

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

NOBOTS LLC
Patent Owner.

Case No. IPR2022-00940
Patent No. 9,595,008

**PETITION FOR INTER PARTES REVIEW
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.1 et seq.**

Nobots LLC - Ex. 2004 IPR2026-00429 Google LLC v. Nobots
--

TABLE OF CONTENTS

MANDATORY NOTICES.....	x
A. Real Party-In-Interest	x
B. Related Matters.....	x
1. United States Patent & Trademark Office	x
2. United States Patent Trial and Appeal Board	x
3. U.S. District Court for the Western District of Texas.....	xi
C. Counsel/Service Information – 37 C.F.R. §§ 42.8(b)(3)-(4).....	xi
I. GROUNDS AND STANDING.....	1
II. THE '008 PATENT	1
A. Described Embodiments.....	1
B. Claims	3
C. POSA	4
D. Prosecution History and Claim Interpretation.....	4
III. GROUND 1: WILLNER ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 1-3, 6-18	6
A. Willner	6
B. Claim 1	9
1. [1PRE] “A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application,”	9
2. [1A] “the method comprising: a) a single user of a client computing device requesting data from a server;”	9
3. [1B] “b) the server presenting data issued by the server to the client computing device;”	10
4. [1C] “c) monitoring at least some data generated by the user at the client computing device in response to the issued data;”	11
5. [1D] “d) comparing the monitored data to model data relating to human interaction with or in response to the issued data;”	11

6. [1E] “e) generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.”	14
C. Claim 2: “The method of claim 1 wherein the model data comprises active model data.”	16
D. Claim 3: “The method of claim 2 wherein the active model data comprises pointing device vector movements and/or cadence; key stroke combinations and/or cadence; and/or time differentials between a display element and a response.”	17
E. Claim 6: “The method of claim 1 wherein b) comprises enabling the client computing device to record input and making such recorded input available to a computing device for comparison according to c).”	17
F. Claim 7: “The method of claim 6 wherein the computing device is the server.”	18
G. Claim 8: “The method of claim 6 wherein the computing device is the client computing device.”	19
H. Claim 9: “The method of claim 6 wherein the computing device is neither the server or the client computing device.”	19
I. Claim 10: “The method of claim 6 wherein the recorded input comprises active model data and the recorded input is delivered to a computing device that is not the client computing device.”	19
J. Claim 11: “The method of claim 1 wherein at least one monitoring program is operatively installed on the client computing device to perform b).”	20
K. Claim 12: “The method of claim 1 wherein d) is performed by neither the server nor the client computing device.”	20
L. Claim 13: “The method of claim 1 wherein at least some issued data is not data specific to determination of the user status.”	21

M. Claim 14: “The method of claim 1 wherein the issued data is in specific response to a request issued by the client computing device.”	23
N. Claim 15: “The method of claim 1 further comprising modifying data delivered to the client computing device subsequent to reaching a predetermined value for d) is reached.”	23
O. Claim 16: “The method of claim 1 further comprising repeating a)-d) for a single user instance.”	24
P. Claim 17: “The method of claim 1 further comprising repeating a)-d) for a single user instance until a predetermined value for d) is reached.”	26
Q. Claim 18: “The method of claim 1 further comprising repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d).”	26
IV. GROUND 2: CLAIMS 1-18, 20 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS	27
A. Kitts.....	27
B. Willner-Kitts Combination.....	28
C. Claims 1-3, 6-18	29
D. Claim 4: “The method of claim 1 wherein the model data comprises passive model data.”	30
E. Claim 5: “The method of claim 4 wherein the passive model data comprises browser cookies; destination IP histories; originating IP address; originating IP address traffic data; originating IP address physical location; and/or third party data regarding abusers comprising originating IP addresses and physical locations.”	31
F. Claim 20: “The method of claim 1 wherein the interest data consists of available data.”	32
V. GROUND 3: O’CONNELL ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 1-18, 20.....	33
A. O’Connell	33
B. Claim 1	34

C. Claim 2	39
D. Claim 3	40
E. Claim 4	40
F. Claim 5	42
G. Claim 6	42
H. Claim 7	43
I. Claim 8	44
J. Claim 9	44
K. Claim 10	44
L. Claim 11	45
M. Claim 12	45
N. Claim 13	45
O. Claim 14	46
P. Claim 15	46
Q. Claim 16	47
R. Claim 17	48
S. Claim 18	49
T. Claim 20	49
VI. GROUND 4: CLAIMS 1-18, 20 WOULD HAVE BEEN OBVIOUS OVER O’CONNELL IN VIEW OF KITTS	50
A. O’Connell-Kitts Combination	50
B. Claims 1-3, 6-18	51
C. Claim 4	51
D. Claim 5	52
E. Claim 20	52
VII. GROUND 5: KITTS ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 19-20.....	52
A. Claim 19	52
1. [19PRE]: “A method for assessing a confidence level that an operator of a client computing device interacting with a	

server is a human being rather than an autonomic computer application, the method comprising:”	52
2. [19A]: “a) acquiring interest data from the client computing device prior to delivery of issued data by the server to the client computing device;”	55
3. [19B]: “b) comparing the interest data to model data relating to human interaction with a computing device prior to the time in which the interest data is acquired; and”	57
4. [19C]: “c) generating a value that represents a confidence level that a human user rather than an autonomic user operated the client computing device prior to the time in which the interest data is acquired.”	59
B. Claim 20	60
VIII.NO BASIS EXISTS FOR DISCRETIONARY DENIAL	61
A. Section 314(a).....	61
B. Section 325(d).....	66
IX. CONCLUSION.....	67
APPENDIX: CLAIM LISTING	68

TABLE OF AUTHORITIES

CASES

<i>Advanced Bionics, LLC v. MED-El Elektromedizinische Geräte GmbH,</i> IPR2019-01469, Paper 6 (Feb. 13, 2020).....	66, 67
<i>Align Tech., Inc. v. 3Shape A/S,</i> IPR2021-01309, Paper 11 (Feb. 9, 2022).....	66
<i>Apple Inc. v. Fintiv, Inc.,</i> IPR2020-00019, Paper 11 (Mar. 20, 2020).....	61, 62, 63, 65
<i>Apple Inc. v. Parus Holdings, Inc.,</i> IPR2020-00687, Paper 9 (Sep. 23, 2020).....	64
<i>Apple Inc. v. Seven Networks, LLC,</i> IPR2020-00235, Paper 10 (July 28, 2020).....	63
<i>Bose Corp. v. Koss Corp.,</i> IPR2021-00297, Paper 16 (June 3, 2021)	62
<i>Dish Network, L.L.C. v. Broadband iTV, Inc.,</i> IPR2020-01280, Paper 17 (Feb. 4, 2021).....	62, 63, 64
<i>Godbersen-Smith Constr. Co. v. Guntert & Zimmerman Const. Div., Inc.,</i> IPR2021-00050, Paper 24 (May 7, 2021)	66
<i>HP Inc. v. Neodron Ltd.,</i> IPR2020-00459, Paper 17 (Sept. 14, 2020)	64
<i>Hulu, LLC v. SITO Mobile R&D IP, LLC,</i> IPR2021-00298, Paper 11 (May 19, 2021)	64
<i>Hyundai Motor Am. v. Stratosaudio, Inc.,</i> IPR2021-01267, Paper 9 (Jan. 25, 2022)	63, 64
<i>IBM Corp. v. Trusted Knight Corp.,</i> IPR2020-00323, Paper 15 (July 10, 2020).....	64
<i>In re Apple Inc.,</i> 979 F.3d 1332 (Fed. Cir. 2020)	61

<i>KioSoft Techs. LLC v. TechTrex, Inc.</i> , PGR2021-00093, Paper 12 (Dec. 17, 2021).....	62, 65
<i>Microchip Tech. Inc. v. HD Silicon Sol’ns LLC</i> , IPR2021-00752, Paper 9 (Nov. 9, 2021).....	64
<i>Micron Tech., Inc. v. Vervain, LLC</i> , IPR2021-01550, Paper 11 (April 11, 2022)	65
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	5
<i>Samsung Elecs. Am., Inc. v. Proxense, LLC</i> , IPR2021-01438, Paper 12 (Feb. 28, 2022).....	65
<i>Samsung Elecs. Co., Ltd. v. Collect, LLC</i> , IPR2020-00477, Paper 14 (Aug. 5, 2020).....	66, 67
<i>Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC</i> , IPR2019-01393, Paper 24 (June 16, 2020)	61, 63, 65

STATUTES

35 U.S.C. § 102(a)	1
35 U.S.C. § 102(e)	1
35 U.S.C. § 282(b)	5
35 U.S.C. § 325(d)	66, 67

REGULATIONS

37 C.F.R. § 42.100(b)	5
37 C.F.R. § 42.104(a).....	1

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,595,008 (“the ’008 patent”)
1002	Prosecution History of U.S. Patent No. 9,595,008
1003	Declaration of Daniel P. Lopresti, Ph.D. (“Lopresti-Declaration”)
1004	Curriculum Vitae of Daniel P. Lopresti, Ph.D.
1005	U.S. Patent Application Publication No. 2009/0024971 (“Willner”)
1006	U.S. Patent Application Publication No. 2008/0319774 (“O’Sullivan”)
1007	U.S. Patent Application Publication No. 2007/0239604 (“O’Connell”)
1008	U.S. Patent Application Publication No. 2005/0278253 (“Meek”)
1009	U.S. Patent Application Publication No. 2008/0114624 (“Kitts”)
1010	RESERVED – NOT USED
1011	U.S. Patent Application Publication No. 2008/0147456 (“Broder”)
1012	U.S. Patent Application Publication No. 2007/0255818 (“Tanzer”)
1013	U.S. Patent Application Publication No. 2008/0086524 (“Afergan”)
1014	U.S. Patent Application Publication No. 2007/0255821 (“Ge”)
1015	U.S. Patent No. 8,838,570 (“English”)
1016	U.S. Patent No. 7,089,241 (“Alspector”)
1017	RESERVED – NOT USED
1018	RESERVED – NOT USED
1019	RESERVED – NOT USED
1020	RESERVED – NOT USED
1021	U.S. Provisional Application No. 61/003,743
1022	<i>Nobots LLC v. Google LLC</i> , Case No. 6:21-cv-01290-ADA (W.D. Tex.), Civil Docket (last checked April 27, 2022)
1023	<i>Nobots LLC v. Google LLC</i> , Case No. 6:21-cv-01290-ADA (W.D. Tex.), Docket Item 1: Complaint for Patent Infringement (Dec. 13, 2021)
1024	<i>Nobots LLC v. Google LLC</i> , Case No. 6:21-cv-01290-ADA (W.D. Tex.), Docket Item 33: Google’s Opposed Motion To Transfer Venue to the Northern District of California Under 28 U.S.C. § 1404(a) (Mar. 30, 2022)
1025	<i>Nobots LLC v. Google LLC</i> , Case No. 6:21-cv-01290-ADA (W.D. Tex.), Docket Item 38: Scheduling Order (April 18, 2022)

Exhibit	Description
1026	Andrew T. Dufresne, et al., <i>How Reliable Are Trial Dates Relied on by the PTAB in the Fintiv Analysis?</i> , https://www.1600ptab.com/2021/10/how-reliable-are-trial-dates-relied-on-by-the-ptab-in-the-fintiv-analysis/ (Oct. 29, 2021) (last checked April 27, 2022)
1027	Scott McKeown, <i>District Court Trial Dates Tend to Slip After PTAB Discretionary Denials</i> , https://www.patentspostgrant.com/district-court-trial-dates-tend-to-slip-after-ptab-discretionary-denials/ (July 24, 2020) (last checked April 27, 2022)
1028	Open Patent Matters Before J. Albright (W.D. Tex.) Not on Appeal, Lex Machina, https://law.lexmachina.com (last checked April 27, 2022)
1029	Open Patent Matters Before J. Albright (W.D. Tex.) Not on Appeal Filed Before December 13, 2021, Lex Machina, https://law.lexmachina.com (last checked April 27, 2022)
1030	Eighth Supplemental General Order Regarding Emergency Procedures Authorized by the Coronavirus Aid, Relief, and Economic Security Act, H.R. 748, P.L. 116-136, 134 Stat. 281, (Cares Act) Including the Use of Video and Telephonic Conference for Various Criminal Events During the COVID-19 Emergency (C.J. Garcia) (Mar. 14, 2022)
1031	Fourteenth Supplemental Order Regarding Court Operations Under the Exigent Circumstances Created by the Covid-19 Pandemic (C.J. Garcia) (Mar. 17, 2021)
1032	Amended Standing Order Regarding Coronavirus (COVID-19) and Court Proceedings (J. Albright) (Mar. 7, 2022)
1033	Ninth Standing Order Relating to Entry Into the Waco United States Courthouse due to the Corona Virus/COVID-19 Pandemic (J. Albright) (Mar. 22, 2021)
1034	Divisional Standing Order Regarding Trials in Waco (J. Albright) (Sep. 23, 2020)
1035	Sixteenth Order Relating to Entry Into the United States Courthouse, Austin, Texas (J. Yeakel & J. Pitman) (Jan. 10, 2022)
1036	April 29, 2022 Letter from Google Counsel to Nobots Counsel in W.D. Tex. Litigation

MANDATORY NOTICES

A. Real Party-In-Interest

Petitioner Google LLC is the real party-in-interest.¹

B. Related Matters

1. United States Patent & Trademark Office

The application from which U.S. Patent No. 9,595,008 issued claims priority to U.S. Provisional Application No. 61/003,743, filed November 19, 2007.

