

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

NOBOTS LLC,
Patent Owner.

Case No. IPR2026-00429
Patent No. 11,810,014

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

TABLE OF CONTENTS

MANDATORY NOTICES.....	x
A. Real Party-In-Interest	x
B. Related Matters.....	x
1. United States Patent & Trademark Office	x
2. USPTO Patent Trial and Appeal Board	x
3. U.S. District Court for the Western District of Texas.....	xi
C. Counsel and Service Information - § 42.8(b)(3) and (4).....	xi
I. INTRODUCTION	1
II. STANDING	3
III. GROUNDS LISTING	3
IV. THE '014 PATENT	4
A. Specification Embodiments.....	4
B. Person of Ordinary Skill in the Art (“POSA”).....	6
C. Prosecution History	6
V. CLAIM INTERPRETATION	9
VI. GROUND 1: CLAIMS 1-8, 10-12, 14, AND 16-29 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS AND BRODER	9
A. Willner (EX1005).....	11
B. Kitts (EX1009)	14
C. Broder (EX1011).....	15
D. Willner-Kitts-Broder Combination	16
1. Passive Data	16
2. Further Testing, Including CAPTCHA	19
E. Mapping to Challenged Claims	23
1. Claim 16: [16Pre] A non-transitory machine readable medium having stored thereon instructions for performing a method for providing a value indicating a judgment of whether a human or an autonomic computer application operating a client computer	

is interacting with a server, which when executed by at least one machine, causes the at least one machine to perform operations comprising:	24
a. [16A] provide data collection data requesting active and passive data of the client computer;.....	26
b. [16B] receive active and passive data responsive to the data collection data, the received active data relating to interactions of the client computer with a website of the server;.....	30
c. [16C] analyze the received active...and...passive data for indication of a human or an autonomic computer application operating the client computer, ...in conjunction with model data based on human interactions from a prior session with the same website and developing a first analysis value;.....	31
d. [16D] determine that the first analysis value fails to meet a first analysis predetermined criteria; and.....	35
e. [16E] provide a request for further data from the client computer based on the determination....	36
2. Claim 17: ...failing to meet the first analysis predetermined criteria indicates that the client computer should not be allowed access to a protected page of the website.....	37
3. Claim 18: ...analyzing the at least one browser cookie, the at least one IP address, and the manual input device activity in conjunction with model data based on human interactions from a prior session with the same website.	39
4. Claim 19: ...decrypt the received active...and...passive data.	40
5. Claim 20:	41
a. [20A] receive further data from the client computer in response to the request for further data;.....	41
b. [20B] perform a second level of analyzing on the received further data; and	41
c. [20C] provide a second analysis value based on the second level of analyzing.	41

6. Claim 21: ...the received further data includes the response of the client computer to a CAPTCHA test provided to the client computer.....	42
7. Claim 1: [1Pre] ...generating a value indicative of a likelihood that a human or autonomic computer application is operating a client computer attempting access to a protected page of a website.....	42
a. [1A] provide data collection data that causes the client computer to collect active data relating to interactions of the client computer with a given page of the website;.....	43
b. [1B] receive at least some of the collected active data...and at least some passive data from the client computer;.....	44
c. [1C] perform a first analysis comprising analyzing at least some of the received active...and...passive data in conjunction with model data based on human interactions from a prior session with the same website;	44
d. [1D] generate a first analysis value based on the first analysis, wherein the client computer is allowed to access the protected page without requiring an operator of the client computer to decipher a CAPTCHA test if the first analysis value meets a first analysis predetermined criteria;.....	45
e. [1E] determine that the first analysis value fails to meet the first analysis predetermined criteria;.....	46
f. [1F] provide a CAPTCHA test to the client computer based on the determination...;	46
g. [1G] receive a response of the client computer to the CAPTCHA test;	46
h. [1H] perform a second analysis comprising assessing accuracy of the response...; and	46
i. [1I] generate a second analysis value based on the second analysis, wherein the client computer is granted access to the protected page based on the second analysis value meeting a second analysis predetermined criteria.	47
8. Claim 2:	49

a. [2A] provide an additional CAPTCHA test to the client computer based on the determination that the second analysis value fails to meet the second analysis predetermined criteria;	49
b. [2B] receive a response of the client computer to the additional CAPTCHA test;	52
c. [2C] perform a third analysis comprising assessing the accuracy of the client computer's response to the additional CAPTCHA test; and	52
d. [2D] generate a third analysis value based on the third analysis, wherein the client computer is granted access to the protected page based on the third analysis value meeting a third analysis predetermined criteria.....	53
9. Claim 3: ...when the first analysis value meets a first analysis predetermined criteria, the client computer is not presented with a CAPTCHA test prior to the client computer being granted access to the protected page.	53
10. Claim 4: ...decrypt the received active data and the received passive data.....	53
11. Claim 5: ...the model data is based on human interaction from a prior session with the same given page.....	53
12. Claim 6: ...the ability of the client computer to collect active data is only active while the client computer is visiting a web page enabled with data collection data.....	54
13. Claim 7: ...receive the first or second analysis predetermined criteria from an operator or administrator of the website.	54
14. Claim 8: ...receive from an operator or administrator of the website a number of CAPTCHA tests that will be provided to a client computer after the second analysis value fails to meet the second analysis predetermined criteria.	55
15. Claim 10: ...the data collection data comprises JavaScript code that causes a browser of the client computer to collect the active data.	58
16. Claim 11: ...analyzing the at least one browser cookie and the at least one IP address in conjunction with the model data.	59

17. Claim 12: ...analyzing manual device input activity of the client computer in conjunction with the model data based on human interaction with the same given page.	59
18. Claim 14: ...the human interaction...includes human interaction of another client computer from the prior session with the same given page.	59
19. Claim 22:	59
a. [22A] provide instructions that allow client computer interactions with a website of the server to be remotely monitored;	60
b. [22B] receive monitored data originating with the client computer, ...comprising active data relating to interactions of the client computer with the website and passive data of the client computer;.....	60
c. [22C] analyze the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including:.....	61
d. [22D] perform a first level of analyzing on the received monitored data for any indication that a human may be operating the client computer to obtain a first-level analysis;.....	61
e. [22E] perform a second level of analyzing to obtain a second-level analysis, when the first-level analysis does not meet a first-level analysis predetermined criteria, the second level of analyzing comprising analyzing the received monitored data in conjunction with previously recorded data relating to human interactions from a prior session with the same website; and.....	62
f. [22F] provide a second-level analysis value when the second-level analysis meets a second-level analysis predetermined criteria.	63
20. Claim 23: ...decrypt the received monitored data.	63
21. Claim 24: ...the monitored data comprises active data relating to interactions of the client computer with a given page of the website and passive data of the client computer, and the	

recorded data relates to human interaction from a prior session with the same given page.	63
22. Claim 25: ...provide a request for further data from the client computer based on the determination that the second-level analysis does not meet the second level analysis predetermined criteria.....	64
23. Claim 26:	64
a. [26A] receive further data from the client computer in response to the request for further data;.....	64
b. [26B] perform a third-level of analyzing on the received further data; and	64
c. [26C] provide a third-level analysis value after completion of the third-level of analyzing.....	64
24. Claim 27: ...the request for further data includes a CAPTCHA test.....	64
25. Claim 28: ...the received monitored data includes at least one browser cookie and at least one IP address.....	64
26. Claim 29: ...the received monitored data includes manual device input activity.	65
VII. GROUND 2: CLAIMS 4, 19, and 23 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND TANZER.....	65
VIII. GROUND 3: CLAIMS 9, 15, AND 30 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND MEEK	67
A. Willner-Kitts-Broder-Meek Combination.....	67
B. Mapping to Challenged Claims	68
1. Claim 9: ...analyzing mouse and keyboard activity of the client computer in conjunction with mouse and keyboard activity from human interactions from a prior session with the same website.....	68
2. Claim 15: ...the received active data comprises keyboard activity of the client computer on the given page and...the step of analyzing...further includes analyzing the keyboard activity in conjunction with the model data.	71

3. Claim 30: ...the manual device input activity comprises mouse movement and key strokes.	73
IX. GROUND 4: CLAIM 13 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND FARAHAT	73
X. CONCLUSION.....	74
XI. CLAIM LISTING APPENDIX	76

TABLE OF AUTHORITIES

CASES

<i>U.S. v. Munsingwear, Inc.</i> , 340 U.S. 36 (1950)	10
--	----

STATUTES

35 U.S.C. §102(b)	4
35 U.S.C. §102(e)	4
35 U.S.C. §103	3
35 U.S.C. §282(b)	9

REGULATIONS

37 C.F.R. §42.100(b)	9
37 C.F.R. §42.104(a)	3

APPENDIX LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 11,810,014 (“the ’014 patent”)
1002	Prosecution History of U.S. Patent No. 11,810,014
1003	Declaration of Daniel P. Lopresti, Ph.D. (“Lopresti-Decl.”)
1004	Curriculum Vitae of Daniel P. Lopresti, Ph.D.
1005	U.S. Patent Application Publication No. 2009/0024971 (“Willner”)
1006	RESERVED
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	U.S. Patent No. 6,405,922 (“Kroll”)
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. 8,112,483 (“Emigh”)
1017	U.S. Patent Application Publication No. 2007/0271466 (“Mak”)
1018	U.S. Patent Application Publication No. 2007/0124288 (“Swanson”)
1019	U.S. Patent No. 8,078,497 (“Ling”)
1020	U.S. Patent No. 6,195,698 (“Lillibridge”)
1021	U.S. Patent Application Publication No. 2002/0147735 (“Nir”)
1022	U.S. Patent Application Publication No. 2005/0144067 (“Farahat”)
1023	Joint Claim Construction Statement (Dkt. #107) filed July 27, 2026, in <i>Nobots LLC v. Google LLC</i> , Case No. 1:22-cv-00585 (W.D. Tex.)
1024	Petitioner Google LLC’s <i>Sotera</i> Stipulation dated July 29, 2026

MANDATORY NOTICES

A. Real Party-In-Interest

Petitioner Google LLC (“Google”) is the real party-in-interest.¹

B. Related Matters

1. United States Patent & Trademark Office

The application from which U.S. Patent No. 11,810,014 (“the ’014 patent”) issued (U.S. Patent Application No. 17/882,082) is a Continuation of U.S. Patent Application No. 16/578,823 (U.S. Patent No. 11,775,853), which is a Division of U.S. Patent Application No. 15/457,099 (U.S. Patent No. 10,423,885), which is a Continuation of U.S. Patent Application No. 12/313,502 (U.S. Patent No. 9,595,008), which claims priority from U.S. Provisional Application No. 61/003,743.

