

1 Majed Nachawati
2 mn@fnlawfirm.com
3 Fears | Nachawati Law Firm
4 4925 Greenville Ave, Suite 715
5 Dallas, Texas 75206
6 Telephone: (214) 890-0711
7 Facsimile: (214) 890-0711

8 Jeremy R. Wilson
9 jeremy@wilsontrosclair.com
10 Kenneth P. Trosclair
11 pete@wilsontrosclair.com
12 Wilson Trosclair & Lovins, P.L.L.C.
13 302 N. Market St., Suite 510
14 Dallas, Texas 75202
15 Telephone: (214) 484-1930
16 Facsimile: (214) 276-1475

17 David C. Parisi (SBN 162248)
18 dcparisi@parisihavens.com
19 Azita Moradmand (SBN 260271)
20 amoradmand@parisihavens.com
21 Parisi & Havens LLP
22 15233 Valleyheart Drive
23 Sherman Oaks, California 91403
24 Telephone: (818) 990-1299
25 Facsimile: (818) 501-7852

26 Attorneys for Plaintiff

27 **IN THE UNITED STATES DISTRICT COURT**
28 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

29 DAVID PITNER and JARED REAGAN,
30 on behalf of themselves and all others
31 similarly situated,
32 Plaintiffs,

33 v.

34 MIDSTREAM MEDIA
35 INTERNATIONAL, N.V., a Netherlands
36 Corporation,
37 Defendant.

CASE NO. _____

CLASS ACTION

COMPLAINT FOR

(1) Violation of CAAFA;

(2) Violation of California'

Computer Crime Law;

(3) Violation of CLRA;

(4) Unfair Competition; and

(5) Restitution

JURY TRIAL DEMAND

1 **COMPLAINT – CLASS ACTION**

2
3 Plaintiffs, DAVID PITNER and JARED REAGAN, on behalf of themselves
4 and all others similarly situated, sue Defendant, MIDSTREAM MEDIA N.V., and
5 in support thereof, state:
6

7 1. This is a class action. Plaintiffs bring this action on their own behalf
8 and on behalf of all similarly situated individuals.

9 **I.**

10 **PARTIES**

11 2. Plaintiff DAVID PITNER is a resident of Newport Beach in Orange
12 County, California.
13

14 3. Plaintiff JARED REAGAN is a resident of Newport Beach in Orange
15 County, California.
16

17 4. Defendant MIDSTREAM MEDIA N.V. is a Netherlands corporation
18 with its principal place of business at E-Commerce Park #18-Q1 E-Zone,
19 Vredenberg, Curacao, Netherlands Antilles. Service of Process can be made on
20 Defendant through its registered agent at its principal place of business at
21 Vredenberg, Curacao, Netherlands Antilles.
22
23
24
25
26
27
28

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

II.

JURISDICTION AND VENUE

5. This Court has jurisdiction over this matter pursuant to 28 U.S.C. §1331 (federal question jurisdiction) as this lawsuit involves violations of Federal law. Furthermore, this Court has supplemental jurisdiction over any accompanying causes of action for violation of the laws of California and of the various States.

6. This Court has personal jurisdiction over Defendant because Defendant conducts business through its website with California residents and has committed torts within the State of California. Defendant's main website, youporn.com is the 61st most popular website in the world.

7. Defendant's business and advertising engagements with California residents constitutes purposeful avilment of this forum sufficient to subject Defendant to suit in this forum and therefore this Court has jurisdiction in this matter.

8. Furthermore, as outlined in greater detail below, Defendant, through its websites, impermissibly accessed information on Plaintiffs' computers, which are located in the State of California, thus purposefully availing itself (albeit illegally) of forum benefits. This controversy is centered on that conduct. Assertion of jurisdiction to remedy this wrong committed in the forum does not offend traditional notions of fair play and substantial justice.