The following U.S. patent applications also claim the benefit of priority of the filing date of U.S. Provisional Application No. 61/003,743:

(i) U.S. Patent Application No. 15/457,099, filed March 13, 2017, now U.S. Patent No. 10,423,885;

(ii) U.S. Patent Application No. 16/578,823, filed September 23, 2019.

2. United States Patent Trial and Appeal Board

Concurrently with the present Petition, Petitioner is filing a petition for *inter partes* review of related U.S. Patent No. 10,423,885, under case no. IPR2022-00941. Petitioner requests that both petitions be reviewed by the same panel, as the patents are commonly assigned and share the same specification.

¹ Google LLC is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc. XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.

3. U.S. District Court for the Western District of Texas

Nobots LLC v. Google LLC, Civil Action No. 6:21-cv-01290

C. Counsel/Service Information – 37 C.F.R. §§ 42.8(b)(3)-(4)

Lead Counsel	Elisabeth H. Hunt, Reg. No. 67,336
Backup Counsel	Richard F. Giunta, Reg. No. 36,149
Service Information	<u>E-mail</u> : EHunt-PTAB@wolfgreenfield.com RGiunta-PTAB@wolfgreenfield.com <u>Post and hand delivery</u> : Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210-2206 <u>Telephone</u> : 617-646-8000 <u>Facsimile</u> : 617-646-8646

A power of attorney is submitted with the Petition. Counsel for Petitioner consents to service of all documents via electronic mail.

I. GROUNDS AND STANDING

All claims (1-20) of U.S. Patent 9,595,008 (“the ’008 patent”) are unpatentable according to the following grounds.

Ground Number and Reference(s)		Claims	Basis
1	Willner (Ex. 1005)	1-3, 6-18	102/103
2	Willner, Kitts (Ex. 1009)	1-18, 20	103
3	O’Connell (Ex. 1007)	1-18, 20	102/103
4	O’Connell, Kitts	1-18, 20	103
5	Kitts	19-20	102/103

Each reference above is prior art under pre-AIA 35 U.S.C. § 102(e) (and O’Connell additionally under § 102(a)) even to the ’008 patent’s earliest claimed priority date.

Petitioner certifies that the ’008 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review as to the challenged claims. 37 C.F.R. § 42.104(a).

II. THE ’008 PATENT

A. Described Embodiments

The ’008 patent describes methods for assessing whether a computing device interacting with a server is being operated by a human or instead by an automated program (a.k.a. “bot”). Ex. 1001 (“’008-patent”), 1:7-16, 2:12-18. Website builders often employ “a variety of tests” to detect and block bots from accessing a website server to “create fictitious accounts or access content” for

“abus[ive]” reasons. ’008-patent, 1:7-16. One well-known test is “CAPTCHA,” which “requir[es] the human user to answer a test that should be simple to most humans but difficult for non-humans, e.g., bots.” ’008-patent, 1:54-60.

The ’008 patent attempts to avoid requiring all users to answer CAPTCHAs by instead assessing “acquired and/or available data relating to the [user’s] operation of the computing device,” such as “user biometrics” including “mouse movements and/or key strokes inputted by the user...attempting to access [the] server.” ’008-patent, 1:65-2:33, 4:44-53. If the biometrics (which are “acquired” “active data”—2:60-3:32) from the device attempting access are inconsistent with human activity patterns, that “would indicate the potential that the user is a bot,” and “[a]ccess could then be denied, or further CAPTCHA tests presented.” ’008-patent, 5:22-31. Alternatively/additionally, “available” “passive data” such as the device’s “browser cookies, destination IP histories, originating IP address, [etc.]” may be compared with “model data” relating to human interaction. ’008-patent, 2:54-3:60.

Such techniques were not new in the ’008 patent. Ex. 1003 (“Lopresti-Declaration”), [0041]-[0043]. For example, O’Connell had already disclosed an alternative to CAPTCHA for “detect[ing] fraud by...automated programs during Internet commerce,” by “comparing the user’s interaction” including “keyboard interactions, movement device [e.g., mouse] interactions, and navigation/selection

tendencies” as well as “[i]dentification information” including “IP address...and cookies.” O’Connell, [0005], [0020], [0027]-[0029]. *See* Grounds 3-4 below. And Willner had likewise disclosed detecting fraud by “automated scripts (clickbots)” by “tracking the movement of a [mouse] cursor on a web page” “to determine if the cursor movement is human-like.” Willner, [0004]-[0006], [0047]. *See* Grounds 1-2 below. Kitts had disclosed detecting “click fraud” perpetrated by “various automated methods” by analyzing “attributes” including the “internet protocol (IP) address of the client-computing device [],...geographic location,...web history,...etc.” via “statistical models” to determine “a probability that the request is originating from an automated system.” Kitts, [0003]-[0005], [0021], [0046], [0049]. *See* Ground 5 below. Indeed, the prior art discussed herein provided far greater detail than the ’008 patent does regarding *how* to use biometrics and other collected data to distinguish human users from bots. Lopresti-Declaration, [0043].

B. Claims

The ’008 patent contains two independent claims (1 and 19) directed to different embodiments. The specification explains, “In a first series of embodiments, a comparison between interest data” (active or passive data) “acquired *prior to* delivery of issued data to the client computing device, and model data is performed to ascertain...human user or bot,” as in claim 19. “[A]

second series of embodiments” uses “monitored data...acquired *after* delivery of issued data,” as in claim 1. ’008-patent, 3:48-58;² Lopresti-Declaration, [0047].

Grounds 1-4 below address claim 1 and its dependents; Ground 5 addresses claim 19.

C. POSA

A person of ordinary skill in the art (“POSA”) would have had a bachelor’s degree in computer science or a related field with coursework relating to computer science, plus two years’ academic and/or industry experience in computer security. More education could substitute for experience, and vice versa. Lopresti-Declaration, [0036]-[0040].

D. Prosecution History and Claim Interpretation

The ’008 patent’s originally examined claims were rejected as anticipated by “Sundstrom.” Ex. 1002 at 53-56. In response, the applicant amended the claims to replace “assessing the likely user status of a client computing device” with “assessing a confidence level that an operator of a client computing device...is a human being rather than an autonomic computer application,” and argued that “Sundstrom merely discusses...predicting a likelihood that a first user will initiate communication with a second user” and “is silent as to **any** distinction between

² Emphases in this Petition are added unless otherwise indicated.

human and autonomic users.” *Id.* at 77, 82-84 (emphasis original). The examiner allowed the amended claims without explanation. *Id.* at 105-109.

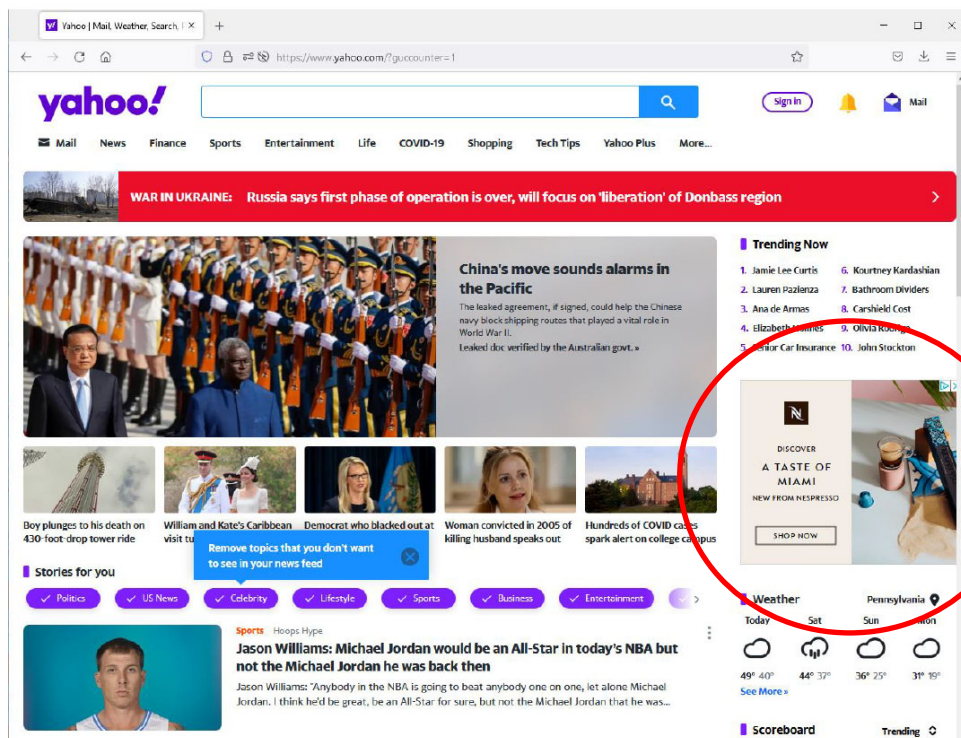
The applicant’s amendment also added a new step “a)” to what became claim 1, and original steps “a)”-“d)” became steps “b)”-“e)” respectively. However, dependent claims 6, 11-12, and 15-18 that refer to original steps “a)”-“d)” were never updated. *Id.* at 77-81. The Board need not decide between the possible interpretations of those dependent claims (e.g., whether “b” in claim 11 refers to [1B] or [1C]), because this Petition’s grounds meet the claims under both interpretations. Lopresti-Declaration, [0044]-[0045]. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“we need only construe terms...only to the extent necessary to resolve the controversy”).

Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. § 282(b), in accordance with the ordinary and customary meaning as understood by a POSA and the patent’s prosecution history. 37 C.F.R. § 42.100(b). This Petition applies the meanings of “model data,” “available data,” “issued data,” “monitored data,” and “interest data” described in the ’008 patent at 2:54-3:46.

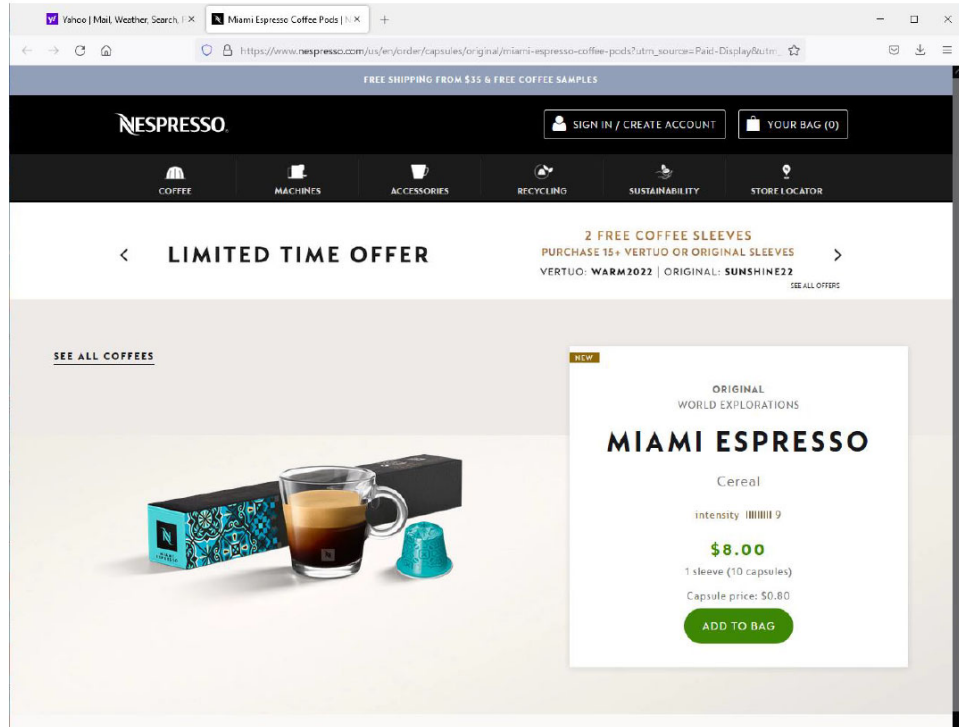
III. GROUND 1: WILLNER ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 1-3, 6-18

A. Willner

Willner describes techniques for detecting “click fraud,” which is a known problem in “Pay Per Click (PPC)” systems of Internet advertising. Willner, Abstract, [0001]-[0002]. PPC advertisers place clickable advertisements on a publisher’s website (e.g., Yahoo), and pay the publisher for each “click through” whereby a user clicks on the advertisement and is referred to the advertiser’s website. Willner, [0002]; Lopresti-Declaration, [0053]-[0055] (providing example screenshots below).



(Yahoo website with Nespresso advertisement)



(Nespresso website displayed on click of advertisement)

“Click Fraud may be accomplished via automated scripts (clickbots)” that “repeatedly generate[] clicks to a PPC advertisement with the intent of generating an improper charge to the Advertiser.” Willner, [0003]-[0004]. To detect and block such click fraud, Willner tracks “movement of a cursor on [the] web page” to determine whether “a human is involved, as opposed to an automated tool,” in “mov[ing] their mouse (thus moving the cursor)” to click on the advertisement. Willner, Abstract, [0006], [0033]; Lopresti-Declaration, [0056].

Recognizing that “[i]t would be virtually impossible for a human controlling a...mouse[] to move the cursor...in a perfectly straight line,” Willner analyzes “a pattern...in the vectors defining the path...to determine if the cursor movement is

human-like.” Willner, [0047]. Willner’s Figure 2 illustrates a “human-like cursor movement” path 211 which “includes a series of multiple vectors,” unlike the “perfectly straight line” 311 in Figure 3 which indicates “click fraud cursor movement...generated by software...or...automation tool.” Willner, [0046]-[0048].

