anthony, Sebastian. "Microsoft, Google Working on Super Cookies to Track Your Activity on Every Device." ExtremeTech. Ziff Davis, Inc., 11 Oct. 2013. Web. 13 Dec. 2013. <http://www.extremetech.com/computing/168418-microsoft-google-working-on-super-cookies-to-track-your-behavior-everywhere>.

Barr, Alistair. "Google May Ditch 'cookies' as Online Ad Tracker." USA Today. Gannett, 17 Sept. 2013. Web. 13 Dec. 2013. <http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/>.

"DoubleClick Settles in Web Privacy Litigation Lawsuit." WARC.com. WARC, 2 Apr. 2002. Web. 13 Dec. 2013. <http://www.warc.com/Content/News/N11131_DoubleClick_Settles_in_Web_Privacy_Litigation_Lawsuit.content?CID=N11131>.

Edwards, Jim. "The Man Who Turned Off Cookies In Firefox Doesn't Care If It Hurts Advertisers." Business Insider. Business Insider, Inc., 8 May 2013. Web. 13 Dec. 2013. <http://www.businessinsider.com/jonathan-mayer-and-cookies-in-firefox-2013-5>.

Evers, Joris. "How HP Bugged E-mail." CNET News. CBS Interactive, 28 Sept. 2006. Web. 13 Dec. 2013. <http://news.cnet.com/2100-1029_3-6121048.html>.

"FAQ on Mozilla's Intention to Block Third-Party Cookies." FAQ on Mozilla's Intention to Block Third-Party Cookies. Interactive

Advertising Bureau, 2013. Web. 13 Dec. 2013. <http://www.iab.net/mozilla>.

Geary, Joanna. "DoubleClick (Google): What Is It and What Does It Do?" Theguardian.com. Guardian News and Media, 23 Apr. 2012. Web. 12 Dec. 2013. <http://www.theguardian.com/technology/2012/apr/23/doubleclick-tracking-trackers-cookies-web-monitoring>.

"Google Safe Browsing Diagnostic Page for Adsafeprotected.com." Google Safe Browsing Diagnostic Page for Adsafeprotected.com. Google, Inc., n.d. Web. 13 Dec. 2013. <http://google.com/safebrowsing/diagnostic?site=adsafeprotected.com>.

Greene, Thomas C. "Fun with Internet Bugs." The Register. The Register, 13 Dec. 2000. Web. 13 Dec. 2013. <http://www.theregister.co.uk/2000/12/13/fun_with_internet_bugs/>.

"IAB Internet Advertising Revenue Report." Interactive Advertising Bureau. PricewaterhouseCoopers LLP and the Interactive Advertising Bureau, 2013. Web. 13 Dec. 2013. <http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2012_rev.pdf>.

Ingraham, Nathan. "Do Not Track's Future in Doubt as Major Ad Group Withdraws from Talks." The Verge. Vox Media, Inc., 17 Sept. 2013. Web. 13 Dec. 2013. <http://www.theverge.com/2013/9/17/4741028/do-not-tracks-future-in-doubt-as-major-ad-group-withdraws-from-talks>.

Junnarkar, Sandeep. "DoubleClick Accused of Unlawful Consumer Data Use - CNET News." CNET News. CBS Interactive, 28 Jan. 2000. Web. 13 Dec. 2013. <http://news.cnet.com/2100-1023-236216.html>.

Kang, Cecilia. "Bills Would Curb Tracking of and Advertising to Children on Internet." The Washington Post. The Washington Post, 15 Nov. 2013. Web. 13 Dec. 2013. <http://www.washingtonpost.com/business/technology/bills-would-curb-tracking-of-and-advertising-to-children-on-internet/2013/11/14/dee03382-4d58-11e3-ac54-aa84301ced81_story.html>.

Kaplan, David A. "Suspicions and Spies in Silicon Valley." Newsweek. IBT Media Inc., 17 Sept. 2006. Web. 13 Dec. 2013. <http://www.newsweek.com/suspicions-and-spies-silicon-valley-109827>.

Kaye, Kate. "Sen. Jay Rockefeller Blasts Ad Industry In Senate Hearing Over Do Not Track." Ad Age. Ad Age, 24 Apr. 2013. Web. 13 Dec. 2013. <http://adage.com/article/digital/sen-jay-rockefeller-blasts-ad-industry-track/241078/>.

Kyrnin, Jennifer. About.com Web Design / HTML. About.com, n.d. Web. 13 Dec. 2013. <http://webdesign.about.com/od/htmltags/p/bltags_noscript.htm>.

Mayer, Jonathan. "The New Firefox Cookie Policy." Web Policy. Jonathan Mayer, 22 Feb. 2013. Web. 13 Dec. 2013. <http://webpolicy.org/2013/02/22/the-new-firefox-cookie-policy/>.

McMillan, Robert. "The Web Bug in HP's Toolbox." CIO. CXO Media Inc., 01 Nov. 2006. Web. 13 Dec. 2013. <http://www.cio.com/article/221091/The_Web_Bug_in_HP_s_Toolbox>.

Metz, Cade. "Facebook Turns out Light on Beacon." The Register. The Register, 23 Sept. 2009. Web. 13 Dec. 2013. <http://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/>.

Nichols, Steve. "Big Brother Is Watching: An Update on Web Bugs." InfoSec Reading Room. SANS Institute, 3 July 2001. Web. 13 Dec. 2013. <https://www.sans.org/reading-room/whitepapers/threats/big-brother-watching-update-web-bugs-445>.

Olsen, Christian. "Supercookies: What You Need to Know About the Web's Latest Tracking Device." Mashable. Mashable, Inc., 02 Sept. 2011. Web. 13 Dec. 2013. <http://mashable.com/2011/09/02/supercookies-internet-privacy/>.

Santos, Alexis. "Microsoft Sets 'do Not Track' as Default on IE10, Ruffles Feathers." Engadget. AOL Tech, 1 June 2012. Web. 13 Dec. 2013. <http://www.engadget.com/2012/06/01/do-not-track-is-default-on-ie10/>.

Smith, Richard M. "The Web Bug FAQ." The Web Bug FAQ. Electronic Frontier Foundation, 11 Nov. 1999. Web. 13 Dec. 2013. <https://w2.eff.org/Privacy/Marketing/web_bug.html>.

Soltani, Ashkan, Andrea Peterson, and Barton Gellman. "NSA Uses Google Cookies to Pinpoint Targets for Hacking." The Switch. The Washington Post, 10 Dec. 2013. Web. 13 Dec. 2013. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/>.

Stampler, Laura. "Firefox Launches 'Nuclear First Strike Against Ad Industry'" Business Insider. Business Insider, Inc., 25 Feb. 2013. Web. 13 Dec. 2013. <http://www.businessinsider.com/firefox-to-block-third-party-cookies-2013-2>.

Temple, James. "Do-not-track Bill a Small Step toward Real Privacy." SFGate. Hearst Communications, Inc., 21 Sept. 2013. Web. 13 Dec. 2013.

<http://www.sfgate.com/technology/dotcommentary/article/Do-not-track-bill-a-small-step-toward-real-privacy-4832949.php>.

Wong, Grace. "Ex-HP Chairman Dunn, Others Charged in Leak Case." CNNMoney. Cable News Network, 05 Oct. 2006. Web. 13 Dec. 2013. <http://money.cnn.com/2006/10/04/news/companies/hp_california/index.htm>.