1 9. Venue is appropriate in this District because members of the proposed
2 class are residents of the District and Defendant has committed torts within the
3 Central District of California. Furthermore, as an alien corporation, venue is
4 appropriate in this District pursuant to 18 U.S.C. § 1391(d).
5

6 **III.**
7

8 **FACTS APPLICABLE TO ALL COUNTS**

9 10. This is a consumer Class Action lawsuit pursuant to Federal Rules of
10 Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).
11

12 11. The basis for Plaintiffs' claims rest on the use by Defendant of
13 "history sniffing" or "history hijacking" techniques to intentionally and knowingly
14 capture personal information from unsuspecting users of its websites, such as
15 Plaintiffs, without their knowledge or consent.
16

17 12. Defendant owns and operates several of the most popular websites on
18 the Internet today. Among the websites in question are "YouPorn", "YouPorn
19 Cocks" and "YouPorn Gay" (hereinafter "YouPorn sites").
20

21 13. The YouPorn sites promote themselves as vehicles to obtain and share
22 free pornographic media and make content generated by third-parties available to
23 their viewers. YouPorn sites are a resource for people who want to view and share,
24 among other things, visual depictions of adult content, including sexually explicit
25 images. Visitors to the website can also "rate" the content they view on a scale of
26 1 through 5.
27
28

1 14. Among other things, the YouPorn sites provide a platform for
2 uploading, sharing and viewing various types of content. The YouPorn sites'
3 dynamic and collaborative services enable registered and unregistered users
4 (visitors and registered members are collectively referred to as "User(s)") to access
5 a host of functionality, including but not limited to various types of media
6 submitted by Users (collectively, "User Submissions").
7
8

9 15. Unfortunately for Plaintiffs, and other members of the class, however,
10 Defendant's website also served as a vehicle for impermissibly accessing their
11 browsing history.
12

13 16. Defendant accomplished its illicit activities through the use of its
14 JavaScript-enabled websites. JavaScript is a language standard that enables the
15 performance of dynamic websites. Due to exploitable vulnerabilities in how most
16 web browsers respond to JavaScript, however, JavaScript can also be used to
17 provide a host site with the opportunity to peek in on the Plaintiffs' internet
18 visitation history.
19
20

21 17. In most browsers, application domains share access to a single visited-
22 page history, file cache and DNS cache. This leads to the possibility of "history
23 sniffing attacks", enabling the YouPorn sites to learn whether a user has visited a
24 specific URL. By embedding Javascript code on its website designed to present
25 Plaintiffs' web browsers with a list of URL's, Defendant was able to ascertain
26
27
28

1 from Plaintiffs' web history files whether Plaintiffs had visited a variety of
2 different websites or not.

3
4 18. This "sniffing history" manipulates the fact that browsers display
5 links differently depending on whether or not their target has been visited.
6 Specifically in JavaScript, the attacker can create a link to the target URL in a
7 hidden part of the page, and then use the browser's DOM interface to inspect how
8 the link is displayed. If the link is displayed as a visited link, the target URL is in
9 the user's history.
10

11
12 19. Essentially, Defendant inserts invisible links into the web page and
13 has JavaScript verify the color field for the link. Because most browsers display a
14 link in a different color if the user has visited that website before, Defendant is
15 thereby able to determine whether the user has visited a particular URL.
16

17
18 20. In this case, Plaintiffs visited Defendant's website. Once they did so,
19 Defendant was able to implement the above-described procedure on Plaintiffs'
20 computers, essentially tricking Plaintiffs' browsers into providing information
21 from Plaintiffs' web history files. Without the deploying the above-described
22 Javascript code on its website, Plaintiffs' browsers would not ordinarily give out
23 this information to Defendant.
24

25
26 21. Particularly troubling, however, were the clear attempts on
27 Defendant's part to disguise its operation and hide what it was doing from its
28 website visitors, including Plaintiffs.

1 22. First, it must be kept in mind that JavaScript is generally invisible to
2 web users. That fact alone is not unusual, as much of the legitimate programming
3 for a website is not seen by the website visitor. There are tools, however, that will
4 allow a web site visitor to read the Javascript on a particular website.
5

6 23. Mindful of this fact, Defendant employed a particularly devious
7 scheme to misdirect users who might use such tools from detecting its tracking
8 activities – cryptography. When a website visitor uses a tool to view the
9 JavaScript on Defendant’s websites, all they would see were a long list of
10 decipherable letters. This is because Defendant changes each letter in the list of
11 URL’s it is checking for by one letter. Thus, qpsoivc/dpn”, for example, becomes
12 “pornhub.com.” It is only at the last minute that this encoded URL is translated to
13 the correct URL to be compared to Plaintiffs’ browsing history.
14
15
16

17 24. Thus, Defendant essentially wrote a code on its websites which, when
18 examined by Plaintiffs’ web browsers, caused that web browser to disclose
19 information from Plaintiffs’ web history files saved on their computers. To make
20 matters worse, Defendant took active steps to hide this fact from its customers such
21 as Plaintiffs by encoding its JavaScript to deceive anyone who might try to
22 ascertain what the JavaScript does.
23
24
25