2. USPTO Patent Trial and Appeal Board

Petitioner Google was the petitioner in IPR2022-00940 concerning related patent 9,595,008 (“the ’008 patent”), and in IPR2022-00941 concerning related patent 10,423,885 (“the ’885 patent”). IPR2022-00940 resulted in a Final Written Decision finding claims 1-17 and 20 of the ’008 patent unpatentable and, following

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.

an appeal to the Federal Circuit, a judgment and mandate that claim 19 of the '008 patent is unpatentable. The certificate canceling all claims except dependent claim 18 of the '008 patent issued on May 18, 2026. IPR2022-00941 resulted in a Final Written Decision finding all non-disclaimed claims of the '885 patent unpatentable, which was not appealed. The certificate cancelling all non-disclaimed claims of the '885 patent issued on February 23, 2024.

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

The '014 patent is currently asserted in *Nobots LLC v. Google LLC*, Case No. 1:22-cv-00585. Petitioner has made a *Sotera* stipulation in that proceeding; a copy is being filed herewith as EX1024.

C. Counsel and Service Information - §42.8(b)(3) and (4)

Lead Counsel	Elisabeth H. Hunt, Reg. No. 67,336
Backup Counsel	George T. Scott, Reg. No. 62,859
Service Information	<p><u>E-mail</u>: EHunt-PTAB@wolfgreenfield.com GScott-PTAB@wolfgreenfield.com</p> <p><u>Post and hand delivery</u>: Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210-2206</p> <p><u>Telephone</u>: 617-646-8000 <u>Facsimile</u>: 617-646-8646</p>

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

Petitioner requests *inter partes* review and cancellation of all claims 1-30 of the '014 patent (EX1001).

I. INTRODUCTION

Patent Owner (“Nobots”) sued Petitioner (“Google”) in December 2021 in the Western District of Texas, asserting patents 9,595,008 (“the '008 patent”) and 10,423,885 (“the '885 patent”), which share a specification. In April 2022, Petitioner filed IPR2022-00940 challenging the '008 patent and IPR2022-00941 challenging the '885 patent. In November 2023, as a result of IPR2022-00941, all claims of the '885 patent were disclaimed or found unpatentable at FWD, which Nobots did not appeal. In IPR2022-00940, all but two claims of the '008 patent were found unpatentable at FWD. Google appealed as to one of those two claims, which was found unpatentable by the Federal Circuit. Only a single dependent claim of the '008 patent now remains, which Nobots’ expert admitted lacks any description in the specification of which he was aware. *See* IPR2022-00940, EX1040 at 99-100.

Nobots filed the '014 patent’s application as a continuation of the same specification in August 2022, during pendency of the IPRs. Unsurprisingly given the specification’s meager disclosure (spanning barely more than two pages of text), the '014 patent’s claims are nothing more than a rearranging of the same elements and concepts that were held unpatentable in the parent patents’ claims, or

minor variations thereon. Most elements of the '014 patent's independent claims are disclosed by Willner (EX1005) in the same way Willner undisputedly anticipated most claims of the '008 patent. *See* IPR2022-00940, Paper 38 (FWD) at 19. The only features in the '014 patent's independent claims that are not anticipated by Willner are met by secondary references Kitts (EX1009) and Broder (EX1011), just as the same or highly similar features in dependent claims of the '008 and '885 patents were met by the same references.

For example, the '014 patent's broadest claim (claim 16) recites receiving and analyzing "*active and passive data.*"² The Willner-Kitts combination satisfies this feature the same way the Board held that it rendered '008 patent claim 4 unpatentable. *See* IPR2022-00940, Paper 38 (FWD) at 30-39. '014 patent claim 16 also recites requesting "*further data from the client computer*" based on a determination from the active/passive data analysis. Incorporating Broder's teachings satisfies this feature the same way the Board held that it satisfied '885 claims 4, 7, 11, and 17, which recited a specific version where the further data requested is a CAPTCHA response. *See* IPR2022-00941, Paper 34 (FWD) at 44-47.

² This Petition uses italics to designate claim language. All bold emphases are added unless otherwise specified.

Yet, though the Petitions of both IPRs were cited in an information disclosure statement with the '014 patent's application, the Examiner failed to apply Willner, Kitts, or Broder in any rejections. Nor did he explain why he did not do so. And Nobots never bothered to inform the Examiner that the Board had instituted the IPRs on the parent patents, finding a reasonable likelihood that nearly all claims were unpatentable, including over grounds involving Willner, Kitts, and Broder. *See* IPR2022-00940, Paper 13 (granting institution); IPR2022-00941, Paper 11 (granting institution).

The '014 patent is just as unpatentable as the patents that spawned it. *Inter partes* review is needed to correct the Office's error in allowing the '014 patent to issue without meaningful consideration and application of the prior art over which Petitioner had established—and the Board ultimately confirmed—that the parent patents' claims reciting similar features were unpatentable.

II. STANDING

Petitioner certifies that the '014 patent is available for IPR and Petitioner is not barred or estopped from requesting IPR as to the challenged claims. 37 C.F.R. §42.104(a).

III. GROUNDS LISTING

The challenged claims are unpatentable under 35 U.S.C. §103 over the following grounds:

Ground Number and Reference(s)		Claims
1	Willner (EX1005), Kitts (EX1009), Broder (EX1011)	1-8, 10-12, 14, 16-29
2	Willner, Kitts, Broder, Tanzer (EX1012)	4, 19, 23
3	Willner, Kitts, Broder, Meek (EX1008)	9, 15, 30
4	Willner, Kitts, Broder, Farahat (EX1022)	13

Each reference above is prior art under pre-AIA 35 U.S.C. §102(e) even to the '014 patent's earliest claimed priority date. Meek and Farahat are prior art under §102(b). With the exception of Farahat (which is applied herein only to dependent claim 13), all the above references were named in grounds over which the Board found claims of the '008 and '885 patents unpatentable in IPR2022-00940 and -00941. For ease of reference, this Petition uses the same exhibit numbers for references that were cited in those IPRs.

IV. THE '014 PATENT

A. Specification Embodiments

The '014 patent discusses 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”). EX1001, 1:18-27, 2:23-29. 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. EX1001, 1:18-27. 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.” EX1001, 1:65-2:4.

The '014 patent attempts to reduce the need to routinely use CAPTCHAs by instead assessing two types of “data relating to the operation of the computing device.” EX1001, 2:9-44. One type is “active data,” such as “mouse movements and/or key strokes inputted by the user...attempting to access [the] server.” EX1001, 3:34-42, 4:64-67, 3:1-19. If the data collected 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.” EX1001, 5:33-42. Or, “if the input data exactly (or statistically sufficiently) matches previously recorded data,” that would also indicate “the input data was derived from a machine,” because “it is impossible to have duplicative input data” if all biometric inputs are from humans. EX1001, 5:9-16. As a second type of data, the patent uses “passive data” such as the device’s “browser cookies, destination IP histories, originating IP address, [etc.],” which may be compared with “model data” relating to human interaction. EX1001, 2:64-4:2.

Such techniques were not new in the '014 patent. For example, Willner (EX1005) had already disclosed an alternative to CAPTCHA for 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,” including detecting input patterns that are too “analogous” to “previously stored” patterns to have been newly produced by a human. Willner, [0004]-[0006], [0047], [0056], [0037]-[0038]. Kitts (EX1009) 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], [0046], [0049], [0021]. Indeed, the prior art discussed herein provided far greater detail than the ’014 patent does regarding *how* to use biometrics and other collected data to distinguish human users from bots. EX1003 (“Lopresti-Decl.”), [0042]-[0044].

B. Person of Ordinary Skill in the Art (“POSA”)

A 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-Decl., [0038]-[0040].

C. Prosecution History

The ’014 patent’s application was filed during pendency of the IPR petitions on the parent ’008 and ’885 patents. Nobots cited the IPR petitions and their prior

art, along with other references, in an information disclosure statement. EX1002 at 17-25. In October 2022, the Examiner issued an Office Action rejecting the claims over a combination of Afergan, McNair, and Farahat—none of which were references named in the combinations proposed in the IPR petitions. EX1002 at 117. Nobots traversed this rejection by arguing, in January 2023, that Afergan and McNair did not teach various claim limitations. EX1002 at 309-323. By that time, the Board had instituted the IPRs in December 2022; but Nobots failed to even inform the Examiner of those institutions, let alone file any copy of the institution decisions into the prosecution record.