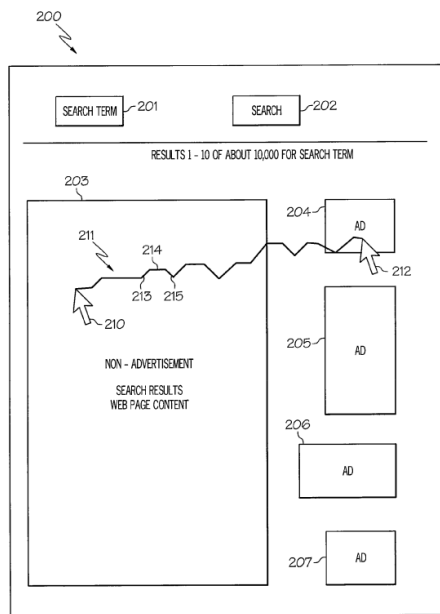


FIG. 2

(human movement)

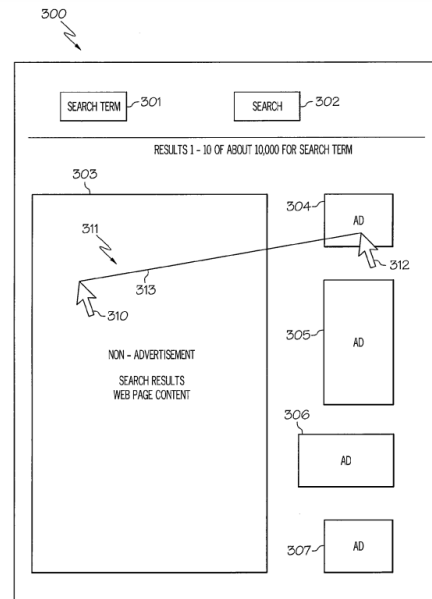


FIG. 3

(clickbot movement)

Willner’s techniques “exploit the stochastic pattern in [human] cursor movement vectors” that are difficult for clickbots to simulate. Willner, [0031]-[0033]. “[O]nly when cursor movement vector analyses...demonstrate[] a pattern as being consistent with a human” is the advertiser’s webpage displayed and the advertiser charged for the click through. Willner, [0036], [0045]. Lopresti-Declaration, [0057]-[0058].

B. Claim 1

1. [1PRE] **“A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application,”**

To the extent the preamble is limiting, Willner discloses it. In Willner’s “*method*,” a “*confidence level* useable in the determination of click fraud is determined.” Willner, Abstract, “*method*” claims 1-11, claim 1 (“determining a *confidence level*”), claim 3 (“determining a *confidence* factor as to...*human*-like manipulations”). The confidence level is assessed to determine whether “a *human* is involved, as opposed to an *automated tool*” ([0033]-[0036], [0047]-[0056]) such as “*software* in a *computer*” ([0048], [0004]-[0005] (“automated scripts (clickbots)”), in operating (“control[ing]” cursor movements of ([0045])) a “*client*” “*computing type device*” to “access the website hosted on the *server*” ([0009], [0022], [0041]-[0044], [0054], FIGs. 1, 7). Lopresti-Declaration, [0065]-[0073].

2. [1A] **“the method comprising: a) a single user of a client computing device requesting data from a server;”**

Willner’s method comprises a single user of client computing device 101 requesting webpage data from server 102. Willner, FIG. 7, [0040]-[0044] (“*A...user* may access the website hosted by the server 102...using a workstation 101 or other computing type device” with “browser 130”) (“workstation 101 (i.e., client device)”), [0033]-[0038] (discussing determining whether the singular “*a* user”/“*the* user” is “*a* human”); Lopresti-Declaration, [0074] (also citing Kitts,

[0001], [0041], [0067], corroborating POSA's knowledge that "client-computing device" navigating to publisher's webpage via browser is "a *request* for [the] web page").

3. [1B] "b) the server presenting data issued by the server to the client computing device;"

The '008 patent defines "issued data" as comprising "data generated by a server or other computing device that is not the same as the computing device for which the assessment as to user status is being performed." '008-patent, 3:33-37.

Willner's "server 102 generates and downloads the web page" 200/300 to "client device" 101's browser. Willner, [0042]; Lopresti-Declaration, [0075]-[0076]. The webpage includes advertisement(s) and "may include markup that enables the cursor tracking," or server 102 may "download[] code (e.g., applets, activeX, Javascript, etc.)" to client 101 to perform the tracking. Willner, [0042], [0046]; Lopresti-Declaration, [0076]. The webpage, markup, and downloaded code are each issued data generated by the server (or by another computing device from which the server obtains them) which is not the same as the client device whose user's status is being assessed as human vs. clickbot. Lopresti-Declaration, [0076].

4. [1C] “c) monitoring at least some data generated by the user at the client computing device in response to the issued data;”

Willner’s method monitors data (i.e., mouse movement data) generated by the client device’s user in response to the downloaded webpage (the claimed “issued data”). Willner, [0045] (“The web pages...use cursor transit *monitoring* to prevent click fraud from occurring on advertisements displayed on the website. In this regard, the server tracks a path of a cursor movement...on the web page towards an advertisement.”), [0033] (“When a *user* moves their mouse...there are a set of vectors established prior to click based on the trajectory that the cursor has taken”), [0043] (“the transit info[] may be sent from...*client device* 101 to a server...that will analyze this information”), Abstract, [0006]-[0011], [0042]-[0054], claims 1, 12, 17; Lopresti-Declaration, [0077].

5. [1D] “d) comparing the monitored data to model data relating to human interaction with or in response to the issued data;”

Willner compares its monitored data (cursor movement) to model data in two ways.

In one aspect (FIG. 5, FIG. 8 steps 807-808), the vectors of the monitored cursor movement are “compar[ed]...with previously stored vector data” from prior cursor click paths by “different users (or the same user).” Willner, [0055]-[0056], [0037]-[0038], claims 7-10, 13-16, 18-19; Lopresti-Declaration, [0078]-[0079].

Because “duplication of vector patterns” does not occur in true human movements, monitored paths having “analogous vector data” to previously stored paths are “dismissed as an automation tool attempting to simulate the actions of a user” to commit click fraud. Willner, [0037]-[0038], [0051], [0056]; Lopresti-Declaration, [0079].

Willner’s previously-stored vector data meet the claimed “model data relating to human interaction with or in response to the issued data.” The vector data were stored when previous users (some of which may be human, e.g., “User A”) interacted with or in response to the webpage and monitoring markup/code (the claimed “issued data”) by clicking on advertisements. Willner, [0037]-[0038]; Lopresti-Declaration, [0080]. The ’008 patent defines “model data” to broadly mean “data indicative of human interaction with a computing environment and that can be received by a computing device that is physically remote from the sample computing environment and equivalents.” ’008-patent, 2:54-58. A POSA would have understood Willner ([0037]-[0038]) to describe that the previously stored vector data can be received by the website server which is physically remote from the users’ sample computing environments (e.g., workstations 101, 103) that access server 102 via the Internet 110, or alternatively that this would have been the obvious way to implement what Willner describes. Willner, FIG. 1; Lopresti-Declaration, [0081].

In another aspect (FIG. 4, FIG. 8 steps 803-806), Willner compares the monitored cursor movement vectors to data indicative of “a human-like pattern” having “multiple vectors having random and/or various slopes/angles.” Willner, [0049], [0036] (“allow a click only when cursor movement vector analyses has demonstrated a pattern as being consistent with a human, denoted by...a discernible set of movement vectors”), [0047] (“a pattern may be analyzed in the vectors...to determine if the cursor movement is human-like”—e.g., “[a] path that includes a series of multiple vectors”), [0050] (“subset of vectors with differing slopes/angles...suggest[s] no click fraud”), [0055] (“determine if the pattern shows a human-like cursor movement (e.g., set of vectors...hav[ing] various different slopes and/or angles)"); Lopresti-Declaration, [0082].

Willner thus “detect[s] click fraud by using *vector analyses/patterns from conventional systems’ usage patterns* that are difficult to generate in automated tools. Specifically,...knowledge of the behaviors of how users use computer systems is taken advantage of.” Willner, [0031]. A POSA would have understood Willner to teach comparing the monitored movement vectors to stored data indicating what vector patterns are human-like in interaction with or in response to the webpage and monitoring markup/code, meeting the claimed “model data relating to human interaction with or in response to the issued data.” Lopresti-Declaration, [0083]. A POSA would have understood Willner to disclose that the

stored “vector analyses/patterns from conventional systems’ usage patterns” representing “the behaviors of how users use computer systems” (Willner, [0031]) can be received by the server which is physically remote from sample client computing environments from which those users’ movement vectors are recorded in the disclosed “conventional systems,” or alternatively that this would have been an obvious way to implement what Willner describes. Lopresti-Declaration, [0083].

6. [1E] **“e) generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.”**

Willner’s analysis of the monitored cursor movement generates a “*confidence level* useable in the determination of click fraud.” Willner, Abstract, FIGs. 4-8. “The confidence factor can be used...to allow a click only when cursor movement vector analyses has demonstrated a pattern as being consistent with a *human*.” Willner, [0036]. If “the cursor movement is a human-like movement,...a high confidence factor may be determined suggesting no click fraud;” “if not,...a low confidence factor may be determined suggesting a possible click fraud attempt.” Willner, [0050], [0055]. Further, if comparing the monitored movement vectors to previously stored vectors “results in a match,” Willner “provid[es] a confidence factor indicative of click fraud” (Willner, claims 7-8) by

“an automation tool attempting to simulate the actions of a user” (Willner, [0038]).

Willner thus generates a confidence level that the monitored data is the result of human interaction on the client device rather than that of an autonomic user (e.g., clickbot) with or in response to the issued webpage and monitoring markup/code.

Willner, claim 3 (“determining a confidence factor as to whether the movement was produced by human-like manipulations”); Lopresti-Declaration, [0084].

A POSA would also have understood Willner to describe that the confidence level is represented as a generated “value” as claimed, for example because Willner repeatedly describes the confidence level being “low” for fraudulent patterns and “high” for human-like patterns. Willner, FIGs. 4-5, 8, [0049]-[0051], [0055]; Lopresti-Declaration, [0085]. Alternatively, a POSA would have understood generating a value to be a straightforward, conventional, and obvious way of representing the confidence level in Willner’s computer-implemented system. Lopresti-Declaration, [0085] (citing Ex. 1013 (“Afergan”), [0040], [0155], corroborating POSA’s background knowledge that a score “that represents a confidence value” regarding whether “the user agent is associated with a human user or an automated agent” “may be represented as a number, a percentage, a code, or in any other convenient symbol, character or representation”).

C. Claim 2: “The method of claim 1 wherein the model data comprises active model data.”

The '008 patent (2:60-3:9) says:

Active model data comprises data acquired from a computing device user's interactions therewith and within the computing environment where such data is not normally stored (logged) or transmitted to a remote location. Such model data includes, without limitation, *pointing device vector movements* and/or cadence,...time differentials between stimulus...and user response..., and similar metrics. Generally, such data must be monitored and stored...by a program operative on the computing device, which makes the data available to another program, preferably on a server..., or actively transmits such data to a server.

As discussed *supra* §§ III.B.5-III.B.6 ([1D]-[1E]), Willner uses model data regarding “cursor *movement vectors* (e.g., those initiated by a *pointing device* such as a mouse) to establish that a human is involved, as opposed to an automated tool.” Willner, [0033], [0040], [0045]-[0048], FIGs. 2-3. Willner also monitors and analyzes “signature information” for “web page viewing duration timing” up to the user's click to “judge whether or not this was click fraud,” which a POSA would have understood to describe comparing the monitored timing to timing model data. Willner, [0042]-[0043]; Lopresti-Declaration, [0087]. The '008 patent explicitly states that such “pointing device vector movements and/or

cadence” and “time differentials between stimulus...and user response” are “active model data” as claimed. ’008-patent, 2:64-3:5; Lopresti-Declaration, [0086]-[0087]. Further, a POSA would have understood that these data are acquired from the user’s interactions with the client device and not normally stored or remotely transmitted, because they are instead monitored and stored by “software code on the...client device...downloaded from the server...or added to the browser by extension” which sends the data to a server. Willner, [0042]-[0043]; Lopresti-Declaration, [0087].

D. Claim 3: “The method of claim 2 wherein the active model data comprises pointing device vector movements and/or cadence; key stroke combinations and/or cadence; and/or time differentials between a display element and a response.”

As discussed *supra* § III.C (claim 2), Willner’s active model data includes pointing-device and time-differential data, either of which meets claim 3 which recites “and/or.” Lopresti-Declaration, [0088].

E. Claim 6: “The method of claim 1 wherein b) comprises enabling the client computing device to record input and making such recorded input available to a computing device for comparison according to c).”

Willner meets claim 6 whether the recited “b)” and “c)” refer to [1B]-[1C] or [1C]-[1D]. *See supra* § II.D.

Willner meets [1B] by downloading markup/code to the client, and [1C] by the markup/code tracking cursor movement data. *Supra* §§ III.B.3-III.B.4. Both

steps thus enable the client device to record input (cursor movement data) and make it available to a server computing device for comparison. Willner, [0009]-[0010] (code on client device tracks cursor movement made via “*input* interface”), [0042]-[0043] (cursor input tracked by markup/code is “sent from...client device 101 to a server...that will analyze this information and judge whether or not this was click fraud”); Lopresti-Declaration, [0089]-[0090]. A POSA would have understood from the disclosure of tracking, sending, and analyzing the input data that the input is recorded. Lopresti-Declaration, [0090]. The ’008 patent contains no definition or limiting description of “record” that would exclude Willner’s described tracking, transmission, and analysis, which a POSA would have understood involve at least temporary data storage. Lopresti-Declaration, [0090]. Willner meets [1C] by tracking the input data and [1D] by comparing the tracked data to model data (*supra* §§ III.B.4-III.B.5); thus the client records input and makes it available for comparison “according to” both steps. Lopresti-Declaration, [0090].