26 25. The YouPorn sites do not mention this process at all in their terms and
27 conditions. In fact, the YouPorn sites’ privacy policies are not available to users
28 and are only briefly mentioned in the sites’ terms and conditions. These terms and

1 conditions state that “[a]s a condition to using the Website, you agree to the terms
2 of the YouPorn Privacy Policy as it may be updated from time to time. You
3 acknowledge and agree that the technical processing and transmission of the
4 Website, including your User Submissions, may involve (a) transmissions over
5 various networks; and (b) changes to conform and adapt to technical requirements
6 of connecting networks or devices. You further acknowledge and agree that other
7 data collected and maintained by YouPorn with regard to its users may be
8 disclosed in accordance with YouPorn Privacy Policy.”
9
10
11

12 26. The Federal Trade Commission recently issued a report criticizing this
13 type of disclosure and empty policy. The FTC recommends that:

14
15 to ensure that choice is meaningful and accessible to
16 consumers, companies should describe consumer choices
17 clearly and concisely, and offer easy-to-use choice
18 mechanisms. To be most effective, companies should
19 provide the choice mechanism at a time and in a context
20 in which the consumer is making a decision about his or
21 her data. Where a company has a relationship with a
22 consumer, the choice mechanism should be offered at the
23 point when the consumer is providing data or otherwise
24 engaging with the company. In the context of an online
25 retailer, the disclosure and control mechanism should
26 appear clearly and conspicuously on the page on which
27 the consumer types in his or her personal information.
28 For an offline retailer, the disclosure and consumer
control should take place at the point of sale by, for
example, having the cashier ask the customer whether he
would like to receive marketing offers from other
companies. With respect to social media services, if
consumer information will be conveyed to a third-party
application developer, the notice-and-choice mechanism
should appear at the time the consumer is deciding

1 whether to use the application and in any event, before
2 the application obtains the consumer's information.
3 Where the information sharing occurs automatically,
4 through a default setting, that fact should be disclosed
5 clearly and conspicuously at the time the consumer
6 becomes a member of the service, not merely buried in
7 the "privacy policy."

8 27. Plaintiffs and members of the proposed class were harmed by
9 Defendant's action in that their personal, private information was obtained without
10 their knowledge or consent. Plaintiffs and members of the proposed class were
11 harmed in that their personal property -- their computers -- were hijacked by
12 Defendant and coerced into giving Defendant information from Plaintiffs' web
13 browsing history files. This information which was wrongfully and impermissibly
14 obtained from files impermissibly accessed by Defendant, was valuable research
15 data which could have been sold to marketing research firms. Defendant
16 wrongfully benefited by taking this economically valuable information from
17 Plaintiffs without their knowledge or consent.

18 28. This information was also personal and private to Plaintiffs.
19 Obtaining this information by invisible, encrypted code placed on Defendant's
20 website for the purpose of tricking Plaintiffs' computers into giving up valuable
21 information about Plaintiffs constitutes a violation of Plaintiffs' privacy interests.

22 29. Plaintiffs and members of the proposed class bring this action to
23 redress this illegal and intrusive scheme designed by Defendant to peer into their
24 personal lives and collect personal information about them.
25
26
27
28

1 Furthermore, to the extent that undersigned counsel has
2 any legal interest to damages or other monetary relief, or
3 other relief due to the putative class (or any other rights
4 as potential putative class members), arising as a result of
5 the causes of action asserted in this litigation, such
6 interest is hereby disclaimed by undersigned counsel.

7 33. The requirements of Fed. R. Civ. P. 23 are met in this case. The Class,
8 as defined, is so numerous that joinder of all members is impracticable. Although
9 discovery will be necessary to establish the exact size of the class, it is likely,
10 based on the nature of Defendant's business, that it numbers in the millions.