Following an interview about a terminal disclaimer (EX1002 at 334), the Examiner allowed the '014 patent's claims without any amendment, and never explained why the prior art highlighted in the IPRs was not applied to these claims. EX1002 at 412-413. The Examiner's "reasons for allowance" stated that "the cited prior art would not make it obvious...to 'perform a first analysis comprising analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data based on human interactions from a prior session with the same website', and then afterwards challenge the user with a CAPTCHA," and that a reference called Gusler "does not disclose using collected passive data to make the determination." EX1002 at 412.

These reasons for allowance are directly at odds with the Board’s findings in the IPRs. Had the Examiner reviewed the Board’s institution decision in IPR2022-00940, for example, he should have applied the Board’s reasoning that, “from Kitts’s teachings,” POSAs “would have appreciated that passive data would have had recognized benefits in detecting click fraud in the type of system conveyed in Willner,” and that, “even assuming that Patent Owner’s arguments surrounding a ‘same webpage’ requirement are correct,...Willner ‘teach[es] that the publisher’s server stores vector data collected from user interactions with the webpages of the website that the server hosts, for subsequent comparison by that server in assessing interactions with any one of those monitored webpages of that same hosted website.” IPR2022-00940, Paper 13 at 25-26, 17-18. And had the Examiner reviewed the Board’s institution decision in IPR2022-00941, he should have applied the Board’s reasoning that, “from Broder’s teachings,” POSAs “would have appreciated the recognized benefits in using an intermediate CAPTCHA” as “an additional or secondary fraud detection technique.” IPR2022-00941, Paper 11 at 19-21.

The fact that these Board findings were not even mentioned, and that the Examiner highlighted “passive data” and “CAPTCHA” as reasons for allowance without ever applying or discussing Willner, Kitts, and Broder, constitutes material error that must be rectified.

V. CLAIM INTERPRETATION

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” and “monitored data” discussed in the '014 patent at 2:64-3:56. (The further defined terms “available data,” “acquired data,” “issued data,” and “interest data” do not appear in the '014 patent's claims.)

In district court, Petitioner proposes that the preambles are limiting and proposes constructions of “active data” and “passive data.” EX1023. This Petition applies these constructions as demonstrated in the Grounds below.

VI. **GROUND 1: CLAIMS 1-8, 10-12, 14, AND 16-29 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS AND BRODER**

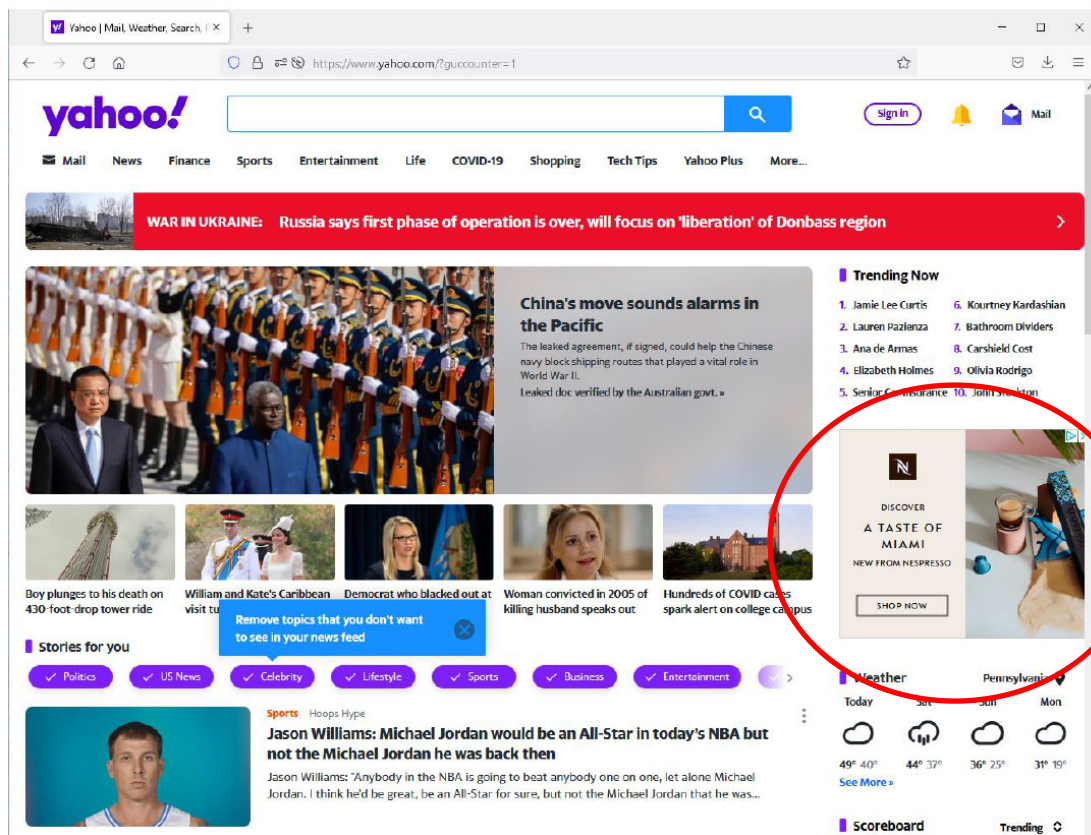
Willner (EX1005) was found in IPR2022-00940 to anticipate or render obvious most claims of the '008 patent, which Nobots did not even dispute. Willner combined with Kitts (EX1009) was found in the Board's FWD in IPR2022-00940 to render obvious '008 patent claims 4-5, because the combination receives and analyzes both Willner's active data and Kitts's passive data. IPR2022-00940, Paper 38 at 30-39. Nobots did not appeal the Board's findings

regarding the Willner-Kitts combination and is now bound by them. *See U.S. v. Munsingwear, Inc.*, 340 U.S. 36, 39 (1950) (issue preclusion becomes “binding...if an appeal, though available, had not been taken”). Broder (EX1011) was used in IPR2022-00941, in combination with Willner and another reference, to address ’885 patent claims 4, 7, 11, and 17 directed to providing a CAPTCHA when initial analysis indicates the client may be a bot. The Board’s FWD found these claims obvious as well. IPR2022-00941, Paper 34 at 44-47. Likewise, Nobots did not appeal the Board’s findings regarding Broder and is now bound by them.

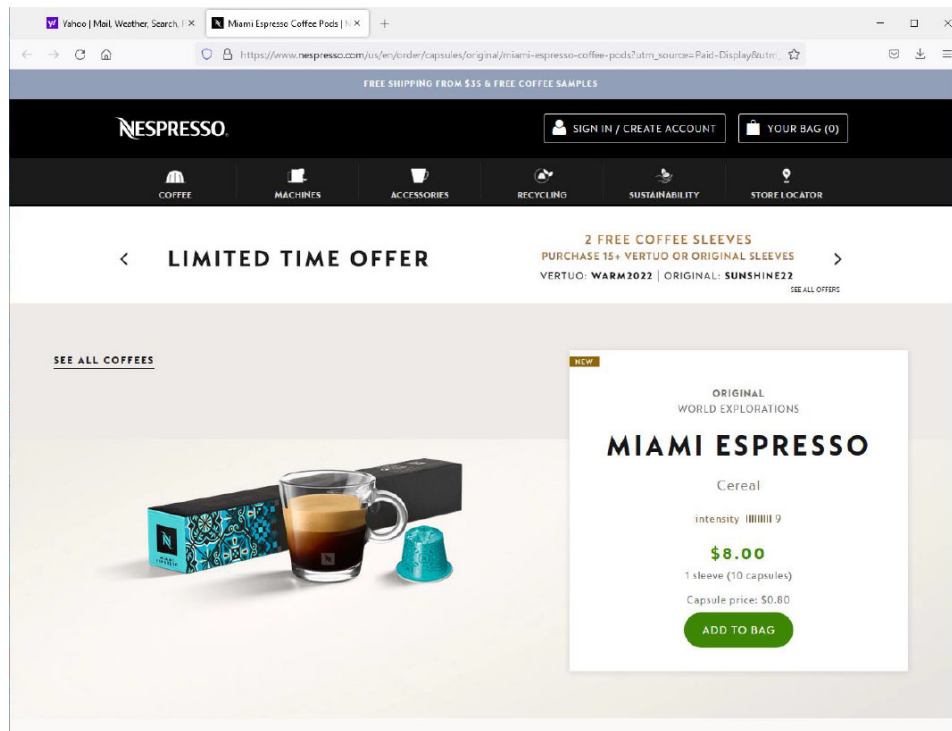
The ’014 patent has three independent claims (claims 1, 16, and 22), with claim 16 being the broadest. Claim 16 recites requesting, receiving, and analyzing active and passive data of a client computer for indication of a human or an autonomic computer application operating the client computer; developing an analysis value; and determining whether the analysis value meets predetermined criteria. These aspects are met by the same combination of Willner and Kitts that the Board found rendered claims 1-17 and 20 of the ’008 patent obvious. The remaining feature in ’014 patent claim 16 is providing a request for further data from the client computer based on determining that the analysis value fails to meet the criteria. This feature is met by Broder, just as the Board found that Broder met the similar (narrower) feature in dependent claims of the ’885 patent.