F. Claim 7: “The method of claim 6 wherein the computing device is the server.”

Willner’s comparison of tracked cursor movements to model data can be “performed by a server hosting the web page” meeting the claimed “server” (*supra* §§ III.B.1-III.B.3). Willner, [0008], [0043] (“the hosting server 102 may be same as the server that judges”), [0053] (“the *publisher’s server*...may analyze a pattern

in the set of vectors and determine a confidence level and/or if click fraud is occurring”), FIG. 6 step 605; Lopresti-Declaration, [0091].

G. Claim 8: “The method of claim 6 wherein the computing device is the client computing device.”

Willner’s tracking and comparison can alternatively be “performed by client code on [the] client device.” Willner, [0009], [0042] (“cursor path vector processing may all be done in software code on the...client device”), [0054] (“*client code* may analyze a pattern in the set of vectors and determine a confidence factor indicative of click fraud”), FIG. 7; Lopresti-Declaration, [0092].

H. Claim 9: “The method of claim 6 wherein the computing device is neither the server or the client computing device.”

Willner teaches that, alternatively, the “server 104, 106...performing the analysis may be a different server from the server 102 hosting the web page” and may be “an outside entity for analysis and/or determination of a confidence level or a possible click fraud.” Willner, [0043], [0053], FIG. 6 step 606; Lopresti-Declaration, [0093].

I. Claim 10: “The method of claim 6 wherein the recorded input comprises active model data and the recorded input is delivered to a computing device that is not the client computing device.”

As discussed *supra* § III.E (claim 6), Willner’s recorded input comprises pointing device vector movements, which are active model data as discussed *supra* § III.C (claim 2). Willner describes delivering the recorded input to a server

computing device that is not the client for analysis, as discussed *supra* §§ III.F, III.H (claims 7, 9). Lopresti-Declaration, [0094].

J. Claim 11: “The method of claim 1 wherein at least one monitoring program is operatively installed on the client computing device to perform b).”

The '008 patent says, “Existing available browsers and operating systems provide the means necessary to temporarily install logging code” on the client, where such “monitoring...means” include “modification of (an) existing program(s) (e.g., such means are included in available browsers), a covert program..., or a servlet/Java applet.” '008-patent, 4:29-35, 4:3-15.

Willner operatively installs the same types of monitoring programs on the client device, including webpage markup, browser code/add-ins, applets, activeX, Javascript, or other downloadable code. Willner, [0042]; *supra* §§ III.B.3, III.G ([1B], claim 8); Lopresti-Declaration, [0096]-[0097]. Willner describes installing the monitoring programs as part of issuing data to the client ([1B]) and monitoring user-generated data ([1C]). *Supra* §§ III.B.3-III.B.4; Lopresti-Declaration, [0095]-[0097].

K. Claim 12: “The method of claim 1 wherein d) is performed by neither the server nor the client computing device.”

As discussed *supra* §§ III.B.5-III.B.6, III.H, Willner describes the “analysis and/or determination of a confidence level” (meeting [1D]-[1E]) being performed

by “an outside entity” that is neither the claimed “server” 102 nor the client device 101. Willner, [0053], [0043]; Lopresti-Declaration, [0098]-[0099].

L. Claim 13: “The method of claim 1 wherein at least some issued data is not data specific to determination of the user status.”

The ’008 patent’s specification does not describe or define how issued data may be “not...specific to determination of the user status.” Lopresti-Declaration, [0100].

As discussed *supra* § III.B.3 ([1B]), Willner’s issued data includes a webpage served to the client device. In the example webpages of FIGs. 2-3, determination of the user’s status as human or clickbot involves tracking the cursor path 211/311 toward advertisement 204/304. *Supra* §§ III.A, III.B.4-III.B.6; Lopresti-Declaration, [0101]. The webpages also include some issued data that is not data specific to determination of the user status because it is not considered in monitoring the cursor movement, including the specific “search results web page content” (e.g., the particular text within box 203/303), “search term” 201/301, “search” button 202/302, advertisements 205-207/305-307 that are not clicked, the specific text/image content of the displayed advertisements, etc. Lopresti-Declaration, [0101].

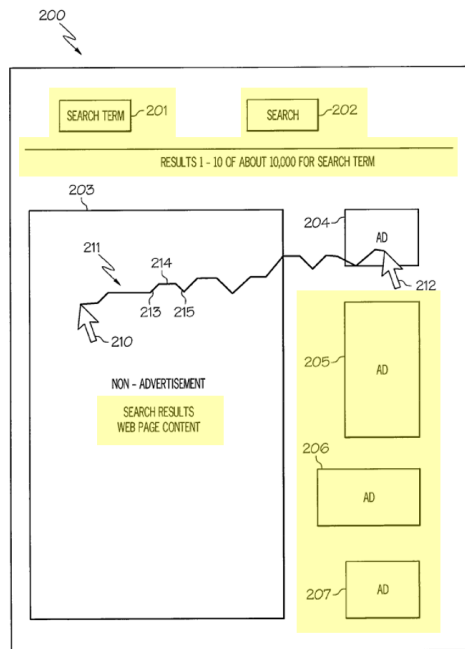


FIG. 2

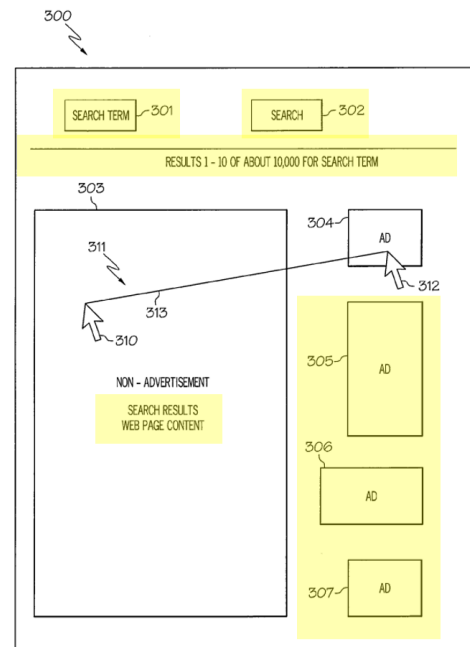


FIG. 3

Willner, FIGs. 2-3 (annotated)

A POSA would have also understood that Willner's webpages would typically include other functional data such as HTTP headers, header icons, other markup/script performing functions unrelated to the cursor monitoring, and other displayed content such as headers, logos, and/or non-interactive icons, any of which are data not specific to determination of the user status, rendering claim 13 anticipated or alternatively obvious. Lopresti-Declaration, [0102].

M. Claim 14: “The method of claim 1 wherein the issued data is in specific response to a request issued by the client computing device.”

Willner’s issued data (webpage with markup/code) is in specific response to the client device issuing a request for the webpage. Willner, [0041]-[0044]; *supra* §§ III.B.2-III.B.3 ([1A]-[1B]); Lopresti-Declaration, [0103].

N. Claim 15: “The method of claim 1 further comprising modifying data delivered to the client computing device subsequent to reaching a predetermined value for d) is reached.”

As discussed *supra* §§ III.B.5-III.B.6, Willner meets [1D]-[1E] by comparing monitored cursor movement data to model data, resulting in a confidence level value as to whether the client’s user is human or clickbot. “The confidence factor can be used to deny the action of click” when “a lower confidence factor [is] determined,” suggesting “algorithmically generated” click fraud. Willner, [0036], [0048]-[0049]. Conversely, “[t]he click on the advertisement may be processed, and an associated web page or information related to the advertisement displayed,” when “a high confidence level/factor [is] determined, suggesting no click fraud.” Willner, [0051].

These teachings disclose to a POSA that the advertiser’s webpage is only displayed if the confidence value from performing [1D]-[1E] exceeds a predetermined level (thus suggesting no fraud), and is not displayed if that value has reached a predetermined lower level that does indicate fraud. Lopresti-

Declaration, [0104]-[0105]. A POSA would have understood that denying the click is modifying data delivered to the client device, because the advertiser's webpage/information would have been delivered for a confidence value indicating no fraud, and instead is not delivered if the predetermined value indicating fraud is reached. Lopresti-Declaration, [0105].

Alternatively, it would have been obvious in view of the POSA's background knowledge to modify what data is delivered to the client device when Willner's confidence value indicates fraud. Lopresti-Declaration, [0106], citing corroborating Ex. 1008 ("Meek"), [0029], [0052]-[0053] (client device's request for web content "is honored" when analysis indicates user is human, and otherwise "is not honored" and a "denial message" delivered to the client device); O'Connell, [0032] ("appropriate course[s] of action" in response to "fraud detection results" include "allow action by the user, deny actions by the user,...request additional authentication information, etc.").

O. Claim 16: "The method of claim 1 further comprising repeating a)-d) for a single user instance."

The '008 patent's specification does not mention "a single user instance." A POSA would have understood the phrase to include at least a session in which the client navigates among a website's webpages. Lopresti-Declaration, [0108].

Willner performs [1A]-[1E] as discussed *supra* §§ III.B.2-III.B.6. A POSA would have understood Willner to disclose (or alternatively to render obvious)

repeating those steps for a single user instance, including performing them each time the same user clicks an advertisement while navigating webpages in a session with a web server, because Willner “perform[s]...pattern analyses for...*iterative clicks* thus allowing for precision in establishing that a human is involved” by testing whether “repeated cursor movements of the same user” are “different from each other.” Willner, [0037]-[0039]; Lopresti-Declaration, [0107]-[0109].

Alternatively, doing so would have been an obvious extension of Willner based on the POSA’s background knowledge. Lopresti-Declaration, [0110]. A POSA would have recognized the benefit of not only relying on analysis of the first click’s cursor movement in attempting to detect click fraud, especially in scenarios where the first click’s confidence level is relatively close to the threshold between human and clickbot. Instead, where subsequent clicks on advertisements are performed on subsequent webpages in a single user instance, a POSA would have been motivated to make use of that additional data by repeating the monitoring and analysis, to improve the likelihood of reaching an accurate confidence level to detect any fraud. Lopresti-Declaration, [0110]-[0111], citing Ex. 1012 (“Tanzer”), [0057]-[0058] (corroborating known benefits of having “individual’s behavior...continuously monitored whenever they are logged on to the system,” so that “even if that user fraudulently gained access to the system, the user will likely be flagged as an imposter shortly after”); Ex. 1011 (“Broder”),

[0059] (“to make a more accurate determination of...human or non human entity,...repeat the steps” of testing and analyzing user’s input), Ex. 1006 (“O’Sullivan”), [0049] (teaching to perform cursor movement monitoring “each time the advertisement on the web page is served”).

This extension would have been well within a POSA’s abilities, as it simply involves repeating the steps already performed. Lopresti-Declaration, [0112].

P. Claim 17: “The method of claim 1 further comprising repeating a)-d) for a single user instance until a predetermined value for d) is reached.”

For the reasons discussed *supra* § III.O (claim 16), Willner discloses or renders obvious repeating [1A]-[1E] for a single user instance until a predetermined confidence value (e.g., a low confidence indicating fraud) is reached, thus enabling detection of click fraud where iterative clicks demonstrate “duplication of vector patterns between...the same user” (Willner, [0037]-[0039]) and/or where a first click is too close to call but a subsequent click lowers the confidence to the predetermined value. Lopresti-Declaration, [0113]-[0114].

Q. Claim 18: “The method of claim 1 further comprising repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d).”

As discussed *supra* §§ III.O-III.P (claims 16-17), Willner discloses or renders obvious repeating [1A]-[1E]. In so doing, Willner compares hash values of first and second click movements, which are generated in the comparison of

[1D]. Willner, [0038]-[0039]; *supra* § III.B.5; Lopresti-Declaration, [0115]-[0116]. A POSA would further have been motivated to compare confidence values generated in [1D]-[1E] for first and second clicks to identify scenarios where a first click is too close to call but a subsequent click lowers the confidence such that click fraud is indicated. Lopresti-Declaration, [0115]-[0116].

IV. GROUND 2: CLAIMS 1-18, 20 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS

A. Kitts

Like Willner, Kitts relates to preventing “click fraud” “perpetrated by...various automated methods” in connection with PPC advertising. Kitts, [0001]-[0005], [0053]; Lopresti-Declaration, [0059]-[0060]. “[A]ttributes associated with the web-page request” are “fed into a statistical model” to “calculate a probability that the web-page request was fraudulently initiated”—e.g., “that the request is originating from an automated system e.g., a program that constantly clicks advertisements.” Kitts, Abstract, [0021]-[0022], [0009], [0031]; Lopresti-Declaration, [0060].

The “attributes” Kitts analyzes include “an internet protocol (IP) address of the client-computing device 202, date, time, geographic location, metadata, key words, HTML tags, or other characteristics associated with the page request,...the user’s gender, ethnicity, age, web history, residence, etc.” Kitts, [0046]-[0048], [0067]. The ’008 patent refers to such data as “passive model data.” ’008-patent,

3:9-17 (“Passive model data...includes, without limitation,...originating IP address,...originating IP address physical location,...etc.”); Lopresti-Declaration, [0061].