11 34. There are questions of fact and law common to the Class as defined,
12 which common questions predominate over any questions affecting only individual
13 members. The common questions include:
14

- 15 a. whether Defendant, as a regular practice, engaged in
16 "history sniffing" or "history hijacking" on members of
17 the class' computers; and
- 18 b. whether Defendant failed to disclose material terms
19 regarding "history sniffing" or "history hijacking" on
20 members of the class' computers; and
- 21 c. what use was made of such "history sniffing" or "history
22 hijacking" including whether they were used for purposes
23 of tracking individuals web surfing and whether personal
24 information was obtained regarding members of the
25 class; and
- 26 d. whether Defendant employed techniques to thwart the
27 class' attempts to not be tracked by Defendant.
28

1 37. Plaintiffs can and will fairly and adequately represent and protect the
2 interests of the Class as defined and have no interests that conflict with the
3 interests of the Class. This is so because:
4

- 5 a. All of the questions of law and fact regarding the liability
6 of the Defendant are common to the class and
7 predominate over any individual issues that may exist,
8 such that by prevailing on their own claims, Plaintiffs
9 will necessarily establish the liability of the Defendant to
10 all class members;
11 b. Without the representation provided by Plaintiffs, it is
12 unlikely that any class members would receive legal
13 representation to obtain the remedies specified by
14 relevant statutes and the common law;
15 c. Plaintiffs have retained competent attorneys who are
16 experienced in the conduct of class actions. Plaintiffs and
17 their counsel have the necessary resources to adequately
18 and vigorously litigate this class action, and Plaintiffs and
19 their counsel are aware of their fiduciary responsibility to
20 the class members and are determined to diligently
21 discharge those duties to obtain the best possible
22 recovery for the Class.

23 38. Defendant's actions have affected numerous consumers in a similar
24 way. The class action is superior to any other method for remedying Defendant's
25 actions given that common questions of fact and law predominate. Class treatment
26 is likewise indicated to ensure optimal compensation for the Class and limiting the
27 expense and judicial resources associated with thousands of potential claims.
28

COUNT 1 – COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030

39. Plaintiffs incorporate by reference each proceeding and succeeding
paragraph as though set forth fully at length herein.

1 40. By “history sniffing” or “history hijacking” the computers of
2 Plaintiffs and members of the class, Defendant has accessed Plaintiffs’ computers,
3 in the course of interstate commerce and/or communication, in excess of the
4 authorization provided by Plaintiffs as described in 18 U.S.C. § 1030(a)(2)(C).
5

6 41. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally
7 accessing Plaintiffs’ and members of the class’ computers without authorization
8 and/or by exceeding the scope of that authorization.
9

10 42. Plaintiffs’ computers, and those of the class, are protected computers
11 pursuant to 18 U.S.C. § 1030(e)(2)(B).
12

13 43. Defendant thus violated the Act by causing the transmission of a
14 program, information, code or command and as a result causing harm to the
15 protected computer aggregating at least \$5,000 in value.
16

17 44. Defendant’s actions were knowing and/or reckless and caused harm to
18 Plaintiffs and members of the proposed class.
19

20 45. Plaintiffs seek recovery for these damages, as well as injunctive relief,
21 to prevent future harm.
22

23 **COUNT II – CALIFORNIA’S COMPUTER CRIME LAW**

24 **CALIFORNIA PENAL CODE § 502**

25
26 46. Plaintiffs incorporate by reference each proceeding and succeeding
27 paragraph as though set forth fully at length herein.
28

1 47. Defendant’s actions constitute a violation of California Penal Code §
2 502 as Defendants knowingly accessed data belonging to Plaintiffs and members
3 of the proposed class in the State of California and/or through servers located in
4 the State of California.
5

6 48. Pursuant to California Penal Code § 502(b)(1), “Access means to
7 gain entry to, instruct, or communicate with the logical, arithmetical, or memory
8 function resources of a computer, computer system, or computer network.”
9

10 49. Pursuant to California Penal Code § 502(b)(6), “Data means a
11 representation of information, knowledge, facts, concepts, computer software,
12 computer programs or instructions. Data may be in any form, in storage media, or
13 as stored in the memory of the computer or in transit or presented on a display
14 device.”
15

16 50. Pursuant to California Penal Code § 502(b)(8), “Injury means any
17 alteration, deletion, damage, or destruction of a computer system, computer
18 network, computer program, or data caused by the access, or the denial of access to
19 legitimate users of a computer system, network, or program.”
20
21

22 51. Defendants have violated California Penal Code § 502(c)(1) by
23 knowingly accessing and without permission, making use of data from Plaintiffs’
24 computers in order to device and execute business practices to deceive Plaintiffs
25 and Class members into surrendering private electronic communications and
26 activities for Defendants’ financial gain, and to wrongfully obtain valuable private
27
28

1 data from Plaintiffs.

