

1 Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
2 David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
3 KamberLaw, LLC
4 100 Wall Street, 23rd Floor
5 New York, New York 10005
6 Telephone: (212) 920-3072
7 Facsimile: (212) 202-6364

8 Interim Class Counsel

9 David C. Parisi (SBN 162248)
dcparsi@parisihavens.com
10 Suzanne Havens Beckman (SBN 188814)
shavens@parisihavens.com
11 Parisi & Havens LLP
12 15233 Valleyheart Drive
13 Sherman Oaks, California 91403
14 Telephone: (818) 990-1299
15 Facsimile: (818) 501-7852

16 Attorneys for Plaintiffs

17 Additional counsel listed on signature page

18 UNITED STATES DISTRICT COURT
19 CENTRAL DISTRICT OF CALIFORNIA

20 In Re QUANTCAST ADVERTISING
21 COOKIE LITIGATION

No. 2:10-CV-05484-GW-JCG
No. 2:10-CV-05948-GW-JCG

22 In Re CLEARSPRING FLASH
23 COOKIE LITIGATION

[Assigned to the Hon. George H. Wu]
**JOINT SUBMISSION OF
SUPPLEMENTAL INFORMATION
REGARDING PLAINTIFFS'
MOTION FOR PRELIMINARY
APPROVAL OF CLASS ACTION
SETTLEMENT**

24 Date: January 13, 2011
25 Location: Courtroom 10
26 312 North Spring Street
27 Los Angeles, CA 90012
28 Time: 8:30 a.m.

1 This Joint Supplemental Information Submission Regarding Plaintiff’s Mo-
2 tion for Preliminary Approval of Class Action Settlement is submitted in response
3 to the Court’s December 16, 2010 request that the parties furnish additional in-
4 formation about the technology at issue in the litigation and how and when defen-
5 dants Quantcast and Clearspring used that technology and the data derived from it.

6 **How Do Third Parties “See” Web Users?**¹

7 Each time an Internet user directs his or her browser to a website by enter-
8 ing a web page address (*i.e.*, its universal resource locator, or URL, and path
9 information), or navigates from one page to another by clicking on a hypertext
10 link, here is what actually happens: the user’s browsing software (browser) trans-
11 mits hypertext transfer protocol (HTTP) commands to request the page from the
12 server where the web page resides.² These commands include information about
13 the user’s browser and the user’s IP (Internet Protocol) address (essentially, the
14 user’s return address). The server responds by transmitting the contents of a
15 document that contains the web page expressed in hypertext markup language
16 (HTML). The user’s browser processes the HTML code, which tells the browser
17 how to display the web page on the user’s computer. (To view the actual HTML
18 code, a user can click *View > Source* option on the browser menu bar.)

19 Often, a web page’s HTML code will include commands to download addi-
20 tional files. For example, the HTML code for the text of a news article may be
21 stored in one file on the news organization’s server (*e.g.*, [http://www.news-](http://www.news-
22 org.com/topstory)
23 [org.com/topstory](http://www.news-org.com/topstory)) while the photos that accompany the article may be stored in

24 ¹ For purposes of this document, this section includes descriptions of typical and
25 representative, but not the sole, technologies used in web communications.

26 ² The global standard for HTTP communications was defined in “RFC 2616,
27 Hypertext Transfer Protocol—HTTP/1.1,” Fielding, *et al.*, Internet Engineering
28 Task Force (IETF), June 1999, available at <http://www.ietf.org/rfc/rfc2616.txt.pdf>
(last accessed January 1, 2011).

1 other files (e.g., <http://www.newsorg.com/photolib/topstory-pic1> and <http://www.newsorg.com/photolib/topstory-pic2>). Thus, a user's single request to view a web
2 page may trigger multiple requests to download content from multiple servers
3 without further action or even awareness on the user's part. Some of this embed-
4 ded web page content, such as advertisements, may come from third-party servers,
5 i.e., from domains controlled by parties other than the website the user chose to
6 visit.