A. Willner (EX1005)

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-Decl., [0072]-[0073] (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].

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].

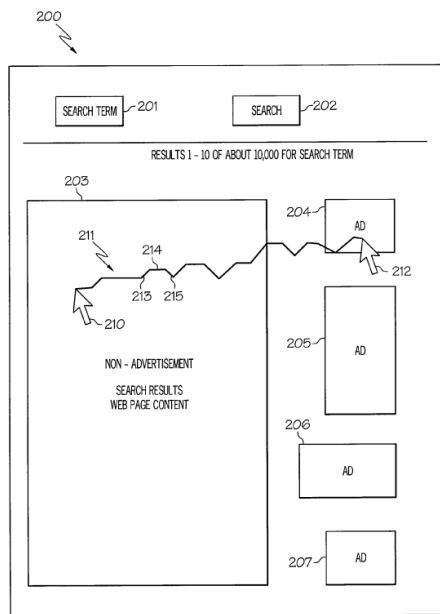


FIG. 2

(human movement)

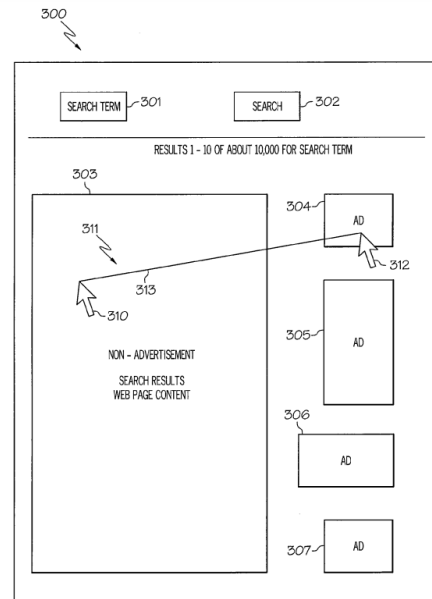


FIG. 3

(clickbot movement)

Additionally, Willner recognizes that “some automation tools may use a very intelligent automation script that may force the cursor to traverse a set of vectors” copying a human-made movement. Willner, [0037]. But Willner also recognizes that “duplication of vector patterns between different users (or the same user) has a zero probability of occurrence” for humans, because human movements always have some randomness and differences between them. Willner, [0037].

Therefore, Willner also stores vector patterns from previous “click action[s]” for later comparison so that “[s]ubsequent clicks that implement analogous hash sequence patterns can then be dismissed as an automation tool attempting to simulate the actions of a user.” Willner, [0038]. In other words, if a cursor movement is too similar to one that occurred previously, it may be a replica being replayed by a bot. Lopresti-Decl., [0076].

Willner’s techniques thus “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-Decl., [0074]-[0077].

B. Kitts (EX1009)

Like Willner, Kitts relates to preventing “click fraud” “perpetrated by...various automated methods” in connection with PPC advertising. Kitts, [0001]-[0005], [0053]. “[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, [0009], [0021]-[0022], [0031].

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,...etc.” Kitts, [0046]-[0048], [0067]. The ’014 patent calls such data “passive model data.” EX1001, 3:19-27 (“Passive model data...includes, without limitation,...originating IP address,...originating IP address physical location,...etc.”). Lopresti-Decl., [0078]-[0079].

C. Broder (EX1011)

Like Willner and Kitts, Broder relates to detecting and avoiding fraudulent internet-based advertisement viewings by “[n]on human entities such as...malicious click-fraud programs.” Broder, Title, Abstract. Broder teaches to “consider a large number of different factors” in “determin[ing] whether the web viewer is a human or not and how the system should proceed.” Broder, [0042]-[0043], [0063]. Broder lists some exemplary factors that are “not exhaustive” and “may be combined in their consideration,” including active-data factors like Willner’s cursor monitoring and passive-data factors like Kitts’s attributes. Broder, [0043]-[0053] (e.g., [0045] (“How fast was the response input?”), [0046] (“mouse-click in an inappropriate region”), [0051] (“Is this request from an IP address that has previously been determined to be a non human entity?”)), [0063]-[0070].

Broder teaches to interject an intermediate webpage after the advertisement click, requiring the user to, e.g., complete a CAPTCHA before receiving the advertiser's webpage. Broder, [0029], [0039]-[0040], Fig. 5. Broder teaches the benefits of not "interject[ing] an intermediate web page every time that a web viewer selects an advertising link," but instead only once a prior stage determines there is reason for suspicion. Broder, [0060]-[0072], Fig. 6. This allows "only few of the web viewers that access the web site [to] be subjected to the intermediate web page that may annoy the web viewer." Broder, [0062]. Lopresti-Deci., [0080]-[0081].

D. Willner-Kitts-Broder Combination

1. Passive Data

POSAs 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* §§VI.A—VI.B), 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. Willner, [0036], [0049]-[0055]; Kitts, [0031]-[0032], [0049], [0067]-[0068]. 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 POSAs 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. 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 that analyzing passive data could help differentiate humans from bots. Lopresti-Decl., [0083], citing corroborating EX1014 (“Ge”), [0082]-[0083]; EX1015 (“English”), 3:17-29.

POSAs would have reasonably expected success based on (1) the level of ordinary skill in the art, (2) the knowledge of a skilled artisan, including the above-discussed teachings of Willner and Kitts, and (3) the nature of the problem addressed in both references, i.e., click fraud detection. *See* IPR2022-00940, Paper 38 (FWD) at 36. Lopresti-Decl., [0084].

The Board already decided that Kitts’s teachings, in combination with Willner, render obvious incorporating passive data collection and analysis into Willner’s system and method. In IPR2022-00940 concerning the ’008 patent, the Board held that Kitts’s teachings “amply convey[] that ‘passive’ data has a recognized role in connection with bot detection systems” such that POSAs “would have recognized the benefit of employing additional data, e.g., Kitts’s passive data,” within Willner’s system and method, and that POSAs “would have had a

reasonable expectation of success in combining the teachings of Willner and Kitts.” IPR2022-00940, Paper 38 (FWD) at 34-36 (citing, e.g., Kitts, [0046]-[0047]). Nobots did not appeal these findings.

In the Willner-Kitts-Broder combination, the obviousness of collecting and analyzing both active and passive data is alternatively and additionally further supported by Broder’s teachings. As discussed *supra* §VI.C, Broder teaches to “consider a large number of different factors” in the bot-detection analysis, lists examples of both active and passive data that “may be combined in their consideration,” and explains that “this list is not exhaustive as other additional factors may be considered.” Broder, [0043]-[0053], [0063]-[0070].

POSAs would have been motivated by the above-discussed teachings to collect and analyze both active data (as Willner and Broder both disclose) and passive data (as Kitts and Broder both disclose) in assessing whether the client computer is being operated by a human or a bot. Lopresti-Decl., [0085]-[0086]. POSAs would have reasonably expected success based on Willner’s, Kitts’s, and Broder’s teachings that these types of data can successfully be collected and analyzed to detect bots for the same purpose of addressing click fraud, as well as because it would have required only ordinary programming skill to implement such data collection and analysis. Lopresti-Decl., [0086]. As the ’014 patent admits, passive data is already “normally stored (logged) or transmitted to a remote

location” and “readily harvestable by query.” EX1001, 3:19-27, 4:9-11. And both Kitts and Broder teach that such data can be analyzed using old and well-known modeling techniques such as, e.g., “Bayesian” classifiers. Kitts, [0049], [0068]; Broder, [0074].