B. Willner-Kitts Combination

A POSA would have been motivated to add Kitts’s statistical model analysis and use of passive model data (Kitts’s “attributes”) to determining the confidence level in Willner’s method. Willner and Kitts address the same problem of preventing automated click fraud on webpage advertisements (*supra* §§ III.A, IV.A), and both analyze data regarding the client device’s interaction with the webpage to determine a value (Willner’s “confidence level” or Kitts’s “quality score”) indicating whether the user is likely a human or bot. *Supra* §§ III.B.1, III.B.6 (Willner); Kitts, [0031]-[0032], [0049], [0067]-[0068]; Lopresti-Declaration, [0118]. Kitts ([0068]) teaches that “[a]dditionally, other user or program parameters may also be used in conjunction with the attributes to determine the probability,” and a POSA would have been motivated to improve Willner’s performance in detecting automated click fraud by analyzing passive data as Kitts teaches, in addition to active data as Willner teaches. Lopresti-Declaration, [0118]. Kitts ([0047]) teaches that “[s]uch information can be an important tool in determining whether the user requesting the web page has a propensity for click fraud,” and it was well known to POSAs that analyzing

passive data could help differentiate humans from bots. Lopresti-Declaration, [0118], citing as corroboration Broder, [0009], [0042]-[0043], [0051]-[0054], [0068]-[0069]; Ex. 1014 (“Ge”), [0082]-[0083]; Ex. 1015 (“English”), 3:17-29.

C. Claims 1-3, 6-18

The Willner-Kitts combination meets claims 1-3, 6-18 for the same reasons as Willner alone discussed *supra* §§ III.B-III.Q, which are unchanged in the combination. Lopresti-Declaration, [0119].

Additionally, the “model data” of [1D] is met in the Willner-Kitts combination by Kitts’s teaching to “execute[] a statistical model” on “the attributes as well as other parameters associated with the user or program initiating the request” (which in the combination include Willner’s monitored cursor movement data) “to calculate the quality score.” Kitts, [0049], Abstract, [0009], [0022], [0068]; Lopresti-Declaration, [0120]. “Examples of statistical models may include, without limitation, a Bayesian model, regression model, neural network, decision tree, or other statistical model capable of determining the quality score for retrieved attributes.” Kitts, [0049].

[1E]’s “generating a value” is further met in the Willner-Kitts combination by Kitts’s ([0031]-[0032]) teaching that “any indicative *value* may be used to designate a quality score” representing “the probability that a selection of an

advertisement impression is initiated from a user or by software attempting to induce click fraud.” Lopresti-Declaration, [0121].

D. Claim 4: “The method of claim 1 wherein the model data comprises passive model data.”

The ’008 patent (3:9-17) says “[p]assive model data comprises data available from a computing device user’s interactions therewith and within the computing environment where such data is normally stored (logged) or transmitted to a remote location” and “includes, without limitation, browser cookies,...originating IP address,...originating IP address physical location,...etc.”

As discussed *supra* §§ IV.B-IV.C, the Willner-Kitts combination analyzes attributes including the client’s originating IP address and geographic location, as well as other data (e.g., date, time, metadata, key words, HTML tags) that a POSA would have understood are available from the user’s interactions with the client device and within the computing environment where such data is normally stored/logged and transmitted to the web server. Kitts, [0046], [0067]; Lopresti-Declaration, [0122]-[0123]. Attributes may also be retrieved via browser cookies. Kitts, [0047].

A POSA would have understood from Kitts’s description that the collected passive data are compared to passive model data relating to human interaction with the webpage to calculate the quality score. Lopresti-Declaration, [0124]. Kitts “executes a statistical *model*” on the passive data, such as “a Bayesian model,

regression model, neural network, decision tree, or other statistical model capable of determining the quality score *for retrieved attributes*.” Kitts, [0049], [0068], claim 11. A POSA would have understood that such statistical models involve considering the retrieved data in relation to prior data of the same type. Lopresti-Declaration, [0124] (citing Ex. 1016 (“Alspector”), 10:1-17, 11:62-67, 12:1-13, corroborating knowledge to train statistical classification models using previously collected data of known classification). The data relate to human interaction with the webpage because they are “characteristics associated with the web page request” or “the user submitting the page request,” and are useful to determine “the probability that a selection of an advertisement impression” or “a web page request or search-engine query is initiated from a [human] user or by software attempting to induce click fraud”—i.e., whether “there is a probability that the request is originating from an automated system” instead of a human. Kitts, [0046], [0031], [0021]; Lopresti-Declaration, [0124].

E. Claim 5: “The method of claim 4 wherein the passive model data comprises browser cookies; destination IP histories; originating IP address; originating IP address traffic data; originating IP address physical location; and/or third party data regarding abusers comprising originating IP addresses and physical locations.”

Claim 5, reciting “and/or,” can be met by any one or more of the listed options. As discussed *supra* § IV.D (claim 4), Kitts’s passive model data comprises browser cookies, the client device’s (originating) IP address and its

physical location, any one or more of which meet claim 5. Lopresti-Declaration, [0125].

F. Claim 20: “The method of claim 1 wherein the interest data consists of available data.”

While there is no antecedent basis for “interest data” in claim 1, the ’008 patent’s specification defines “interest data” as comprising “active or passive data, whether available or acquired, that correlates to any data within model data, whether obtained prior to or after the generation of issued data.” ’008-patent, 3:41-45. “[A]vailable data” is “a type of passive data” that is “associated with a computing device’s operation and its interaction with a computing environment, such as the Internet, that is generally recorded within the computing device and/or by other devices that have been affected by the computing device’s operation.” ’008-patent, 3:17-24.

As discussed *supra* §§ IV.B-IV.D, the Willner-Kitts combination analyzes “passive data” including Kitts’s “attributes,” by feeding them into a statistical model. The Willner-Kitts combination thus uses interest data (including passive data that correlates to any data within model data) that consists of available data. Lopresti-Declaration, [0126]-[0127]. A POSA would have understood Kitts’s attributes including client IP address, date, time, geographic location, metadata, key words, HTML tags, etc., are associated with the client’s operation and its interaction with the Internet (e.g., they are transmitted by the client device in a

webpage request via the Internet), and generally recorded within the client and/or by other devices affected by the client's operation (e.g., in the client in creating the webpage request including them, and in the server which is affected by the client's operation by receiving and processing the client's webpage request). Kitts, [0041]-[0048]; Lopresti-Declaration, [0127].

V. GROUND 3: O'CONNELL ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 1-18, 20

A. O'Connell

O'Connell describes analyzing user interaction data to detect fraudulent behavior by humans or automated programs during e-commerce sessions such as website purchases. O'Connell, Abstract, [0003], [0005]. Based on "keyboard interactions, movement device interactions, and navigation/selection tendencies," O'Connell determines a "fraud detection score" indicating "the likelihood that the...entity[] acting as the user of the current session is in fact the actual user or is actually a different user or automated program instead engaging in fraudulent behavior." O'Connell, [0027]-[0028], [0034]; Lopresti-Declaration, [0062]-[0063]. For example, "data that is entered too rapidly, a mouse pointer that never moves,...data transmitted in a form without keystrokes being recorded" "may represent potential fraudulent behavior by an automated program," whereas "if a key or keys are typed while the page has focus and then the form data appears,"

that is likely legitimate human use of a “hotkey.” O’Connell, [0048]-[0049]; Lopresti-Declaration, [0063].

B. Claim 1

[1PRE]: To the extent the preamble is limiting, O’Connell discloses it. O’Connell’s “*method*” (Abstract, claims 1-8) determines a “fraud detection score” that provides “an indication of the *likelihood* that the person (or entity) acting as the user of the current session is in fact the actual [human] user or is actually a[n]...*automated program*” ([0034], [0046]). Lopresti-Declaration, [0129]. The person/entity acting as the user operates a “*client computer* system 102 to *interact* with an e-commerce application 118 of an application *server* 106.” O’Connell, [0025]-[0026], [0008], [0024], [0033] (“*operation*...by the user”); Lopresti-Declaration, [0129]. A POSA would have understood that O’Connell’s determining a likelihood score assesses a “confidence level,” as the ’008 patent uses the terms “confidence level,” “confidence score,” and “likelihood” interchangeably. Lopresti-Declaration, [0129] (explaining ’008 patent uses “confidence level” only in claims, “confidence score” in figures, “likelihood” in Abstract, and “probability” in Summary). Alternatively, it would have been obvious to assess a confidence level as O’Connell’s score. Lopresti-Declaration, [0130] (citing Afergan, [0040], [0155], corroborating well-known use of a “score”

to “represent[] a confidence value...that the user agent is associated with a human user or an automated agent”).

[1A]: O’Connell’s method comprises a single user of client device 102 requesting data from application 118 on server 106. O’Connell, [0025] (“*a user* may interact with an e-commerce application 118 to perform tasks such as purchasing goods or services, requesting or viewing information”), [0024] (discussing “response to a *request* by *the user* for an action”), [0032] (“*user request*” for accessing information), [0050] (“*the user* accesses a webpage”), [0055] (authenticating “*a user*”/“*the user*”) [0056] (“*request* for information”); Lopresti-Declaration, [0131].

[1B]: O’Connell’s server 106 includes e-commerce application 118 that “provide[s] services, content, or information to...client computer system 102,” including webpages. O’Connell, [0032], [0050]; Lopresti-Declaration, [0132]. “[E]very page sent by...server 106” may include “JavaScript™ code [that] track[s] details of the user’s interaction with the browser 112 and transmit[s] an indication of such interaction...to a specified server.” O’Connell, [0026]. The services/content/information/webpages and JavaScript are each issued data generated by the server (or by another computing device from which the server obtains them) which is not the same as the client device to which the server

presents the data and whose user's status is being assessed as human vs. bot.

Lopresti-Declaration, [0132]; *see* '008-patent, 3:33-37 (describing "issued data").

[1C]: O'Connell monitors "user-browser interaction *data*" including "keyboard interactions, movement device interactions, and navigation/selection tendencies" generated by the user at the client device in response to the issued data. O'Connell, [0027]-[0028], [0026] (JavaScript tracks user-browser interaction at "client computer system" "on every page sent by the application server 106"), [0050] (same); Lopresti-Declaration, [0133].

[1D]: O'Connell detects fraud by "*comparing*" the monitored "user-browser interaction data to known fraudulent human or automated program behavior." O'Connell, Abstract, FIG. 6, [0006], [0019]-[0020], [0045], [0048], [0053].

A POSA would have understood that O'Connell's comparison to "known fraudulent automated program behavior" compares the user-browser interaction data with "model data relating to human interaction with or in response to the issued data" as claimed. Lopresti-Declaration, [0134]-[0135]. O'Connell says "behavior indicative of an automated program attempting to improperly enter data may include data entry that is too rapid, a mouse pointer that does not move, etc." O'Connell, [0020], [0048] ("Factors that may represent potential fraudulent behavior by an automated program and thus raise potential security issues may

include data that is entered too rapidly, a mouse pointer that never moves, a large form that is filled out without the browser window scrolling, data transmitted in a form without keystrokes being recorded, or other factors.”). Thus, O’Connell detects automated program behavior by contrasting the monitored behavior with what is expected from a human interaction. Lopresti-Declaration, [0135]. For example, O’Connell’s “automated fraud detector” 410 (FIG. 4) does not penalize human users who use form filling tools, by recognizing that “[i]f the pointer goes off the web page, the form data appears, and then the pointer comes back over the page, the user has likely just clicked a form filler tool,” and that “if a key or keys are typed while the page has the focus and then the form data appears, the user has just engaged the form filler tool with a hotkey”—both of which are legitimate human behavior. O’Connell, [0049]; Lopresti-Declaration, [0135]. O’Connell contrasts these known human behaviors with an automated program that “may typically have a mouse pointer that never moves.” O’Connell, [0049]; Lopresti-Declaration, [0135].

A POSA would have understood that O’Connell stores data to identify the above-discussed behavior expected from a human interaction, and that data is used for “comparing” with the current session interaction data (*see, e.g.*, FIG. 6, 612) such as by comparing the current “speed of selecting keys” with typical past human data entry times to determine whether the data entry is “too rapid” and thus

indicative of an automated program. O’Connell, [0020], [0048]; Lopresti-Declaration, [0136].

A POSA would have understood that this stored data of expected human interaction is model data indicative of human interaction with the computing environment that can be received by O’Connell’s fraud detection server 110 which is physically remote from a sample computing environment from which the data was collected. Lopresti-Declaration, [0137]; *see* ’008-patent, 2:54-58 (describing “model data”). To the extent O’Connell does not explicitly discuss a sample computing environment, that would have been an obvious way to collect data representative of human interaction. Lopresti-Declaration, [0137], citing Broder, [0073]-[0074] (corroborating POSA’s knowledge that “collect[ing] a large amount of data” from “web viewers” interacting with webpages allows “build[ing] a better system for determining whether a web viewer is a human or non human entity”).

[1E]: O’Connell’s system can “detect fraudulent behavior by both humans and automated programs” or choose to “detect one of the two.” O’Connell, [0046], [0053]-[0054]. When detecting automated-program fraudulent behavior, O’Connell’s generated “fraud detection score” ([0034]) is “a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data” as [1E] recites, for the reasons discussed in this section above in

connection with [1PRE] and [1D]. Lopresti-Declaration, [0138]. A POSA would have understood that O’Connell’s “score” is a “value” as claimed; or alternatively that a “value” would have been an obvious implementation. Lopresti-Declaration, [0138] (citing corroborating Afergan, [0040], [0155]).