7
8 Some embedded images are invisible to the user. For example, when a web-
9 site wants to use a third-party service to monitor traffic levels on a web page, the
10 website may embed third-party images that display nothing at all, but permit the
11 third party to monitor user activity. These images, known as "web beacons" (the
12 term preferred by the advertising industry), "pixel tags," "clear GIFs," or "web
13 bugs," are so small the user cannot see them but, just like a web page statement to
14 display an advertisement, they cause the user's browser to communicate with the
15 third party's server. In the process, the user's browser automatically sends the
16 third party information that includes details about the user's browser and Internet
17 address, making the user "visible" to the third party.

18 **What is an HTTP cookie?**

19 Although the communications process of downloading web content makes a
20 user somewhat visible to the party hosting that content, it does not necessarily
21 make the user recognizable. For example, the user's IP "return" address allows a
22 third party to send the user's browser an advertisement to be embedded in a web
23 page display, but the IP address does not reliably allow the advertiser to recognize
24 that it is serving an ad to the same user the next day or even a few minutes later.

25 This is because, in the most basic user-server communications on the web,
26 each communication is "stateless." That is, even though the user may have a sense
27 of being "connected to" a website, no continuous connection exists. The user has
28 merely downloaded one or more documents that are displayed on the user's com-

1 puter screen. When the user clicks on a hypertext link on the web page, the user
2 initiates a download request that starts from scratch, without any history or context
3 from the page the user was just viewing, such as whether the user was viewing an
4 online shopping cart and is now ready to pay for the items in the cart. Without any
5 way to maintain a continuous state of user-to-server communications, the web
6 cannot support complex transactions—such as online shopping—that require a
7 succession of related web page displays and user responses.

8 To avoid this disconnection from page view to page view or session to ses-
9 sion, HTTP includes a mechanism by which a website can affix identifying infor-
10 mation to a user’s browser, to “recognize” the user and “remember” the last ex-
11 change in the communication between user and server. That mechanism is an
12 HTTP cookie. A cookie is a small string of text transmitted to and from a user’s
13 computer in a communication between a server group and a particular instance of
14 browser client software.³ A cookie may contain whatever information the website
15 obtains from or attaches to the user, such as a zip code entered by the user for
16 viewing the local weather each time the user visits the website, a username the
17 user selected for interactions with the website, or a unique identifier the website
18 operator assigns to the user.

19 Cookies transmitted from a website are automatically stored by the browser
20 on the user’s computer. Each cookie is a separate file. On each new page view, the
21 website operator can read, update, or replace the cookie. One website operator can
22

23 _____
24 ³ The global standard for HTTP cookies was initially defined in “RFC 2965,
25 HTTP State Management Mechanism,” Kristol and Montulli, Internet Engineering
26 Task Force, Oct. 7, 2000, available at <http://www.ietf.org/rfc/rfc2965.txt.pdf>
27 (January 3, 2011); *see also*, “RFC 2964, BCP (Best Current Practice) 44, Use of
28 HTTP State Management,” Moore and Freed, Internet Engineering Task Force,
Oct. 12, 2000, available at <http://www.ietf.org/rfc/rfc2964.txt.pdf> (last accessed
January 3, 2011).

1 set multiple cookies on a user's computer and, at any point in time, the typical
2 user's computer may contain hundreds or thousands of cookies.⁴

3 For browsers that operate according to IETF standards, the operator of one
4 website cannot view the contents of another website operator's cookie. However,
5 when a website operator is a third-party advertiser or metrics company, it can set a
6 common cookie that it uses to track a user's activities across the many websites on
7 which it serves ads or gathers traffic data.

8 By default, commercial browsers, such as Firefox or Internet Explorer, as-
9 sume a user wants to accept first-party cookies (from the visited website) and
10 third-party cookies (such as those from advertisers and metrics companies). A user
11 who does not want these parties to set cookies can change the default browser
12 setting and block all cookies, although doing so would likely render many web-
13 sites nonfunctional. A user who does not want to be tracked by third parties can
14 set his or her browser controls to block only third-party cookies (although even
15 this action may affect the functionality of some websites). For example, in Safari,
16 this control is accessed as follows:

17 Safari > Preferences > Security > Accept cookies: Only
18 from sites I visit / Block cookies from third parties and
19 advertisers

20 In addition, a user can delete browser cookies previously stored by third parties to
21 attempt to prevent the third party from associating previously acquired tracking
22 data with the consumer's subsequent web activity. Blocking or deleting can be
23 accomplished "by hand," that is, for specific cookies, or automatically, using tools
24

25 _____
26 ⁴ For example, a number of U.S. district courts set a cookie called "MENU" that,
27 in at least some instances, contains a single word, such as "slow." In addition,
28 some U.S. courts set cookies named "_utmz" and "_utma" that contain lengthy
numeric and alphanumeric codes.