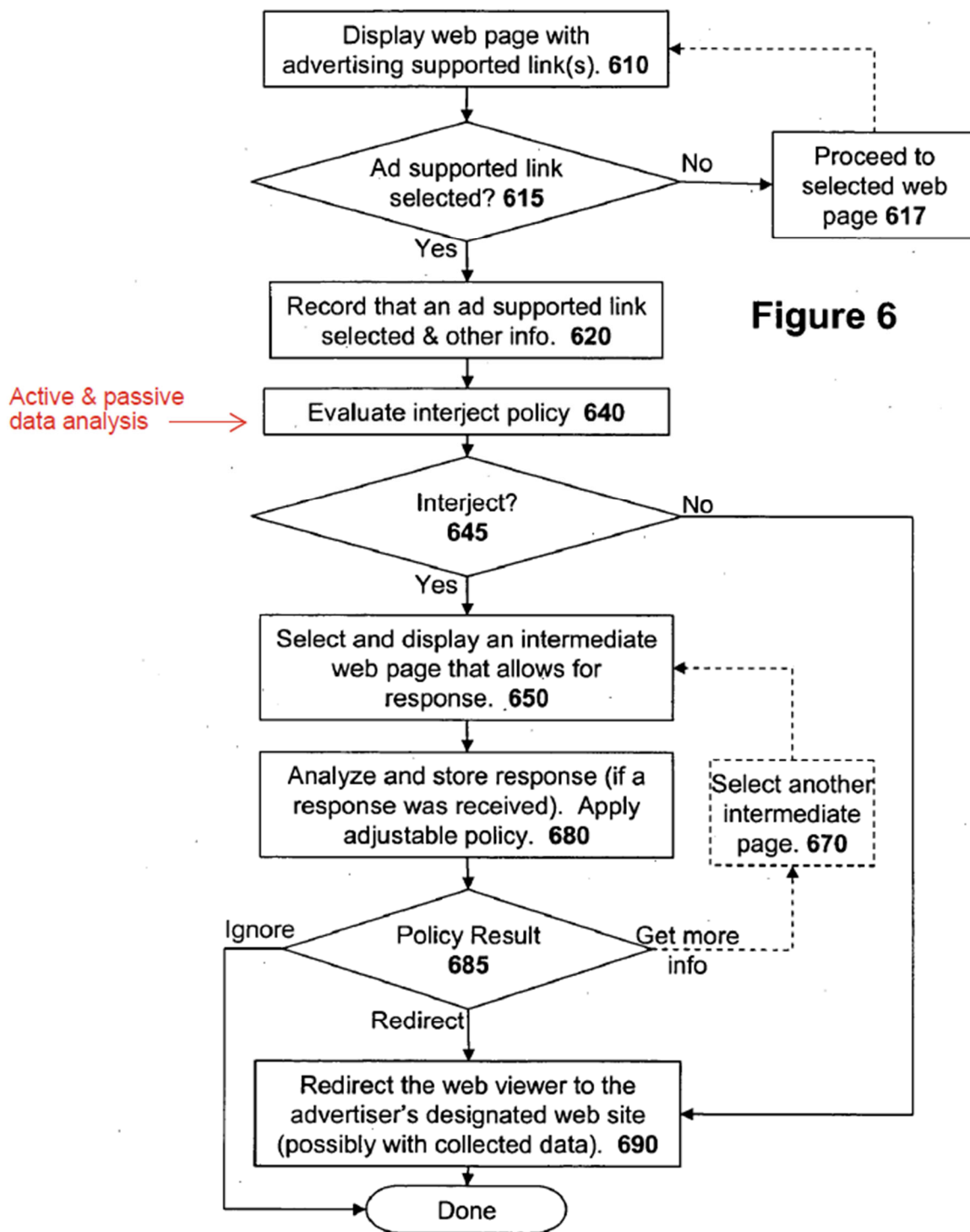
2. Further Testing, Including CAPTCHA

As discussed *supra* §VI.C, Broder teaches benefits of “interjecting an intermediate web page” after a click on an advertisement, to “test for and reduce non human web site traffic.” Broder, [0029]. “The intermediate page may take many different forms...to help determine” whether the clicking user “was a human or non human entity.” Broder, [0029]. One type of intermediate page is “a CAPTCHA page” that presents “a challenge-response test.” Broder, [0039]. Broder teaches that “[w]ith a CAPTCHA intermediate page, the ability to determine whether a particular web viewer is a human or a non human entity is greatly simplified.” Broder, [0039].

Broder recognizes that although CAPTCHA “presents the best system” for differentiating humans from bots, “the annoyance of having to complete a CAPTCHA task will tend to drive many web viewers away.” Broder, [0041]. “Consumers that browse the web can be notoriously impatient and easily alienated,” so “one may not wish to interject an intermediate web page every time.” Broder, [0060]. Therefore, Broder teaches to “evaluate[] an adjustable

interject policy” to “determine[] whether or not an intermediate web page should be displayed.” Broder, [0061]-[0062]. “The adjustable interject policy may consider a large number of different factors depending on what information is collected from the web viewer and the desires of the advertiser.” Broder, [0063]. Broder provides “a list of factors” which is “not exhaustive as other additional factors may be considered,” and includes, e.g., the client’s “IP address” and any “other click fraud indicators” that “raise the level of suspicion regarding this web viewer.” Broder, [0062]-[0070]. “After evaluating the adjustable interject policy..., the system either interjects with an intermediate web page or not.” Broder, [0071]. For example, if the analysis determines that the client is “very likely” a bot, “the interject policy may specify that a CAPTCHA intermediate page be selected” for further “testing of the web viewer’s response.” Broder, [0072].

POSAs would have understood that the analysis of active and passive data performed by the Willner-Kitts-Broder combination discussed *supra* §VI.D.1 is a suitable type of policy for determining whether “the level of suspicion” is high, by “consider[ing] a large number of different factors” based on “information...collected from” the client including, e.g., “IP address” (like Kitts’s passive data) and “other click fraud indicators” (like Willner’s active data) as Broder discusses. Broder, [0063]-[0070]; Lopresti-Decl., [0087]-[0090].



Broder, Figure 6 (annotated)

In situations where the analysis of active and passive data produces a confidence level indicating that the client is likely a bot, POSAs would thus have been motivated to incorporate Broder's technique to interject an intermediate page, such as a CAPTCHA, to achieve the benefits Broder describes of "help[ing] determine if the entity that selected the advertisement link was a human or a non human entity" by "analyz[ing] the web viewer's response to the intermediate [CAPTCHA] web page...along with other information" (e.g., the active and passive data analyzed by Willner-Kitts-Broder). Broder, [0029], [0010]. POSAs knew that it was not always necessary or desirable to simply deny access outright to an entity that is initially analyzed as likely to be a bot, as the initial analysis may not always be correct, and "request[ing] additional authentication information" is also an "appropriate course of action" based on "fraud detection results." Lopresti-Decl., [0091] (quoting corroborating EX1007 ("O'Connell"), [0032]; EX1016 ("Emigh"), 9:64-66, 10:21-42, 11:7-9, 14:47-62). POSAs would further have understood interjecting the CAPTCHA page to be desirable even if the initial analysis is correct that the client is a bot, to slow down the attempted automated click fraud. Lopresti-Decl., [0092] (citing EX1007 (O'Connell), [0049], corroborating POSAs' knowledge that "slow[ing] down the automated program" helps to "make it less efficient (and thus useful)").

POSAs would have reasonably expected success based on Broder's teachings of successfully interjecting intermediate webpages in the same context of detecting click fraud that concerns Willner and Kitts, and because it would have required only POSAs' ordinary programming skill to implement such an intermediate page. Lopresti-Decl., [0093].

The Board already decided, based on Broder's teachings, that "'CAPTCHA' is a well-known tool for use in click fraud detection systems"; that POSAs would "reasonably expect success in incorporating a well-known CAPTCHA intermediate page of one click fraud detecting system (e.g., Broder) into other click fraud detecting systems (e.g.,...Willner)"; and that POSAs would "reasonably and readily have understood interjecting the CAPTCHA page to be desirable to slow down a clickbot attempting click fraud." IPR2022-00941, Paper 34 (FWD) at 46-47 (quotation omitted). Nobots did not appeal these findings.

E. Mapping to Challenged Claims

The sections below address independent claim 16 (the '014 patent's broadest claim) and its dependent claims first (*infra* §§VI.E.1—VI.E.6), then independent claim 1 and its dependents (*infra* §§VI.E.7—VI.E.18), and then independent claim 22 and its dependents (*infra* §§VI.E.19—VI.E.26).

1. **Claim 16: [16Pre] A non-transitory machine readable medium having stored thereon instructions for performing a method for providing a value indicating a judgment of whether a human or an autonomic computer application operating a client computer is interacting with a server, which when executed by at least one machine, causes the at least one machine to perform operations comprising:**

Petitioner believes the preamble is limiting. *See* EX1023

(Petitioner's/Defendant's district-court constructions). Willner-Kitts-Broder satisfies [16Pre]. Lopresti-Decl., [0095]-[0098].

The Willner-Kitts-Broder combination's functionality is implemented as "a computer program product on a computer-usable storage medium having computer-usable program code embodied in the medium;" i.e., a "***computer readable medium***" which may be "tangible" (i.e., *non-transitory*). Willner, [0024]-[0025]. The "***stored***" program "***instructions***" are "***execute[d]***" by "a ***machine***" to "***cause...operations to be performed***" that satisfy elements [16A]-[16E] as §§VI.E.1.a—VI.E.1.e below demonstrate. Willner, [0028]-[0030], claims 17-19. Willner says these operations can all be performed by, e.g., a website publisher's "server 102." Willner, [0045], [0043], [0053]; *see also* Kitts, [0044]-[0049] (web server performs the operations).

The Willner-Kitts-Broder functionality *performs* a "***method*** for detecting click fraud," whereby "[a] confidence level...is determined." Willner, Abstract, [0049], claims 8-9 ("***providing*** a confidence factor ***indicative*** of click fraud").

POSAs would have understood that the confidence level/factor is *a value*, because it can be “low”/“lower” or “high”/“higher.” Willner, [0049]-[0051]. “[A] low confidence factor...suggest[s] a possible click fraud attempt,” whereas “a high confidence factor...suggest[s] no click fraud”; therefore, the confidence *value indicates a judgment of whether* click fraud is occurring. Willner, [0050]-[0051], [0043] (Willner’s analysis is used to “**judge** whether or not this was click fraud”).

Specifically, Willner’s “confidence factor” is generated based on analyzing “cursor movement” to assess whether “a **human** is involved, as opposed to an **automated** tool” fraudulently moving the cursor. Willner, [0033]-[0036]. Such an “**automation** script” may be a “clickbot[]”—i.e., “**software** in a **computer**” (*an autonomic computer application*). Willner, [0004]-[0005], [0048]. The cursor is moved by either “a human controlling a pointing device (e.g., a mouse)” or “an automation tool” in a “**client** device” (“**computer**”) that is “access[ing] [a] website hosted by [a] **server**.” Willner, [0046]-[0047], [0054], [0048], [0041], [0044]. “[H]uman-like movement” produces “a high confidence factor,” while “not” human-like movement produces “a low confidence factor.” Willner, [0050]. Thus, the confidence *value indicates a judgment of whether a human or an autonomic computer application operating a client computer is interacting with a server*.