C. Claim 2

As discussed *supra* § V.B, O’Connell “compare[s] the user-browser interaction data with known fraudulent behavior indicative of an automatic program interacting with a website” by using the same type of active model data the ’008 patent describes, including model data regarding “keyboard interactions, movement device interactions, and navigation/selection tendencies” indicating when, e.g., “data [] is entered too rapidly,” or when a typical human “user’s pointer...has likely just clicked a form filler tool...[or] the user has just engaged the form filler tool with a hotkey.” O’Connell, [0048]-[0049], [0027]; ’008-patent, 2:60-3:5 (“Active model data...includes, without limitation, pointing device vector movements and/or cadence, key stroke combinations and/or cadence, time differentials between stimulus...and user response (e.g.,...completion of form field...)”); Lopresti-Declaration, [0139]. A POSA would have understood that these data are acquired from the user’s interactions with the client device and not normally stored or remotely transmitted, because they are instead tracked and transmitted to a server by “JavaScript on every page sent [to the client] by the

application server.” O’Connell, [0026]; *see* ’008-patent, 2:60-64 (describing “active model data”); Lopresti-Declaration, [0139].

D. Claim 3

As discussed *supra* § V.C (claim 2), O’Connell’s active model data comprises pointing device vector movements and/or cadence (“a mouse pointer that never moves”; “tracking of the user’s pointer”), key stroke combinations and/or cadence (“data transmitted in a form without keystrokes being recorded”; “form filler tool [engaged] with a hotkey”), and time differentials between a display element and a response (“data [] is entered too rapidly”), any one or more of which meet claim 3 which recites “and/or.” O’Connell, [0048]-[0049]; Lopresti-Declaration, [0140].

E. Claim 4

In addition to the active data discussed *supra* §§ V.C-V.D (claims 2-3), O’Connell’s tracked user-browser interaction data includes “identification information” such as “browser code name, browser major version, browser minor version, country code of the browser installation, CPU class, platform, IP address, user agent, system language and cookies.” O’Connell, [0027], [0029]. O’Connell analyzes the total user-browser interaction data to determine a “likelihood” that the user is an “automated program...engaging in fraudulent behavior.” O’Connell, [0034]; Lopresti-Declaration, [0141]. O’Connell thus describes using the same

type of “passive model data” the ’008 patent describes, which a POSA would have understood are available from the user’s interactions with the client device and within the computing environment where such data is normally stored/logged and transmitted to the application server. ’008-patent, 3:9-17 (“[p]assive model data...includes, without limitation, browser cookies,...originating IP address,...originating IP address physical location”); Lopresti-Declaration, [0141].

O’Connell’s fraud analyzer 406 passes user-browser interaction data analysis to both human fraud detector module 408 and automated fraud detector module 410. O’Connell, FIG. 4, [0045]. O’Connell describes examples of data analyzed by these modules but says “other factors” may be used. O’Connell, [0045]-[0048]. O’Connell ([0047]) discusses the human fraud detector module analyzing “source IP address as indicator of ISP or country” but does not expressly describe which module analyzes the “cookies” or “country code of the browser installation” described in [0029]. Lopresti-Declaration, [0142]. A POSA would have understood O’Connell to expressly disclose that these factors can be used (e.g., by FIG. 4’s automated program fraud detector) to determine a “likelihood” that the user is an “automated program...engaging in fraudulent behavior” (O’Connell, [0034]), because O’Connell never states (and a POSA would not have understood) that these factors are relevant only to human fraud detection, and a POSA would have understood that these factors are useful for automated fraud

detection, such as by determining whether the client device's IP address or physical location is associated with known bot activity. Lopresti-Declaration, [0142], citing Broder, [0051]-[0052] (corroborating background knowledge to analyze whether "request [is] from an IP address that has previously been determined to be a non human entity," etc.).

F. Claim 5

As discussed *supra* § V.E (claim 4), O'Connell's passive model data comprises browser cookies, originating IP address and physical location, any one or more of which meet claim 5 reciting "and/or." Lopresti-Declaration, [0143].

G. Claim 6

O'Connell meets [1B] by sending JavaScript code to the client, and [1C] by the code tracking the user's interaction data. O'Connell, [0026]; *supra* § V.B. Both steps thus enable the client device to record the user's input and make it available to a server computing device for O'Connell's comparison analysis.

O'Connell, [0025] ("user may interact with the browser 112 via user *input* devices"), [0026] ("JavaScript™ code may track details of the user's interaction with the browser 112 and transmit an indication of such interaction...to a specified server"); Lopresti-Declaration, [0144]-[0145]. A POSA would have understood from the disclosure of tracking, sending, and analyzing the input that the input is recorded. Lopresti-Declaration, [0145]; *see supra* § III.E. O'Connell meets [1C]

by tracking the input data and [1D] by comparing the tracked data to model data (*supra* § V.B); thus the client records input and makes it available for comparison “according to” both steps, meeting claim 6. Lopresti-Declaration, [0144]-[0145].

H. Claim 7

O’Connell’s system 100 includes application server 106 that presents issued data to the client (*supra* § V.B) and fraud detection server 110 that “compare[s] the user-browser interaction data” to determine “a fraud detection score.” O’Connell, FIG. 1, [0024], [0034]. “[A]ny of the components of the e-commerce fraud detection system 100 may be...located as part of the same computer system in some network arrangements.” O’Connell, [0036]. Thus, O’Connell teaches that fraud detection server 110 (the “computing device” performing the comparison in claims 6-7) can be the same computer device as application server 106 (the claimed “server”), meeting claim 7. Lopresti-Declaration, [0146]. Indeed, in “[a]n example,” all three servers 106, 108, and 110 in O’Connell’s FIG. 1 “may be an International Business Machine (IBM) eServer® server.” O’Connell, [0036]; Lopresti-Declaration, [0146]. Alternatively, it would have been obvious to implement O’Connell’s servers as software components operating on the same physical device. Lopresti-Declaration, [0147] (citing Tanzer, FIG. 1, [0061], corroborating POSA’s knowledge that server serving webpages/code and server analyzing client attribute data can be “housed on one electronic device”).

I. Claim 8

O'Connell's client 102 is a component of O'Connell's e-commerce fraud detection system 100. O'Connell, FIG. 1. Thus, O'Connell's teaching that "any of the components of the e-commerce fraud detection system 100 may be...part of the same computer system" (O'Connell, [0036]) teaches that fraud detection server 110 and client 102 may be on the same computing device, meeting claim 8. Lopresti-Declaration, [0148]. Alternatively, it would have been obvious to implement O'Connell's system to run the fraud detection module on the client computing device. Lopresti-Declaration, [0149] (citing Meek, [0027], [0043], corroborating POSA's knowledge that determination of "human effort" can be performed by "attestation unit" on client device).

J. Claim 9

O'Connell teaches that, alternatively, fraud detection server 110 (the claimed "computing device" performing the comparison) and application server 106 (the claimed "server") may each be a distinct computer system. O'Connell, FIG. 1, [0024], [0036]; Lopresti-Declaration, [0150]. Thus, fraud detection server 110 can be on a computer that is neither application server 106 nor client device 102, meeting claim 9. Lopresti-Declaration, [0150].

K. Claim 10

As discussed *supra* § V.G (claim 6), O'Connell's recorded input comprises the user-browser interaction data which includes active model data as discussed

supra § V.C (claim 2). O’Connell teaches delivering this recorded input to a server computing device that is not the client, as discussed *supra* §§ V.H, V.J (claims 7, 9). Lopresti-Declaration, [0151].

L. Claim 11

O’Connell operatively installs at least one monitoring program—e.g., “JavaScript code [that] track[s] details of the user’s interaction”—on the client device’s browser, as part of issuing data to the client ([1B]) and monitoring user-generated data ([1C]), meeting claim 11. O’Connell, [0026], [0050]; *supra* § V.B; *compare* ’008-patent, 4:3-35; Lopresti-Declaration, [0152]-[0153].

M. Claim 12

As discussed *supra* §§ V.B, V.J, O’Connell teaches that the fraud detection server 110 that performs the analysis meeting [1D]-[1E] may be implemented on a computing device that is neither the application server 106 (the claimed “server”) nor the client device 102, meeting claim 12. O’Connell, FIG. 1, [0024], [0036]; Lopresti-Declaration, [0154]-[0155].

N. Claim 13

As discussed *supra* § V.B, O’Connell’s application server issues data including webpages to the client. O’Connell, [0026], [0032], [0050]. A POSA would have understood that such webpages would typically include at least some data that is not considered in, and therefore not specific to, determination of the user’s status as human or fraudulent automated program, such as HTTP headers,

header icons, other markup/script performing functions unrelated to tracking the user interaction data, as well as non-interactive displayed content such as headers, logos, and/or icons. Lopresti-Declaration, [0156].

O. Claim 14

As discussed *supra* § V.B, O’Connell’s issued data (services/content/information/webpages and JavaScript served to the client) is in specific response to the client device issuing a request for the data (e.g., a request to access the webpage or other information/content/service). O’Connell, [0024]-[0025], [0032], [0050], [0056]; Lopresti-Declaration, [0157].

P. Claim 15

As discussed *supra* § V.B, O’Connell meets [1D]-[1E] by generating a fraud detection score indicating the “degree of likelihood of fraudulent behavior evidenced by the user.” O’Connell, [0034]. Thereafter, the e-commerce application “analyze[s] the fraud detection results to determine an appropriate course of action with respect to the user.” O’Connell, [0057]. Different actions may result if fraud is “highly unlikely” vs. “a possibility” (*id.*), each of which determinations a POSA would have understood to involve comparing the fraud detection score to a predetermined value/threshold to determine whether the score value represents that fraud is “a possibility” rather than “highly unlikely.” Lopresti-Declaration, [0158]. Alternatively, this would have been the conventional

and obvious way to implement what O’Connell discloses. Lopresti-Declaration, [0158].

O’Connell teaches that when the fraud detection score reaches a value indicating possible fraud, the e-commerce application may “deny actions by the user,...flag any transactions as ones that cannot complete until further verification, request additional authentication information, etc.” O’Connell, [0032], [0057]; Lopresti-Declaration, [0159]. Any of the above result in modifying data delivered to the client device from the data that would have been delivered if the fraud detection score indicated fraud was unlikely. Lopresti-Declaration, [0159].

Q. Claim 16

As discussed *supra* § III.O, a POSA would have understood the claimed “single user instance” to include at least a session in which the client navigates among a website’s webpages. Lopresti-Declaration, [0161].

O’Connell performs [1A]-[1E] as discussed *supra* § V.B. A POSA would have understood O’Connell to disclose (or alternatively to render obvious) repeating those steps for a single user instance, including performing them each time the user navigates to and interacts with a subsequent webpage in a session with the e-commerce application by submitting a transaction or other request for which fraud detection may be desired, because O’Connell includes the monitoring

“JavaScript on *every page* sent by the application server.” O’Connell, [0026]; Lopresti-Declaration, [0160]-[0162].

Alternatively, doing so would have been an obvious extension of O’Connell based on the POSA’s background knowledge. Lopresti-Declaration, [0163]. A POSA would have recognized the benefit of not only relying on the analysis of the first user interaction (keyboard/mouse interaction, etc.) in attempting to detect fraud, especially in scenarios where the fraud detection score from the first interaction was relatively close to the threshold between human and automated program. Instead, where further interactions with further issued data (e.g., further webpage forms) are performed in a single user instance, a POSA would have been motivated to make use of that additional data by repeating the monitoring and analysis, to improve the likelihood of reaching an accurate fraud detection. Lopresti-Declaration, [0163], citing corroborating Tanzer, [0057]-[0058]; Broder, [0059]; O’Sullivan, [0049]; *see supra* § III.O.

This extension would have been well within a POSA’s abilities, as it simply involves repeating the steps already performed. Lopresti-Declaration, [0163].

R. Claim 17

For the reasons discussed *supra* § V.Q (claim 16), O’Connell discloses or renders obvious repeating [1A]-[1E] for a single user instance until a predetermined fraud detection score value (e.g., one indicating fraud is likely) is

reached, thus enabling detection of fraud where the user's first interaction is too close to call but a subsequent interaction brings the score to the predetermined value. Lopresti-Declaration, [0164]-[0165].

S. Claim 18

As discussed *supra* §§ V.Q-V.R (claims 16-17), O'Connell discloses or renders obvious repeating [1A]-[1E]. In so doing, a POSA would have been motivated to compare the score values generated in [1D]-[1E] for first and second interactions by the user to identify scenarios where a first interaction is too close to call but a second interaction adjusts the score to a value indicating fraud. Lopresti-Declaration, [0166]-[0167].

T. Claim 20

As discussed *supra* §§ V.E-V.F (claims 4-5), O'Connell discloses collecting identification information (e.g., IP address, country code, cookies, etc.) that correlates to passive model data. O'Connell, [0029]. O'Connell thus uses interest data (including passive data that correlates to any data within model data) that consists of available data, meeting claim 20. Lopresti-Declaration, [0168]; *see supra* § IV.F.