1 available in or in addition to the browser. Mechanisms to block and delete third-
2 party cookies are generally available to consumers using commercial browsers.

3 See Exhibit A, attached, for an illustration of third-party data collection on a
4 web page.

5 **What is a “Flash cookie”?**

6 Adobe Flash Player, a popular program originally distributed by Macrome-
7 dia Corp. and now distributed by Adobe Corporation, is widely used to display
8 videos and games. Flash Player has its own method—called local shared objects,
9 or “LSOs”—of storing bits of data on the computers using the software. For
10 example, many online games run in Adobe Flash Player. If a user seeks to play a
11 game over multiple sessions, Flash stores information about the player’s previous
12 session, including where the player left off, in an LSO. Where Flash Player oper-
13 ates on a news or sports website, to use another example, the LSO may contain
14 information about the user’s volume choice, screen resolution and other settings,
15 so the user does not need to select those settings on each subsequent visit to the
16 same site. According to Adobe, LSOs were designed to support consumers’ ability
17 to experience “rich Internet application” content using the Adobe Flash Player.
18 Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at [http://www.-](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf)
19 [ftc.gov/os/comments/privacyroundtable/544506-00085.pdf](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf) (last accessed Dec. 6,
20 2010).

21 Just as with HTTP cookies, Flash Player LSOs can be set to contain unique
22 user identifiers. There are, however, important differences between HTTP cookies
23 and Flash Player LSOs: for example, Flash Player LSOs can be much larger than
24 HTTP cookies (four kilobytes for cookies versus up to 100 kilobytes for LSOs),
25 can contain more complex information, and, by default, do not expire. LSOs also
26 are stored in a different place than HTTP cookies and are not deleted or rejected
27
28

1 when a user instructs his or her browser to delete or not to accept HTTP cookies.⁵
2 In addition, as mentioned above, HTTP cookies are designed so that one website
3 operator cannot read cookies set by another website operator whereas LSOs per-
4 mit “cross-domain” access. Website operators using LSOs can override the re-
5 quirement to maintain encrypted communications that a user establishes with a
6 secure (HTTPS) website. Finally, HTTP cookies are essentially vendor-
7 independent; the manner in which they operate is governed by global standards
8 and by usage conventions shared by all commercially available browsers. LSOs
9 are subject to Adobe Corporations implementation of Flash Player software.

10 **How Do Quantcast and Clearspring Use Cookies and LSOs?**

11 A study entitled “Flash Cookies and Privacy” was published in August 2009
12 by the University of California, Berkeley and is annexed hereto as Exhibit B (the
13 “Berkeley Study”). Plaintiffs’ Consolidated Amended Complaint refers exten-
14 sively to the Berkeley Study. Quantcast and Clearspring concur with the material
15 findings of the Berkeley Study specifically to Quantcast and Clearspring and to
16 the extent it reported observations relating collectively to third-party metrics and
17 advertising companies that include Quantcast and Clearspring,

18 Quantcast and Clearspring further offer the following description of their
19 current uses of cookies and LSOs.

20 When a user visits a website (call it “Widget.com”), the user may receive a
21 cookie from Widget.com itself, but also may receive third party cookies placed by
22 advertisers on or vendors to the Widget.com website. In the case of defendant
23 Quantcast, for example, the operators of the Widget.com website may wish to
24 determine how many unique (vs. repeat) visitors view the website during a given
25 period—a service Quantcast provides. To provide this service, Quantcast places a

26 _____
27 ⁵ Adobe offers a tool for managing LSOs. This tool resides on Adobe’s servers and
28 is proprietary to Adobe. See http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html (last accessed January 3, 2011).