Broder likewise teaches to output “a **judgment** as to whether the web viewer is human or not,” as a “probabilistic” value. Broder, [0054], [0057]. Further,

providing the confidence level/factor as *a value indicating the judgment* would also have been obvious from Kitts's teaching that "any indicative **value** may be used to designate a quality score" that represents "the probability that a selection of an advertisement impression is initiated from a user or by software attempting to induce click fraud," as Willner's confidence level/factor and Broder's probabilistic judgment does. Kitts, [0031]-[0032]; Lopresti-Decl., [0098] (also citing EX1013 ("Afergan"), [0040], [0155], corroborating POSAs' background knowledge to *indicate a human/bot judgment as a value*).

a. [16A] provide data collection data requesting active and passive data of the client computer;

The '014 patent's specification never uses the term "*data collection data*." It does say that "[a]ctive and passive data" can be "collected" (FIG. 4), and it discusses collecting passive data the way such data is "normally...transmitted," such as in "browser cookies,...originating IP address,...etc.," and collecting "acquired data" (which is active data) via "some form of information capture means" implementable in, e.g., a "browser[]," "program," or "servlet/Java applet." EX1001, 3:19-27, 4:9-24. POSAs would therefore have understood such types of information capture means, and the listed browser cookies, etc., to be examples of *data collection data*.

Willner discloses *providing such data collection data requesting active data of the client computer*. For example, when the client device "accesses a web page

containing an advertisement[,] [c]lient code on the device tracks the movement of a cursor on the web page.” Willner, [0010]. The code can be “downloaded” from the server together with the webpage, and may be implemented as “markup that enables the cursor tracking” and/or as “applets, activeX, Javascript, etc.” Willner, [0042], [0054] (“code” may be “plug in used for the browser”). The webpage and/or its included markup/code are thus *data collection data provided* to the *client computer* like in the ’014 patent.

Based on the ’014 patent’s discussion of “active” model data, Petitioner proposes construing “*active data*” as “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.” *Active data* “includ[es], without limitation, **pointing device vector movements** and/or cadence, key stroke combinations and/or cadence, time differentials between stimulus...and user response..., and similar metrics.” EX1001, 3:3-15; *see* EX1023 (Petitioner’s/Defendant’s proposed district-court constructions).

It is undisputed that “cursor **movement vectors**” made “by a **pointing device** such as a mouse”—such as those Willner’s webpage markup/code requests and collects (Willner, [0033], [0046])—are examples of *active data* given in the ’014 patent. *See* EX1023 (parties’ proposed constructions of “*active data*”). Further, POSAs would have understood that these data are acquired from the user’s

interactions with the client computing device and are 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 the server. Willner, [0042]-[0043]; Lopresti-Decl., [0102]. This *data collection data* thus *requests active data of the client computer*.

As to *passive data*, based on the '014 patent's discussion of “passive” model data, Petitioner proposes construing “*passive data*” as “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.” Passive data “includ[es], without limitation, browser cookies, destination IP histories, originating IP address, originating IP address traffic data, originating IP address physical location, third party data regarding abusers (including originating IP addresses and physical locations), etc.” EX1001, 3:19-27; *see* EX1023 (Petitioner's/Defendant's proposed district-court constructions).

As discussed *supra* §VI.D.1, Willner-Kitts-Broder incorporates Kitts's teachings to analyze 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 POSAs 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-Decl., [0104]. Attributes may also be retrieved via browser cookies. Kitts, [0047]. Kitts thus teaches collecting *passive data of the client computer*, including via cookies which satisfy *providing data collection data requesting passive data*, as discussed above.

POSAs would have had motivation and reasonable expectation of success in incorporating such *passive data* collection and analysis for the reasons discussed *supra* §VI.D.1. These include Kitts’s teachings, which the Board already found “amply convey[] that ‘passive’ data has a recognized role in connection with bot detection systems” such that POSAs “would have recognized the benefit of employing additional data, e.g., Kitts’s passive data, specifically intended for bot detection in other systems, such as Willner’s,” and that POSAs “would have had a reasonable expectation of success in combining the teachings of Willner and Kitts.” IPR2022-00940, Paper 38 (FWD) at 34-36 (citing, e.g., Kitts, [0046]-[0047]).

Alternatively or additionally, as discussed *supra* §VI.D.1, POSAs would have had motivation and reasonable expectation of success in incorporating such *passive data* collection and analysis based on Broder’s teaching to “consider a large number of different factors,” including active and passive data, in differentiating humans from clickbots. Broder, [0043]-[0052], [0063]-[0070]. In

addition to *active data* such as data regarding mouse clicks (Broder, [0045]-[0046]), Broder teaches to also collect and analyze *passive data* such as IP address ([0051], [0068]), physical geographic origin ([0052], [0069]), and/or information from browser cookies ([0027]), which are examples of *passive data requested by data collection data* in the '014 patent.

Lopresti-Decl., [0099]-[0105].

- b. [16B] receive active and passive data responsive to the data collection data, the received active data relating to interactions of the client computer with a website of the server;**

Willner's method "includes *receiving data* related to...movement of a cursor" (*active data*). Willner, [0012]-[0014], [0055]. The webpage markup/code "enables the cursor tracking" for transmission to the server; thus, the data are received *responsive to the data collection data* as discussed *supra* §VI.E.1.a ([16A]). Willner, [0042]-[0043]. As discussed *supra* §VI.E.1 ([16Pre]), the cursor-movement data *relate to interactions of the client computer with a website of the server*. Willner, [0041] (client is "access[ing] the *website hosted on the server*"), [0042]-[0048], [0054].

Willner-Kitts-Broder also *receives passive data responsive to the data collection data* (e.g., via cookies) as discussed *supra* §VI.E.1.a ([16A]).

Lopresti-Decl., [0106]-[0107].

- c. [16C] analyze the received active...and...passive data for indication of a human or an autonomic computer application operating the client computer, ...in conjunction with model data based on human interactions from a prior session with the same website and developing a first analysis value;

Willner's method "detects a click fraud based on an *analysis of the received data*." Willner, [0012]-[0014]. "[A] confidence factor" (*a value—see supra* §VI.E.1 ([16Pre])) "may be determined based on the *analysis*" (Willner, [0036])—thus, *a first analysis value*. Willner's method "perform[s] vector *analyses* prior to click actions, and pattern *analyses* for hash values associated with iterative clicks" to "establish[] that a human is involved" or "an automation tool"—i.e., *analyzing the received active data for indication of a human or an autonomic computer application operating the client computer*. Willner, [0039]. Per Kitts's and/or Broder's teachings discussed *supra* §VI.D.1, Willner-Kitts-Broder also incorporates "*analytics*" on *the received passive data* "to calculate the quality score" (the combination's confidence-factor *first analysis value*) which indicates "a probability that the request is originating from an automated system." Kitts, [0049], [0021], [0032]-[0033]; Broder, [0010] (teaching to "*analyze[]* the web viewer's response...along with other information" (*passive data*) to determine "whether the web viewer is a human or non-human entity"), [0042]-[0057].

Willner's *analyzing includes analyzing the received active data in conjunction with model data* including "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. Willner explains that “duplication of vector patterns” does not occur in true human movements—instead, “the vector patterns for one user are substantially different from that of another user,” and even “repeated cursor movements of the same user...will be different from each other.” Willner, [0037]. Therefore, a cursor movement that is too similar to a past movement is likely “an automation tool attempting to simulate the actions of a user” (Willner, [0038]), like the ’014 patent discusses (EX1001, 5:9-23). Willner detects this by storing each previously collected cursor movement “as a linked list of vectors...represented as a sequence of hash codes” on the “server hosting the web page.” Willner, [0038]. When a later cursor movement is monitored, it “may be compared with previously stored hash codes or linked lists,” and “if the two compared items are analogous..., a low confidence level or factor may be determined, suggesting a possible click fraud attempt.” Willner, [0051], [0056].

The ’014 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.” EX1001, 2:64-3:1. POSAs would have understood Willner ([0037]-[0038]) to describe that the previously stored vector data can have been 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-Decl., [0110].

The vector data for previous cursor movements were stored when prior human users (e.g., “User A,” “User B”) interacted with “the web page associated with the click action.” Willner, [0037]-[0038]. Thus, the data are based on and indicative of human interaction with a computer environment. Each stored cursor movement is “from one position to another position with a control/URL on screen” in the webpage containing the advertisement (Willner, [0037]), and Willner’s claims discuss comparing current and previously stored vector data “associated with **the** path” taken by the cursor on that webpage (Willner, claims 10-11, 13-16, 18-19). POSAs would thus have understood, and alternatively would have found obvious, that the *model data* representing previous cursor movements were stored from when the prior users interacted with the same webpage by clicking on the same advertisements, thus allowing detection of automated “duplication” of the same movement path (“**the** path”). Willner, [0037], claims 10-19; Lopresti-Decl., [0111]. POSAs knew it was obvious to gather “user input for each user selection or target button on which the user clicks” and then “compare[]” the collected inputs from each “screen that a user may interact with” to “*previous sessions for those same screens*” so that common inputs may be appropriately compared or

correlated.” Lopresti-Decl., [0111] (quoting EX1017 (“Mak”), [0047], corroborating POSAs’ background knowledge).