VI. GROUND 4: CLAIMS 1-18, 20 WOULD HAVE BEEN OBVIOUS OVER O'CONNELL IN VIEW OF KITTS

A. O'Connell-Kitts Combination

A POSA would have been motivated to add Kitts's statistical model analysis and use of passive model data (Kitts's "attributes") to determining the fraud score in O'Connell's method, for similar reasons as discussed *supra* § IV.B for the Willner-Kitts combination. Lopresti-Declaration, [0170]. O'Connell and Kitts address the same type of problem of preventing automated fraud on webpages, and both analyze data regarding the user's/client's interaction with the webpage to determine a score indicating whether the user is likely a human or bot. *Supra* §§ V.A-V.B (O'Connell); Kitts, [0031]-[0032], [0049], [0067]-[0068]; Lopresti-Declaration, [0170]. Kitts ([0068]) teaches that "[a]dditionally, other user or program parameters may also be used in conjunction with the attributes to determine the probability," and a POSA would have been motivated to improve O'Connell's performance in detecting automated fraud by analyzing passive data as Kitts teaches, in addition to active data as O'Connell teaches. Lopresti-Declaration, [0170]. Kitts ([0047]) teaches that "[s]uch information can be an important tool in determining whether the user requesting the web page has a propensity for click fraud," and it was well known to POSAs that analyzing passive data could help differentiate humans from bots. Lopresti-Declaration,

[0170], citing corroborating Broder, [0009], [0042]-[0043], [0051]-[0054], [0068]-0069]; Ge, [0082]-[0083]; English, 3:17-29.

B. Claims 1-3, 6-18

The O’Connell-Kitts combination meets claims 1-3, 6-18 for the same reasons as O’Connell alone discussed *supra* §§ V.B-V.D, V.G-V.S, which are unchanged in the combination. Lopresti-Declaration, [0171].

Additionally, [1D]’s “model data” is met by Kitts’s teaching to “execute[] a statistical model” on “the attributes as well as other parameters associated with the user or program initiating the request” (which in the O’Connell-Kitts combination include O’Connell’s user-browser interaction data) “to calculate the quality score.” Kitts, [0049], Abstract, [0009], [0022], [0068]; Lopresti-Declaration, [0172]; *see supra* § IV.C.

[1E]’s “generating a value” is further met by Kitts’s ([0031]-[0032]) teaching that “any indicative *value* may be used to designate a quality score.” Lopresti-Declaration, [0173]; *see supra* § IV.C.

C. Claim 4

The O’Connell-Kitts combination uses Kitts’s attributes which are passive data as discussed *supra* §§ IV.A, IV.D, and uses Kitts’s statistical modeling techniques which compare the collected passive data to passive model data as

discussed *supra* § IV.D. The O’Connell-Kitts combination’s model data thus comprises passive model data, meeting claim 4. Lopresti-Declaration, [0174].

D. Claim 5

As discussed *supra* §§ IV.D-IV.E, VI.C, Kitts’s passive model data in the O’Connell-Kitts combination comprise browser cookies, the client device’s (originating) IP address and its physical location, any one or more of which meet claim 5 reciting “and/or.” Lopresti-Declaration, [0175].

E. Claim 20

The O’Connell-Kitts combination (*supra* § VI.A) analyzes passive data including Kitts’s “attributes” by feeding them into a statistical model. The O’Connell-Kitts combination thus uses interest data (including passive data that correlates to any data within model data) that consists of available data, for the same reasons as the Willner-Kitts combination discussed *supra* § IV.F. Lopresti-Declaration, [0176].

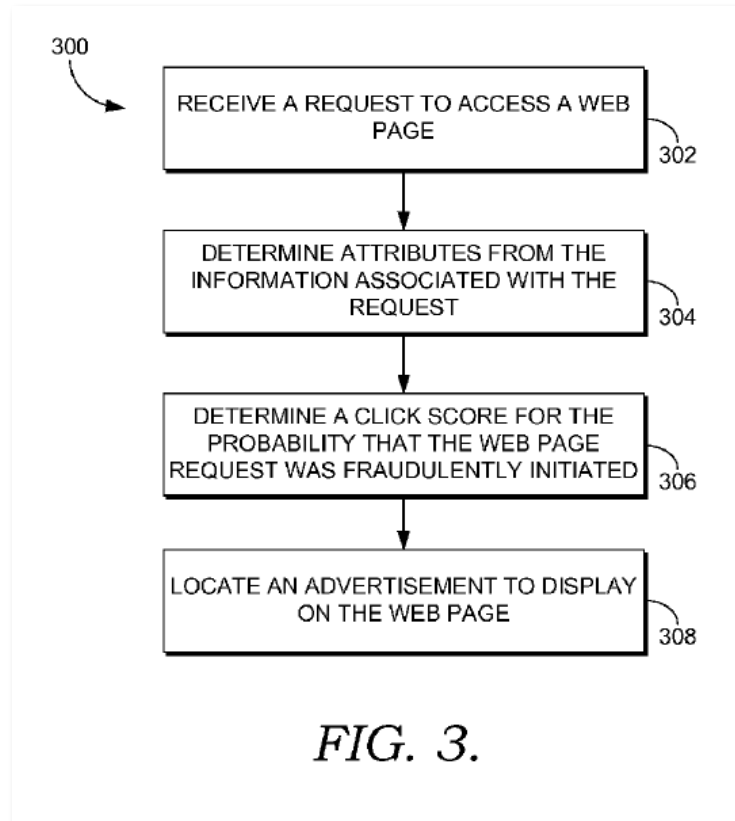
VII. GROUND 5: KITTS ANTICIPATES OR ALTERNATIVELY RENDERS OBVIOUS CLAIMS 19-20

A. Claim 19

1. **[19PRE]: “A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:”**

To the extent the preamble is limiting, Kitts discloses it. Kitts describes a method for preventing “click fraud” “perpetrated by...various *automated*

methods,” by determining “a *probability* that the request is originated from an *automated* system e.g., a program that constantly clicks advertisements.” Kitts, [0003], [0005], [0021], [0053], Abstract, FIG. 3; Lopresti-Declaration, [0178].



“*[C]lient-computing device 202*” interacts with “*server 204*” by “submit[ing] a request for a web page.” Kitts, [0041]. “Attributes relating to the user or program responsible for the request”—i.e., claimed “operator” of the client device—are determined from “information associated with the request [that] is sent to the server.” Kitts, [0067]; Lopresti-Declaration, [0179]. “The attributes are used to determine the *probability* (i.e., quality *score*) that the request was fraudulently initiated.” Kitts, [0068]. Computation component 208 can be

configured to calculate the quality score “to identify *robots*, or *automated* systems, used to conduct click or impression fraud,” in which embodiments the score indicates “a probability that the request is originating from an *automated* system e.g., a program that constantly clicks advertisements.” Kitts, [0049], [0053], [0021]; Lopresti-Declaration, [0179]. A POSA would thus have understood that Kitts’s quality score represents a probability regarding whether the operator of the client device is a human or instead an autonomic computer application. Lopresti-Declaration, [0179].

A POSA would have understood that Kitts’s determining a “quality score” for the “probability” that the user is a click-fraud bot (Kitts, [0031]) is assessing a “confidence level” as claimed, as the ’008 patent uses the terms “confidence level,” “confidence score,” and “probability” interchangeably. Lopresti-Declaration, [0180] (explaining ’008 patent uses “confidence level” only in claims, “confidence score” in figures, “likelihood” in Abstract, and “probability” in Summary). Alternatively, it would have been obvious to assess a confidence level as Kitts’s score. Kitts, [0032] (“While the discussion herein refers to a quality score as a probability, any indicative value may be used to designate a quality score.”); Lopresti-Declaration, [0181] (citing Afergan, [0040], [0155], corroborating well-known use of a “score” to “represent[] a confidence value...that the user agent is associated with a human user or an automated agent”).

2. [19A]: “a) acquiring interest data from the client computing device prior to delivery of issued data by the server to the client computing device;”

The '008 patent says that “interest data” comprises “active or passive data, whether available or acquired, that correlates to any data within model data, whether obtained prior to or after the generation of issued data. Thus, interest data includes time independent available data and acquired data, unless qualified differently.” '008-patent, 3:41-46. Further, “[p]assive model data comprises data available from a computing device user’s interactions therewith and within the computing environment where such data is normally stored (logged) or transmitted to a remote location,” and “includes, without limitation, browser cookies, destination IP histories, originating IP address,...[and] originating IP address physical location.” '008-patent, 3:9-17. A POSA would have understood from this description of “passive model data” that “passive data” also includes a client device’s originating IP address and originating IP address physical location, so that the same types of data can be compared with the model data. Lopresti-Declaration, [0182].

As discussed *supra* §§ IV.A, VII.A.1, Kitts’s server “retrieve[s] attributes from the page request” received from the client device, including “*an internet protocol (IP) address of the client-computing device 202*, date, time, *geographic location*, metadata, key words, HTML tags,” and possibly also “the user’s gender,

ethnicity, age, web history, residence, etc.” Kitts, [0046]-[0048], [0067], claims 2, 4. These attributes meet the ’008 patent’s description of passive data; they are available from the client device’s user’s interactions therewith and within the computing environment where such data is normally stored or transmitted to the remote server, in the same way the ’008 patent’s passive data are. Kitts, [0046]-[0048] (the attributes are retrieved “from the page request” using “cookies” and in “the page request itself”); Lopresti-Declaration, [0183]. Further, at least the cookies, web history, IP address and/or geographic location attributes are explicitly listed as passive data in the ’008 patent (3:12-17). Lopresti-Declaration, [0183].

Kitts’s passive data attributes are available data as discussed *infra* § VII.B (claim 20), and correlate to data within model data because they compare with statistical model data as discussed *infra* § VII.A.3 ([19B]). *See also supra* §§ IV.D-IV.E. Therefore Kitts’s attributes are “interest data” as claimed. Lopresti-Declaration, [0184].

Kitts describes the server acquiring the attributes prior to delivery of any issued data by the server to the client device. Lopresti-Declaration, [0185]. Initially, “the client-computing device 202 submits a request for a web page...by a user entering a...(URL)...into...a web browser.” Kitts, [0041], [0023], [0067]. The server “retrieve[s] attributes” from “***the page request itself*** [which] contain[s] the IP address of the client-computing device 202. From the IP address, the

geographic location of the client-computing device 202 can be determined. Also, a user's profile information may be sent *along with the request.*" Kitts, [0048].

Thus, the interest data (attributes including IP address, geographic location, user profile information) are acquired by the server in the first communication from the client device requesting the webpage, prior to the server delivering the requested webpage (issued data) to the client device. Lopresti-Declaration, [0185]. The webpage that is then "rendered by [the] web server" (Kitts, [0042]) is generated by that server which is not the same as the client device whose user's status is being assessed as human vs. bot; therefore the webpage is "issued data" as claimed.

'008-patent, 3:33-37; Lopresti-Declaration, [0185].

3. [19B]: "b) comparing the interest data to model data relating to human interaction with a computing device prior to the time in which the interest data is acquired; and"

Kitts's attributes (the claimed "interest data") are "fed into a statistical *model*" to calculate the "probability that the web-page request was fraudulently initiated"—i.e., the "probability that the request is originating from an automated system." Kitts, Abstract, [0021], [0009], [0022], [0049], [0068]; Lopresti-Declaration, [0186]. The statistical model may be "a Bayesian model, regression model, neural network, decision tree, or other statistical model capable of determining the quality score for retrieved attributes." Kitts, [0049], [0068], claims 5, 11. A POSA would have understood that such statistical models compare

the retrieved attributes to model data, including previously collected data of the same type. Lopresti-Declaration, [0186] (citing corroborating Alspector, 10:1-17, 11:62-67, 12:1-13). The data (attributes) can be received by the web server which is physically remote from the sample computing environment (i.e., client devices submitting webpage requests). Lopresti-Declaration, [0187]; *see* '008-patent, 2:54-58 (describing “model data”). The data relate to human interaction with a computing device because they are “characteristics associated with the page request” or “the user submitting the page request,” and are useful to determine “the probability that a selection of an advertisement impression” or “a web page request or search-engine query is initiated from a [human] user or by software attempting to induce click fraud”—i.e., whether “there is a probability that the request is originating from an automated system” instead of a human. Kitts, [0046], [0031], [0021]; Lopresti-Declaration, [0188]. Because the statistical model exists and can be “execute[d]” on the retrieved attributes (the acquired interest data), the model data are built based on and relate to human interaction prior to the time in which the interest data is acquired. Kitts, [0049]; Lopresti-Declaration, [0188].

Alternatively, these would have been obvious ways to implement what Kitts describes, meeting [19B]. Lopresti-Declaration, [0189] (citing Alspector, corroborating that “Bayesian classifier” (12:1-13) was “known” type of “classification model” (11:62-67) trained using a set of previously-collected data

of known classification (e.g., “known as spam or legitimate”) (10:1-17) to then determine the likely classification of future data of the same type (11:62-67)).

4. [19C]: “c) generating a value that represents a confidence level that a human user rather than an autonomic user operated the client computing device prior to the time in which the interest data is acquired.”

Kitts’s execution of the statistical model on the attributes retrieved from the client’s web page request generates a “quality score” indicating “the probability...that the request was fraudulently initiated,” which can be the “probability that the request is originating from an automated system.” Kitts, [0067]-[0068], [0021], [0031]. That quality score can differentiate genuine human users from “various automated methods” of click fraud. Kitts, [0005], [0021], [0053]; Lopresti-Declaration, [0190]. As discussed *supra* § VII.A.1 ([19PRE]), Kitts’s quality score represents a confidence level that a human user rather than an autonomic user operated the client computing device in submitting the webpage request. The webpage request contains the attributes that the server analyzes to generate the score; therefore the score assesses the user who operated the client device (by initiating the webpage request) prior to the time in which the interest data (attributes) are acquired by the server (in the webpage request after it is transmitted from client to server). *See supra* § VII.A.2 ([19A]); Lopresti-Declaration, [0190]. The quality score can be generated as “any indicative *value*.” Kitts, [0032].

Kitts thus meets [19C]. Lopresti-Declaration, [0190].