1 very simple cookie on the user's computer containing only a randomly-generated
2 number and the time of day. In the Widget.com example, when the user com-
3 mands his or her computer to load the Widget.com web page, Widget.com's
4 HTTP code would cause the user's computer also to query Quantcast. If the user's
5 computer already had a Quantcast number cookie stored on it, the request the
6 user's computer sends to Quantcast would contain a copy of that previously-set
7 Quantcast cookie, allowing Quantcast to determine if the user is a new visitor or
8 one who has visited the Widget.com site before. If the user has no extant Quant-
9 cast cookie, Quantcast will count the user as a new visitor, and send one.

10 Quantcast collects no personally-identifiable information in this process. All
11 it does is assign an anonymous user a random number. But—and this is the key to
12 Quantcast's service—when that user visits either Widget.com again, or another
13 website serviced by Quantcast, Quantcast can tell that he or she is the *same*
14 anonymous user who visited Widget.com previously.

15 Clearspring uses cookies for similar anonymous purposes. Clearspring pro-
16 vides a service that allows website publishers to include online “buttons” on their
17 websites, which visitors to the websites can click on to quickly share website
18 content to social networks like Facebook and other online destinations. At certain
19 times, Clearspring has utilized HTTP cookies and LSOs to anonymously track
20 basic information about users' interactions with the websites that use its tools. For
21 example, when a user visits a website that uses Clearspring's technology, Clear-
22 spring places a cookie on the user's computer with a unique computer-generated
23 number so that it can count the number of unique users to the particular web page
24 (in other words, if that same user visits the webpage again, Clearspring will know
25 not to count that user again because it will know from the unique identifier on the
26 cookie that the user has previously visited the website). Like Quantcast, Clear-
27 spring's use of cookies and LSOs has at all times been limited to these anonymous
28 types of web analytics and Clearspring has never used cookies or LSOs to track

1 personally identifiable information. Moreover, both Clearspring and Quantcast no
2 longer store information from LSOs at all in any of their services.

3 The sorts of anonymous information maintained in cookies are useful for a
4 number of reasons. One important reason is that Internet advertising (and thus the
5 economic viability of the Internet) depends on the ability to measure *unique*
6 visitors to a website. Advertisers need to know how many *different* people their
7 ads will reach for a given cost. It is far more valuable to an advertiser to have
8 multiple people view its ad once than to have a single user view it multiple times.
9 As noted above, however, the Internet is inherently stateless. Thus, if one's
10 browser is constantly refreshing (for example) a news site or the progress of a
11 sporting event, the same user's computer may query the same website hundreds of
12 times in an hour. Absent a cookie of the type placed by Quantcast and Clearspring,
13 the website operator would not know if those requests were coming from the same
14 user or different users. This type of cookie also allows website operators to better
15 understand what various content on its site the same user chooses to visit, how
16 long the same user spends on the site, etc.⁶

17 As companies that provide advertising-related services, Quantcast and
18 Clearspring generate information about the same users' visits to multiple websites
19 with which those networks have relationships. They can determine, for example,
20 that an anonymous user assigned number "12345678" visited Widget.com and
21 then WidgetReviews.com (assuming both those sites have relationships with the
22 same network). Like any other website operator, however, Quantcast and Clear-
23 spring can see and update only the cookies they themselves placed; they cannot

24 ⁶ At best, this method can provide only a fairly accurate picture of the number of
25 unique visitors to a site. If a user deletes his or her cookies from one browsing
26 session to the next, he or she will be assigned a new random number upon the next
27 visit to the website, and be considered a second unique visitor, rather than the
28 return visitor he or she actually is. Various methodologies exist to correct for this
effect, but none are perfect.

1 see the contents of the first-party cookies placed by the website the user is visiting.
2 Thus, even if the user identifies himself or herself by name to the first-party web-
3 site, Quantcast and Clearspring do not learn that name or any other information
4 passed from the user to the first-party website.