Willner-Kitts-Broder thus *analyzes the received active data in conjunction with model data based on human interactions from a prior session with the same website*. See IPR2022-00940, Paper 13 at 18 (Board agreeing that Willner’s “server stores vector data collected from user interactions with the webpages of the website that the server hosts, for subsequent comparison by that server in assessing interactions with any one of those monitored webpages of that same hosted website.”).

Per Kitts’s and/or Broder’s teachings, Willner-Kitts-Broder also *analyzes the received passive data* as discussed above. Kitts teaches to feed “attributes and other parameters” including *passive data* “into a statistical **model**” to calculate the probabilistic *first analysis value*. Kitts, [0009], [0022], [0049], [0068]. The attributes/parameters can include “the number of new users who have accessed **the** web page” previously, “the number of times the user or program has selected **the** advertisement, requested **the** web page,...etc.,” which are *based on human interactions from a prior session with the same website*. Kitts, [0047], [0049]. POSAs knew that statistical models that Kitts discusses (e.g., “Bayesian model, regression model, neural network,” etc.—Kitts, [0049], [0068]) are commonly trained on data including the same attributes/parameters they are later used to test.

See, e.g., Broder, [0073]-[0074] (corroborating POSAs' knowledge that statistical models like "Bayesian classifier[s]" are built by "post-process[ing]" the same data collected from past users that the model will analyze from new users); EX1016 ("Emigh"), 18:31-67 (similar); Lopresti-Decl., [0113]. Therefore, Kitts teaches and renders obvious *analyzing the received passive data in conjunction with model data* including the same attributes/parameters *based on human interactions from a prior session with the same website*.

Broder likewise teaches to use "a Bayesian classifier" (statistical *model data*) trained on post-processed data collected from "how web viewers *interact*" with the same "web page." Broder, [0073]-[0074]. These data include "all of [the] available information" Broder discusses collecting, which includes active and passive data as discussed *supra* §VI.D. Broder, [0073].

Lopresti-Decl., [0108]-[0114].

d. [16D] determine that the first analysis value fails to meet a first analysis predetermined criteria; and

Willner teaches that when "an analogous hash sequence pattern and/or an analogous linked list" is detected by comparing the current cursor movement to "previously stored hash codes or linked lists," a "low confidence factor" is "determined suggesting a possible click fraud attempt." Willner, [0050]-[0051], [0055]-[0056]. In Willner-Kitts-Broder, passive data also contributes to the confidence level based on Kitts's and/or Broder's teachings, as discussed *supra*

§VI.D.1. “The confidence factor can be used to deny the action of click” if the determined confidence level is too low (i.e., not “consistent with a human”).

Willner, [0036]. POSAs knew it was typical to pre-specify “target criteria” as to a “threshold...value” that such a “score...must have” in order to allow the requested action. *See* Kitts, [0060], [0068]; Lopresti-Decl., [0115]-[0116] (also citing corroborating EX1016 (“Emigh”), 10:57-60). POSAs would have understood and found it obvious, therefore, that the threshold value the confidence factor must surpass is a *predetermined criteria*. Willner-Kitts-Broder thus *determines that the first analysis value* (confidence factor/level) *fails to meet a first analysis predetermined criteria* when it is lower than a pre-specified threshold under which the confidence value is considered “low” and access to the advertised webpage is disallowed. Lopresti-Decl., [0116].

e. [16E] provide a request for further data from the client computer based on the determination....

As discussed *supra* §VI.D.2, Willner-Kitts-Broder applies Broder’s teaching to “consider a large number of different factors...collected from the web viewer” to determine whether to “interject[] an intermediate page” after the click on the advertisement. Broder, [0062]-[0063]; *see also* EX1007 (“O’Connell”), [0032], corroborating POSAs’ background knowledge that “request[ing] additional authentication information” is “appropriate course of action” based on “fraud detection results.” The analysis can consider any “click fraud indicators” that may

“raise the level of suspicion” that the client may be a bot (Broder, [0070]-[0072]); in Willner-Kitts-Broder as discussed *supra* §VI.D.2, this analysis includes the active and passive data analysis discussed *supra* §§VI.E.1.a—VI.E.1.d ([16A]-[16D]). When *the first analysis value fails to meet the first analysis predetermined criteria* (i.e., the confidence value is lower than a pre-specified threshold, raising the level of suspicion of click fraud as discussed *supra* §VI.E.1.d ([16D])), the combination “selects and displays an intermediate web page for testing the web viewer” as Broder ([0072]) teaches.

“The intermediate page may take many different forms” which “may vary widely depending on the circumstances.” Broder, [0029], [0032]. Various options may “require[] a web viewer to click a specified location,” and/or may “*request*[]” “demographic information,” or request a response to a CAPTCHA. Broder, [0034], [0036], [0039]-[0040]. Any of these examples *provides a request for further data from the client computer based on the determination that the first analysis value fails to meet the first analysis predetermined criteria*.

Lopresti-Decl., [0117]-[0118].

2. Claim 17: ...failing to meet the first analysis predetermined criteria indicates that the client computer should not be allowed access to a protected page of the website.

Willner teaches that a low “confidence factor” (*the first analysis value failing to meet the first analysis predetermined criteria*) “can be used to deny the

action of click on an advertisement.” Willner, [0036]. If the action were not denied, “a *web page*...associated with clicking on the advertisement” would “be displayed.” Willner, [0045]. Because it will only be “displayed” if “a high confidence level/factor [is] determined, suggesting no click fraud” (Willner, [0051]), the page linked to the advertisement is *a protected page*. While a publisher’s website that contains the advertisement (Willner, [0041], [0044]) may “typically” be “unaffiliated” with the advertiser (Willner, [0002]), POSAs knew that in other cases the publisher and advertiser can be “the same entity,” as Broder teaches. Broder, [0025] (“For example, an advertising network may also provide its own web content and thus also be the web publisher.”). In this scenario, POSAs would have understood that the publisher’s page containing the clickable advertisement (with which the client is interacting) and the advertiser’s page to which the advertisement links (the *protected page*) can both be *pages of the same website* hosted by the publisher-advertiser. Lopresti-Decl., [0119]-[0120].

Therefore, in the Willner-Kitts-Broder combination, *the first analysis value failing to meet the first analysis predetermined criteria indicates that the client computer should not be allowed access to a protected page of the website* at that time. This is further consistent with Broder’s teaching to “interject[] with an intermediate web page” rather than “redirect[ing] the web viewer to the advertiser’s designated web site,” if any “click fraud indicators...raise the level of

suspicion regarding this web viewer.” Broder, [0070]-[0071]. Although *the client computer should not be allowed access* at the time of interjection, the client may later gain access by responding properly to the intermediate page, as the ’014 patent’s claims contemplate. *See infra* §§VI.E.5—VI.E.6 (claims 20-21).

Lopresti-Decl., [0121].

3. Claim 18: ...analyzing the at least one browser cookie, the at least one IP address, and the manual input device activity in conjunction with model data based on human interactions from a prior session with the same website.

Willner’s *received active data includes* “cursor movement vectors (e.g., those initiated by a pointing device such as a mouse)”—i.e., *manual input device activity*. Willner, [0033], [0046]-[0047]. It is *analyzed in conjunction with model data based on human interactions from a prior session with the same website*, as discussed *supra* §VI.E.1.c ([16C]). Willner, [0037]-[0039].

Willner-Kitts-Broder’s *received passive data includes at least one browser cookie and at least one IP address* per Kitts’s and/or Broder’s teachings. Kitts, [0046] (“**(IP) address**”), [0047] (“**cookies** provide the web server with the **IP address** of a user submitting a page request as well as the time the page was requested[,]. . . the identity of a user requesting a web page, the number of new users who have accessed the web page, or how often a visitor has visited the web page.”), [0048], [0067]; Broder, [0027] (“‘**cookie**’ information..., the web viewer’s Internet Protocol (**IP) address**”). The *browser cookie(s)* and *IP address* are

analyzed in conjunction with model data based on human interactions from a prior session with the same website, as discussed supra §VI.E.1.c ([16C]). Kitts, [0047]-[0049]; Broder, [0073]-[0074].

Lopresti-Decl., [0122]-[0123].

4. Claim 19: ...decrypt the received active...and...passive data.

POSAs knew, as background knowledge, that some pay-per-click advertising platforms were configured such that “client and server computers communicate using” encrypted “communications protocols, such as Secure Hypertext Transfer protocol (HTTPS),” Secure Sockets Layer (SSL), etc. Lopresti-Decl., [0124] (quoting corroborating EX1018 (“Swanson”), [0039], [0006]-[0007], [0058]) (also citing corroborating EX1019 (“Ling”), 4:52-55 (“[A]ll or some of links can be encrypted using conventional encryption technologies such as the secure sockets layer (SSL), Secure HTTP and/or virtual private networks (VPNs).”), 3:43-61). POSAs would have found it obvious that when the Willner-Kitts-Broder bot-detection techniques are applied in this environment, data transmitted from client to server are encrypted, including *the received active data and the received passive data*, and the server would then *decrypt that received data* to analyze it. Lopresti-Decl., [0125].