B. Claim 20

Although claim 20 recites dependency from claim 1, there is no antecedent basis in claim 1 for “the interest data” in claim 20. Claim 20 numerically follows claim 19, which does recite “interest data.” If claim 20 is interpreted to depend from claim 1, it is unpatentable per Grounds 1-4 above. If claim 20 is instead interpreted to depend from claim 19, it is unpatentable over Kitts.

The '008 patent says that “available data” is a “type of passive data” that “comprises data associated with a computing device’s operation and its interaction with a computing environment, such as the Internet, that is generally recorded within the computing device and/or by other devices that have been affected by the computing device’s operation.” '008-patent, 3:17-24.

As discussed *supra* §§ IV.A, IV.D-IV.F, VII.A.2, Kitts’s “attributes” meet the claimed “interest data” and are “passive data.” A POSA would have understood that Kitts’s attributes including client IP address, date, time, geographic location, metadata, key words, HTML tags, etc., are associated with the client’s operation and its interaction with the Internet (e.g., they are transmitted by the client device in a webpage request via the Internet), and are generally recorded within the client and/or by other devices affected by the client’s operation (e.g., in the client in creating the webpage request including them, and in the server which

is affected by the client's operation by receiving and processing the client's webpage request). Kitts, [0041]-[0048]; Lopresti-Declaration, [0191]-[0193]. Therefore Kitts's attributes consist of "available data," meeting claim 20. Lopresti-Declaration, [0193].

VIII. NO BASIS EXISTS FOR DISCRETIONARY DENIAL

A. Section 314(a)

The '008 patent has not previously been challenged before the Board, and the *Fintiv* factors (below) weigh against discretionary denial. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential) ("*Fintiv*").

Factor 1: "[N]o stay has been requested or ordered in the related district court litigation;" therefore Factor 1 is neutral. *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative) ("*Sand*").

Factor 2: The Board's Final Written Decision should be due by November 2023. In the district court litigation, Petitioner's motion to transfer venue has not yet been decided. Ex. 1024. The preliminary, tentative trial date is August 17, 2023 (Ex. 1025 at 4), but the Western District of Texas "has not historically resolved cases so quickly." *In re Apple Inc.*, 979 F.3d 1332, 1344 (Fed. Cir. 2020) (explaining that "a court's general ability to set a fast-paced schedule is not particularly relevant" to address "court congestion"); Exs. 1026-1027. The court's

docket remains congested with 806 patent-related cases, 520 of which were filed before Nobots’s suit and thus should be tried first. Exs. 1022-1023, 1028-1029. *See Bose Corp. v. Koss Corp.*, IPR2021-00297, Paper 16 at 12 (June 3, 2021) (noting the court’s docket numbers at the time—548 patent cases with 309 filed before the patent owner’s—“on their face are high” and implicate “concern about the viability of the...trial date”).

Given the congested docket, COVID-19 (Exs. 1030-1035), and the pending transfer motion, it would be unreasonably speculative to assume the district court trial will occur in August 2023. *See* Ex. 1026 (study showing the Board was “***almost always wrong***...(94% of the time)” in “evaluating future trial dates”); *Dish Network, L.L.C. v. Broadband iTV, Inc.*, IPR2020-01280, Paper 17 at 16-18, 26 (Feb. 4, 2021) (“*Dish*”) (granting institution: “We cannot ignore the fact that the currently scheduled trial date is more than nine months away and much can change during this time;” thus with “trial scheduled for less than three months before the due date for the final written decision and a motion to transfer pending,...the efficiency and system integrity concerns that animate the *Fintiv* analysis are not particularly strong,” as “whether the Texas court actually will hold a trial before, contemporaneously with, or after our final written decision statutory deadline is still uncertain.”); *KioSoft Techs. LLC v. TechTrex, Inc.*, PGR2021-00093, Paper 12 at 10-11 (Dec. 17, 2021) (“*KioSoft*”) (current trial date three months before FWD

is “around the same time,” so “the efficiency and fairness concerns that underlie the *Fintiv* analysis are not as strong, and the decision whether to institute will instead implicate other factors”).

Furthermore, Factor 2 is assessed on a “sliding scale,” with trial proximity balanced against petitioner’s diligence. *Apple Inc. v. Seven Networks, LLC*, IPR2020-00235, Paper 10 at 9-10 n.6 (July 28, 2020). This Petition has been filed less than five months after Nobots’s infringement complaint, and *seven months* before Petitioner’s statutory bar. Exs. 1022-1023.

Factor 3: Minimal investment has been made in the district court toward assessing the ’008 patent. By the time of institution, expected in November 2022, litigation pleadings may yet be amended, there will be months left in fact discovery, no expert discovery will have occurred, nor any summary judgment motions filed. Ex. 1025 at 3. *Dish* at 19-20 (Board was “not persuaded that [this] level of investment...supports exercising our discretion to deny institution,” where preliminary and final infringement and invalidity contentions had been exchanged, *Markman* hearing and order had occurred, but fact discovery was ongoing and expert discovery had not begun) (citing *Sand* at 10-11); *Hyundai Motor Am. v. Stratosaudio, Inc.*, IPR2021-01267, Paper 9 at 13-15 (Jan. 25, 2022) (“*Hyundai*”) (same).

“Petitioner’s diligence in filing its Petition also weighs against exercising...discretion to deny institution.” *Dish* at 20. Petitioner filed this Petition before resolution of its transfer motion; less than two months after receiving Nobots’s preliminary infringement contentions; **before** serving preliminary invalidity contentions or exchanging claim terms or proposed constructions; and **seven months** before the statutory bar. Exs. 1022-1024, 1025 at 1-2. *Dish* at 21 (Factor 3 “weighs **strongly** against” discretionary denial where petitioner filed “less than three months after” infringement contentions and before exchanging and briefing claim constructions); *Hyundai* at 16-17 (Factor 3 “weighs against...discretionary denial where “Petitioner was reasonably diligent in filing...approximately two months after receiving...preliminary infringement contentions”); *Hulu, LLC v. SITO Mobile R&D IP, LLC*, IPR2021-00298, Paper 11 at 10-11 (May 19, 2021) (“*Hulu*”) (similar); *IBM Corp. v. Trusted Knight Corp.*, IPR2020-00323, Paper 15 at 12 (July 10, 2020) (instituting trial where “Petitioner filed its Petition expeditiously,” “soon **after** it served its invalidity contentions”); *Apple Inc. v. Parus Holdings, Inc.*, IPR2020-00687, Paper 9 at 16 (Sep. 23, 2020) (same); *Microchip Tech. Inc. v. HD Silicon Sol’ns LLC*, IPR2021-00752, Paper 9 at 11 (Nov. 9, 2021) (granting institution: “Petitioner acted without delay in filing...five months after being served with a complaint” and “seven months before statutory bar”); *HP Inc. v. Neodron Ltd.*, IPR2020-00459, Paper 17 at 40-41 (Sept.

14, 2020) (“*HP*”) (granting institution: “Petitioner acted diligently in filing...more than five months in advance of the statutory bar date..., approximately two months after...preliminary infringement contentions..., and...prior to...preliminary invalidity contentions”).

Factor 4: Petitioner stipulates that, if this IPR is instituted, Petitioner will not pursue in the district court litigation any invalidity ground that is instituted in this IPR. Ex. 1036. The Board has routinely found similar stipulations sufficient to cause Factor 4 to weigh against denial. *See Sand* at 11-12 (informative); *Micron Tech., Inc. v. Vervain, LLC*, IPR2021-01550, Paper 11 at 11-12 (April 11, 2022) (“*Micron*”); *Samsung Elecs. Am., Inc. v. Proxense, LLC*, IPR2021-01438, Paper 12 at 12-13 (Feb. 28, 2022).

That this petition challenges claim 8, which is unasserted in the litigation, also weighs against denial. *Micron* at 11-12.

Factor 5: While Petitioner is a party to the district court litigation, this factor is outweighed by the other factors which favor institution. *See KioSoft* at 14 (granting institution: where “the currently scheduled trial date and the final written decision statutory deadline are close in time, about three months apart,...factor 5 weighs, at most, slightly in favor” of denial).

Factor 6: The Petition’s merits weigh against denial. *Fintiv* at 14-16.

B. Section 325(d)

In applying § 325(d), the Board uses the two-part framework of *Advanced Bionics, LLC v. MED-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8-9 (Feb. 13, 2020) (precedential).

This Petition’s grounds rely on references neither considered during prosecution nor duplicative of art previously considered. *See supra* § II.D.

The first *Advanced Bionics* prong is unmet where “neither [the references] nor similar prior art was before the examiner...[and] the prosecution history does not include any overlapping arguments directed to this prior art,” such that the Board “need not address part two of the analysis.” *Godbersen-Smith Constr. Co. v. Guntert & Zimmerman Const. Div., Inc.*, IPR2021-00050, Paper 24 at 19-21 (May 7, 2021). None of this Petition’s references were before the Examiner, nor were any similar disclosures discussed. Lopresti-Declaration, [0046]. Where “[t]he Petition does not rely on any prior art that was cited during examination” nor any that is “substantially the same,” Section 325(d) denial is inappropriate, and the Board “need not consider” *Advanced Bionics* prong two. *Samsung Elecs. Co., Ltd. v. Collect, LLC*, IPR2020-00477, Paper 14 at 9-10 (Aug. 5, 2020) (“*Samsung*”); *see Align Tech., Inc. v. 3Shape A/S*, IPR2021-01309, Paper 11 at 15 (Feb. 9, 2022) (where several grounds “challenge[] the patent with a combination of

references...not previously presented to the Office,...part one of the *Advanced Bionics* framework” is unmet, and Section 325(d) denial is inappropriate).

Patent Owner distinguished the only art applied in prosecution as allegedly being “silent as to *any* distinction between human and autonomic users.” Ex. 1002 at 84-86. Willner, O’Connell, and Kitts—uncited during prosecution—disclose such distinction, which “strongly favors institution.” *Samsung* at 13-14.

Hence *Advanced Bionics* part one is unmet, and the Board need not reach part two. No basis exists to discretionarily deny institution.

IX. CONCLUSION

The Board should institute review and cancel claims 1-20.

Date: April 29, 2022

Respectfully submitted,
Google LLC
/Elisabeth Hunt/
Elisabeth H. Hunt, Reg. No. 67,336
WOLF, GREENFIELD & SACKS, P.C.

APPENDIX: CLAIM LISTING

[1PRE] A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:

[1A] a) a single user of a client computing device requesting data from a server;

[1B] b) the server presenting data issued by the server to the client computing device;

[1C] c) monitoring at least some data generated by the user at the client computing device in response to the issued data;

[1D] d) comparing the monitored data to model data relating to human interaction with or in response to the issued data; and

[1E] e) generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.

[2] The method of claim 1 wherein the model data comprises active model data.

[3] The method of claim 2 wherein the active model data comprises pointing device vector movements and/or cadence; key stroke combinations and/or cadence; and/or time differentials between a display element and a response.

[4] The method of claim 1 wherein the model data comprises passive model data.

[5] The method of claim 4 wherein the passive model data comprises browser cookies; destination IP histories; originating IP address; originating IP address traffic data; originating IP address physical location; and/or third party data regarding abusers comprising originating IP addresses and physical locations.

[6] The method of claim 1 wherein b) comprises enabling the client computing device to record input and making such recorded input available to a computing device for comparison according to c).

[7] The method of claim 6 wherein the computing device is the server.

[8] The method of claim 6 wherein the computing device is the client computing device.

[9] The method of claim 6 wherein the computing device is neither the server or the client computing device.

[10] The method of claim 6 wherein the recorded input comprises active model data and the recorded input is delivered to a computing device that is not the client computing device.

[11] The method of claim 1 wherein at least one monitoring program is operatively installed on the client computing device to perform b).

[12] The method of claim 1 wherein d) is performed by neither the server nor the client computing device.

[13] The method of claim 1 wherein at least some issued data is not data specific to determination of the user status.

[14] The method of claim 1 wherein the issued data is in specific response to a request issued by the client computing device.

[15] The method of claim 1 further comprising modifying data delivered to the client computing device subsequent to reaching a predetermined value for d) is reached.

[16] The method of claim 1 further comprising repeating a)-d) for a single user instance.

[17] The method of claim 1 further comprising repeating a)-d) for a single user instance until a predetermined value for d) is reached.

[18] The method of claim 1 further comprising repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d).

[19PRE] A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:

[19A] a) acquiring interest data from the client computing device prior to delivery of issued data by the server to the client computing device;

[19B] b) comparing the interest data to model data relating to human interaction with a computing device prior to the time in which the interest data is acquired; and

[19C] c) generating a value that represents a confidence level that a human user rather than an autonomic user operated the client computing device prior to the time in which the interest data is acquired.

[20] The method of claim 1 wherein the interest data consists of available data.

CERTIFICATE OF SERVICE UNDER 37 C.F.R. § 42.6 (E)(4)

I certify that on April 29, 2022, I will cause a copy of the foregoing document, including any exhibits or appendices filed therewith, to be served via Priority Mail Express at the following correspondence address of record for the patent:

LEE & HAYES, P.C.
601 W. RIVERSIDE AVENUE
SUITE 1400
SPOKANE WA 99201

Date: April 29, 2022

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24, the undersigned certifies that the foregoing Petition for *Inter Partes* Review contains 13,220 words excluding a table of contents, a table of authorities, Mandatory Notices under § 42.8, a certificate of service or word count, or appendix of exhibits or claim listing. Petitioner has relied on the word count feature of the word processing system used to create this paper in making this certification.

Date: April 29, 2022

/MacAulay Rush/
MacAulay Rush
Paralegal
WOLF, GREENFIELD & SACKS, P.C.