5 Simply knowing that the same user visited multiple websites, however, as
6 Quantcast and Clearspring do, facilitates “Online Behavioral Advertising” (or
7 “OBA”). Without collecting personally-identifiable information or knowing a
8 user’s identity, but by placing a unique identifier cookie, it is possible to deter-
9 mine that the visitor to a particular news site today visited a particular car com-
10 pany’s website yesterday and a travel company’s website the day before. Knowing
11 this information, the news site can show the user an ad for a new car or for a travel
12 service, and can seek a higher price for the placement of that ad, because the
13 consumer viewing the ad has a demonstrated likelihood to find the ad useful. This
14 kind of targeted advertising helps advertisers, enables millions of website opera-
15 tors to provide deep, broad, and useful content free of charge to the consumer,
16 and, for that reason, is seen by many as pro-consumer.⁷ Although no one likes
17 advertising in the abstract, much of the Internet is free only because of advertising,
18 and if people must view ads, many may prefer to see one for something they might
19 want rather than for goods or services they don’t want. Neither Clearspring nor
20 Quantcast has ever delivered OBA based on LSOs, and Clearspring only began
21 offering advertising-related service in December 2009 using a platform that util-
22 izes only HTTP cookies, which are not at issue in this litigation.

23
24
25 ⁷ Quantcast and Clearspring also provide methods for consumers to “opt out” of
26 receiving any OBA. They accomplish this by placing what is known as an “opt
27 out” cookie on the user’s computer, which instructs Defendants not to serve tar-
28 geted ads to that user. Quantcast is a member of the Network Advertising Initia-
tive (“NAI”) and complies with the NAI’s opt-out procedures.

1 **Quantcast and Clearspring's Former Use of LSOs**

2 Quantcast and Clearspring further make the following representations about
3 their former uses of cookies and LSOs.

4 The differences between LSOs and HTTP cookies gave rise to the since-
5 discarded practice underlying this dispute. As noted, users must employ different
6 tools to manage or delete HTTP cookies and LSOs. As a result, (again using
7 Quantcast's past system as an example) a Quantcast-placed LSO and a Quantcast-
8 placed HTTP cookie on the same computer, which should contain the same
9 unique, anonymous identifier, might not. If a user deleted his or her HTTP cook-
10 ies, the next HTTP request to Quantcast would cause the creation of a new unique
11 identifier. In an attempt not to count the same user as multiple unique visitors to
12 the same sites, Quantcast formerly utilized a synchronization process. The process
13 looked at the various cookies, and, if they did not match, found the oldest value,
14 and set the others to the same value, bringing them back into synch.

15 Clearspring's use of LSOs was similar. When Clearspring stored an LSO on
16 a computer, it also stored a back-up HTTP cookie at the same time. Both cookies
17 contained the same anonymous user ID number and were used for the same
18 anonymous purpose as described above. If a user deleted the HTTP cookie (but
19 not the LSO) and then later accessed a web page using Clearspring's technology,
20 Clearspring's servers would detect that there was an LSO but no HTTP cookie
21 associated with the computer. Clearspring's systems would then place a new
22 HTTP cookie that would adopt the same user ID as the existing LSO. This unique
23 user ID is the *only* information that was restored in this process and the *only*
24 consequence to the user was that Clearspring would then use the LSO and back-
25 up HTTP cookie for the same anonymous analytics as described above (put sim-
26 ply, no personally identifiable information was impacted by the use of LSO).
27 Again, Clearspring and Quantcast no longer use LSOs even for this limited pur-
28 pose.

1 As researchers discovered and publicized in the Berkeley Study last August,
2 this synchronization process had a side effect. Viewed from the user's perspective,
3 the Berkeley Study portrayed, and Plaintiffs in this action contend that the effect
4 of synchronizing HTTP cookies and LSOs in circumstances where a user had
5 deleted his or her HTTP cookie was to regenerate or "respawn" this information,
6 which the user had deleted, and to do so without the user's express consent.

7 The Berkeley Study researchers published their findings on August 10,
8 2009. By August 12, 2009, Quantcast had modified its systems to cease "respawn-
9 ing." Since then, if a user deletes his or her Quantcast-placed HTTP cookies, they
10 stay deleted, and any newly-placed cookies would contain a new identifier unre-
11 lated to the value contained in the user's LSOs or prior HTTP cookies.