2 52. Defendants have violated California Penal Code § 502(c)(2) by
3 knowingly accessing and without permission, taking, or making use of data from
4 Plaintiffs' computers.
5

6 53. Defendants have violated California Penal Code § 502(c)(3) by
7 knowingly and without permission, using and causing to be used Plaintiffs'
8 computer services.
9

10 54. Defendants have violated California Penal Code § 502(c)(6) by
11 knowingly and without permission providing, or assisting in providing, a means of
12 accessing Plaintiffs' computers, computer system, and/or computer network.
13

14 55. Defendants have violated California Penal Code § 502(c)(7) by
15 knowingly and without permission accessing, or causing to be accessed, Plaintiffs'
16 computer, computer system, and/or computer network.
17

18 56. California Penal Code § 502(j) states: "For purposes of bringing a
19 civil or a criminal action under this section, a person who causes, by any means,
20 the access of a computer, computer system, or computer network in one
21 jurisdiction from another jurisdiction is deemed to have personally accessed the
22 computer, computer system, or computer network in each jurisdiction."
23
24

25 57. Plaintiffs have also suffered injury from these unauthorized acts of
26 disclosure, to wit: their personal, private, and sensitive electronic communications
27 have been harvested, viewed, accessed, stored, and used by Defendants, and have
28

1 not been destroyed, and due to the continuing threat of such injury, have no
2 adequate remedy at law, entitling Plaintiffs to injunctive relief.

3
4 58. Plaintiffs and Class members have additionally suffered loss by
5 reason of these violations, including, without limitation, violation of the right of
6 privacy and the taking of their economically sellable web browsing history.

7
8 59. As a direct and proximate result of Defendants' unlawful conduct
9 within the meaning of California Penal Code § 502, Plaintiffs and Class Members
10 have suffered irreparable and incalculable harm and injuries from Defendant's
11 violations. The harm will continue unless Defendant is enjoined from further
12 violations of this section. Plaintiffs and Class Members have no adequate remedy
13 at law.

14
15
16 60. Defendants' unlawful access to Plaintiffs' computers and electronic
17 communications has caused Plaintiffs irreparable injury. Unless restrained and
18 enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law
19 is not adequate to compensate it for these inflicted and threatened injuries, entitling
20 Plaintiffs to remedies including injunctive relief as provided by California Penal
21 Code § 502(e).

22
23
24 61. Plaintiffs are also entitled to recover their reasonable attorneys' fees
25 pursuant to California Penal Code § 502(e).

26
27 62. Plaintiffs seek all remedies available under the Act, including
28 injunctive relief and recovery of reasonable attorneys' fees.

COUNT III - CONSUMER LEGAL REMEDIES ACT
CALIFORNIA CIVIL CODE § 750 (“CLRA”)

1
2
3 63. Plaintiffs incorporate by reference each proceeding and succeeding
4 paragraph as though set forth fully at length herein.

5
6 64. Defendant failed to disclose the fact that it was “history sniffing” or
7 “history hijacking” Plaintiffs’ and members of the Class’ computers. Plaintiffs,
8 and members of the class, would not ordinarily expect “history sniffing” or
9 “history hijacking” to be used to track their online web browsing behavior.
10

11 65. Such actions by Defendant constitute deceptive and unfair acts and
12 practices pursuant to CLRA.
13

14 66. Defendant’s actions were intended to, and in fact, likely resulted in
15 sales to Plaintiffs and members of the class.
16

17 67. Plaintiffs and members of the proposed class are consumers under the
18 CLRA.
19

20 68. Defendant violated the act in at least the following ways: 1)
21 representing that its services have characteristics, uses, and benefits that they do
22 not have; 2) representing that its services are of a particular standard, grade, quality
23 which they are not; and/or advertising its services with the intent to not sell them as
24 advertised.
25
26
27
28

1 69. Such actions have caused harm to the Plaintiffs and the Class.
2 Plaintiffs and the proposed class seek to remedy this harm by appropriate
3 injunctive relief.
4

5 **COUNT IV – UNFAIR COMPETITION LAW,**
6 **CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200**

7 70. Plaintiffs incorporate by reference each proceeding and succeeding
8 paragraph as though set forth fully at length herein.
9

10 71. Defendant’s above-described actions constitute unlawful and unfair
11 competition within the meaning of the UCL.
12

13 72. Defendant’s actions constitute false advertising in that they failed to
14 disclose to Plaintiffs and members of the proposed class the precise nature of the
15 information which was being wrongfully obtained from Plaintiffs’ computers and
16 those of the proposed class.
17