12 Quantcast and Clearspring both have represented that they had no intention
13 to return to the prior practice and, under the proposed settlement, they will be
14 enjoined from doing so. They also will agree to provide consistent and reliable
15 disclosure of other uses of Flash LSOs. Those provisions are set out in detail in the
16 settlement agreement and proposed orders. Briefly summarized, they (i) ban
17 entirely the use of LSOs to respawn HTTP cookies; (ii) prohibit the use of LSOs
18 "as an alternative method to HTTP cookies for storing information about a user's
19 web browsing history, unrelated to the delivery of content through the Flash
20 Player or the performance of the Flash Player in delivering such content, without
21 adequate disclosure"; (iii) prohibit the use of LSOs to "otherwise counteract any
22 computer user's decision to either prevent the use of or to delete previously cre-
23 ated HTTP cookies"; and, (iv) require Defendants to advocate that the relevant
24 trade associations adopt such provisions as model rules for the use of LSOs by all
25 of their members. The parties believe that these provisions will provide important
26 privacy protections to all Internet users, and will assure that the issues raised by
27 the previous use of LSOs to respawn cookies will not recur.

Other Defendants and Settlement Participants

1 **Other Defendants and Settlement Participants**
2 The Berkeley Study (Exhibit B hereto) reported on substantially similar
3 practices of a number of other third-party metrics and advertising companies.
4 Some of these entities are named in other cases pending before this Court and
5 other U.S. District Courts. The representations herein relate to Quantcast and
6 Clearspring

7 The defendants in this matter other than Quantcast and Clearspring are
8 arm's-length customers of Quantcast and/or Clearspring ("Customer Defen-
9 dants"). The consolidated complaint alleges class members had contact with
10 Quantcast and/or Clearspring when class members accessed the Customer Defen-
11 dants' websites and web content.

12 The Customer Defendants, on their own behalf and on behalf of their corpo-
13 rate parents and affiliates, have represented to Quantcast and Clearspring that the
14 Customer Defendants were unaware that LSOs were being used to store informa-
15 tion regarding consumers who accessed their websites and web content. Quantcast
16 and Clearspring do not dispute that representation and, to the extent of their know-
17 ledge, information, and belief, adopt and incorporate it here.

18 In the settlement agreement before the Court, certain participants are re-
19 ferred to as "Undertaking Parties." The Undertaking Parties consist of Customer
20 Defendants and certain of the Customers Defendants' corporate parents or affili-
21 ates who have agreed to undertake the obligations imposed by the settlement
22 agreement. The remedial value of the injunctive relief agreed to by the Undertak-
23 ing Parties is generally applicable to their relationships with any of the third-party
24 metrics and advertising companies identified in the Berkeley Report and benefits
25 any classes of consumers that might have been affected by the conduct of those
26 companies. Because the scope of injunctive relief agreed to by the Undertaking
27 Parties encompasses relationships they had with Quantcast and Clearspring, plus
28 any relationships they may have had with other third-party metrics and advertising

1 companies, the proposed settlement would provide the Undertaking Parties with a
2 release from claims involving Quantcast and Clearspring as well as the other third-
3 party metrics and advertising companies.

4 Should the Court have questions about the relevant technologies not ad-
5 dressed in this submission or in the attached Berkeley Report, the parties will be
6 prepared to address those questions at the hearing currently scheduled for January
7 13, 2011.

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CONFIDENTIAL DRAFT

1 DATED: January 7, 2011 Respectfully submitted,

2
3 KAMBERLAW, LLC

4 s/David A. Stampley

5 Scott A. Kamber
6 David A. Stampley
7 KamberLaw, LLC
8 100 Wall Street, 23rd Floor
9 New York, New York 10005
10 Interim Class Counsel

11
12 COOLEY LLP

13 s/Michael Rhodes

14 Whitty Somvichian
15 101 California Street, 5th Floor
16 San Francisco, California 94111
17 Attorneys for Defendant
18 Clearspring Technologies, Inc.

19
20 DURIE TANGRI LLP

21 s/Michael H. Page

22 Michael H. Page
23 217 Leidesdorff Street
24 San Francisco, California 94111
25 Attorneys for Defendant Quantcast Corp.
26
27
28

EXHIBIT A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

“Data Usage & Control Primer:
Best Practices & Definitions” at
Interactive Advertising Bureau, May 2010, at 6,
[http:// www.iab.net/media/file/data-primer-final.pdf](http://www.iab.net/media/file/data-primer-final.pdf) (last accessed Jan. 1, 2011).

EXHIBIT B

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28