18 73. Furthermore, as described in the other counts in this Complaint,
19 Defendant’s actions were in violation of several statutes and therefore unlawful.
20

21 74. Plaintiffs and members of the proposed class have been harmed by
22 Defendant’s actions.
23

24 75. Plaintiffs and the proposed class seek damages for this harm as well as
25 injunctive relief to remedy this harm.
26
27
28

COUNT V – RESTITUTION/UNJUST ENRICHMENT

1
2 76. Plaintiffs incorporate by reference each proceeding and succeeding
3 paragraph as though set forth fully at length herein.
4

5 77. Defendant has improperly and illegally profited from the obtainment
6 and/or sale of Plaintiffs’ and members of the class’ personal, private data.
7 Defendant’s actions have been done knowingly and secretively with the intent that
8 Plaintiffs not realize what was being done.
9

10 78. These actions constitute violations of both statutory as well as
11 common law obligations as outlined above.
12

13 79. Defendant’s actions caused harm to Plaintiffs and members of the
14 proposed class.
15

16 80. Plaintiffs and the proposed class seek damages for this harm as well as
17 injunctive relief to remedy this harm.
18

19 81. Defendant should not, in equity, be allowed to retain their ill begotten
20 gains. Plaintiffs therefore seeks recovery from Defendant under the equitable
21 theory of unjust enrichment.
22

23 WHEREFORE, Plaintiffs demand judgment on their behalf and on behalf of
24 the other members of the Class to the following effect:
25

- 26 a. declaring that this action may be maintained as a class
27 action;
28 b. granting judgment in favor of Plaintiffs and the other
 members of the Class against the Defendant;

- 1 c. treble and/or punitive damages should be the Court find
2 that the Defendant acted in willful or reckless disregard
3 of the law;
4 d. injunctive relief preventing Defendant from further using
5 "history sniffing" or "history hijacking" and/or requiring
6 more detailed disclosure and informed consent from the
7 class regarding their use; and
8 e. such other relief as the Court deems appropriate.

8 **DEMAND FOR JURY TRIAL**

9 Plaintiffs demand a trial by jury of all issues so triable.
10

11 Respectfully submitted,

12 Dated: December 3, 2010

PARISI AND HAVENS LLP

13
14 By: 

15 David C. Parisi (SBN 162248)
16 15233 Valleyheart Drive
17 Sherman Oaks, CA 91403-1545
18 Telephone: 818-990-1299
19 Facsimile: 818-501-7852
20 Email: dcparisi@parisihavens.com
21 FEARS | NACHAWATI LAW FIRM

22 Majed Nachawati
23 State Bar No. 24038319
24 mn@fnlawfirm.com
25 Bryan Fears
26 State Bar No. 24040886
27 4925 Greenville Ave, Suite 715
28 Dallas, Texas 75206
Telephone: (214) 890-0711
Facsimile: (214) 890-0712

WILSON TROSCLAIR & LOVINS,
P.L.L.C.
Jeremy R. Wilson
State Bar No. 24037722
Kenneth P. Trosclair
State Bar No. 24033548
302 N. Market St., Suite 510
Dallas, Texas 75202
Telephone: (214) 484-1930
Facsimile: (214) 276-1475

ATTORNEYS FOR PLAINTIFFS
(pro hac vice application pending)

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

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

DECLARATION OF DAVID C. PARISI

I, David C. Parisi, hereby declare on oath as follows:

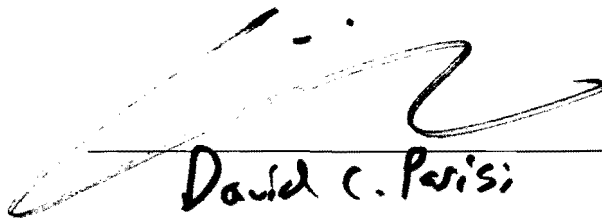
1. I am an attorney licensed to practice law in the state of California. I am over the age of 18 years and I have personal knowledge of the matters attested to herein. If called upon to testify, I would and could competently do so.

2. I make this declaration pursuant to California Civil Code section 1780(c) on behalf of my client, plaintiffs DAVID PITNER and JARED REAGAN, on behalf of themselves and all others similarly situated.

3. Defendant, MIDSTREAM MEDIA N.V., is a Netherlands corporation with its principal place of business at E-Commerce Park #18-Q1 E-Zone, Vredenberg, Curacao, Netherlands Antilles.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Dated this 3 day of December 2010 at Shuman Oaks, California.


David C. Parisi