5. Claim 20:

- a. [20A] receive further data from the client computer in response to the request for further data;**

When Willner-Kitts-Broder interjects an intermediate page as discussed *supra* §VI.E.1.e ([16E]) (*the request for further data*), *the client computer responds* by providing *further data* accordingly. Broder, [0042] (“after displaying the intermediate web page...if any *response* was *received*,” the “system then stores and analyzes the web viewer’s response”).

- b. [20B] perform a second level of analyzing on the received further data; and**

Willner-Kitts-Broder *performs a second level of analyzing* when it “*analyzes* the web viewer’s response to the intermediate page.” Broder, [0042].

- c. [20C] provide a second analysis value based on the second level of analyzing.**

The “output” of this *second level of analyzing* includes “a judgment as to whether the web viewer is human or not,” which “is only probabilistic.” Broder, [0054], [0057]. POSAs would have found it obvious to implement such a probabilistic judgment by *providing a value* (here, *a second analysis value*) such as a score or confidence level. *See* Kitts, [0032] (“any indicative *value* may be used to designate a quality score” that can refer to a human/bot “probability”).

Lopresti-Decl., [0126]-[0128].

6. Claim 21: ...the received further data includes the response of the client computer to a CAPTCHA test provided to the client computer.

As discussed *supra* §VI.E.1.e ([16E]), one option for the interjected intermediate webpage requesting *further data* is “a **CAPTCHA** page” that presents “a challenge-response *test* used to determine whether or not the web viewer is human.” Broder, [0039].³ One example “requires [] the web viewer to...type in the letters and numbers displayed in the distorted image.” Broder, [0040]. Thus, *the received further data includes the response of the client computer to a CAPTCHA test provided to the client computer. See also infra* §VI.E.7.i ([11I]) (discussing the *second analysis value* when Broder’s intermediate page includes a *CAPTCHA test*). Lopresti-Dec1., [0129]-[0130].

7. Claim 1: [1Pre] ...generating a value indicative of a likelihood that a human or autonomic computer application is operating a client computer attempting access to a protected page of a website...

Petitioner believes the preamble is limiting. *See* EX1023 (Petitioner’s/Defendant’s district-court constructions).

³ Broder’s CAPTCHA is thus a test to determine if a computer user is a human or a bot, which was a construction Petitioner originally proposed for “*CAPTCHA test*” in communication between the district-court parties. Petitioner subsequently withdrew that proposed construction following a meet-and-confer to narrow terms.

[1Pre] shares much of the same language as [16Pre], which Willner-Kitts-Broder satisfies for reasons discussed *supra* §VI.E.1.

The Willner-Kitts-Broder *method generates* a confidence level/factor (the *value* discussed *supra* §VI.E.1 ([16Pre])). Willner, Abstract, [0049] (“confidence factor may be ***generated***”). “[H]uman-like movement” produces “a high confidence factor” that “suggest[s] no click fraud” (i.e., the client is likely human), while “not” human-like movement produces “a low confidence factor” that “suggest[s] a possible click fraud attempt” (i.e., the client is likely a bot). Willner, [0050]-[0051]. Thus, the confidence *value* is *indicative of a likelihood that a human or autonomic computer application is operating a client computer*. By “clicking on [an] advertisement” (Willner, [0045]), the client is *attempting access to a protected page of a website*, for the reasons discussed *supra* §VI.E.2 (claim 17). Lopresti-Decl., [0131]-[0132].

- a. **[1A] provide data collection data that causes the client computer to collect active data relating to interactions of the client computer with a given page of the website;**

Willner discloses *providing data collection data that causes the client computer to collect active data*, as discussed *supra* §VI.E.1.a ([16A])). For example, when the client device “accesses a web page containing an advertisement,” markup/code downloaded with the webpage becomes “[c]lient code on the device [that] tracks the movement of a cursor on the web page.”

Willner, [0010], [0042], [0054]. The cursor-movement *active data relate to interactions of the client computer with a given page of the website* (i.e., the client moving a cursor to click on an advertisement in the page). As discussed *supra* §VI.E.2 (claim 17), the webpage containing the advertisement can be *a given page of the same website* as the *protected page* to which the advertisement links—e.g., when the *website* host is both publisher and advertiser. Lopresti-Decl., [0133].

- b. [1B] receive at least some of the collected active data...and at least some passive data from the client computer;**

Willner-Kitts-Broder meets [1B] for the reasons discussed *supra* §VI.E.1.b ([16B]). The *active* and *passive data* are *received from the client computer*.

Willner, [0043]; Kitts, [0047]-[0048]; Broder, [0043], [0063].

- c. [1C] perform a first analysis comprising analyzing at least some of the received active...and...passive data in conjunction with model data based on human interactions from a prior session with the same website;**

Willner-Kitts-Broder *performs a first analysis* meeting [1C] in the manner discussed *supra* §VI.E.1.c ([16C]).

- d. **[1D] generate a first analysis value based on the first analysis, wherein the client computer is allowed to access the protected page without requiring an operator of the client computer to decipher a CAPTCHA test if the first analysis value meets a first analysis predetermined criteria;**

Willner-Kitts-Broder *generates a first analysis value* (a confidence factor/level) *based on the first analysis* as discussed *supra* §VI.E.1.c ([16C]).

Willner teaches that when “a high confidence level/factor [is] determined, suggesting no click fraud[,] [t]he click on the advertisement may be processed, and an associated web page...displayed.” Willner, [0051]. Thus, *the client computer is allowed to access the protected page without requiring an operator of the client computer to decipher a CAPTCHA test if the first analysis value meets a first analysis predetermined criteria* (a confidence level higher than a pre-specified threshold; *see* discussion *supra* §VI.E.1.d ([16D])). As discussed *supra* §VI.D.2, this also comports with Broder’s teachings to “only occasionally interject[] an intermediate page” for those “few of the web viewers” whose “click fraud indicators...raise the level of suspicion,” and that “a CAPTCHA task” “should be avoided in most situations.” Broder, [0062], [0070], [0041]. Broder likewise teaches that “[i]f the system opts not to interject, the system proceeds...to redirect the web viewer to the advertiser’s designated web site” (*the protected page*). Broder, [0071].

Lopresti-Decl., [0134]-[0137].

- e. **[1E] determine that the first analysis value fails to meet the first analysis predetermined criteria;**

See supra §VI.E.1.d ([16D]).

- f. **[1F] provide a CAPTCHA test to the client computer based on the determination...;**

Willner-Kitts-Broder meets [1F] for the reasons discussed *supra* §VI.E.1.e ([16E]) and §VI.E.6 (claim 21). Broder further teaches that “*if* it seems that a web site is being attacked by a malicious robot program” (e.g., if *the first analysis value fails to meet the first analysis predetermined criteria*), “that web site may elect to use a **CAPTCHA** intermediate page.” Broder, [0041]. *See also* EX1016 (“Emigh”), 10:21-42 (corroborating POSAs’ background knowledge to issue CAPTCHA challenge based on whether “spam likelihood value” crosses a “threshold”). Lopresti-Decl., [0138]-[0139].

- g. **[1G] receive a response of the client computer to the CAPTCHA test;**

See supra §§VI.E.5—VI.E.6 (claims 20-21).

- h. **[1H] perform a second analysis comprising assessing accuracy of the response...; and**

Willner-Kitts-Broder meets [1H] for the reasons discussed *supra* §§VI.E.5—VI.E.6 (claims 20-21). In particular, Broder teaches to “*analyze*[] the web viewer’s response to the intermediate page,” including analyzing “the content of the response.” Broder, [0042], [0046]. For example, “[i]f the response” is “not logical then the response may be from a computer program.” Broder, [0046].

POSAs would have known that for a CAPTCHA intermediate page (e.g., a “CAPTCHA that requires the entry of letters and/or digits displayed in a distorted image”) (Broder, [0039]-[0041]), analyzing whether the response is logical *comprises assessing accuracy of the response to the CAPTCHA test*. Lopresti-Decl., [0140]-[0141]; *see also* EX1020 (“Lillibridge”, Abstract (incorporated by reference in Broder, [0040])).

- i. **[1I] generate a second analysis value based on the second analysis, wherein the client computer is granted access to the protected page based on the second analysis value meeting a second analysis predetermined criteria.**

Broder teaches to “analyze[] the web viewer’s response to the intermediate page” using an “adjustable policy” to “output” a “judgment as to whether the web viewer is human or not and a determination of how to proceed with the request.” Broder, [0042], [0054]. The human/bot “judgment is only probabilistic”⁴ and can

⁴ For example, POSAs would have known that when the client responds correctly to the CAPTCHA, there may still be some probability that the client is a bot, such as “[i]f a response is received nearly instantaneously,” in “the middle of the night,” or “from an IP address that has previously been determined to be a non human entity.” Broder, [0045]-[0052]. Likewise, POSAs knew that even humans sometimes respond incorrectly to CAPTCHAs. Lopresti-Decl., [0142]; *cf.*

be made using, e.g., “a Bayesian classifier.” Broder, [0057], [0074]. POSAs would therefore have understood and found it obvious that the judgment *generates a second analysis value based on the second analysis*, reflecting a probability that the client is human or bot. See Kitts, [0031]-[0032] (“any indicative *value* may be used” to “refer to the probability”); Lopresti-Decl., [0142]-[0144] (also citing corroborating EX1016 (“Emigh”), 26:55-57 (“a Bayesian...classifier may be used to create a numeric *value* that corresponds to an estimated likelihood”).

Broder teaches that “[i]f the adjustable policy determines that the web viewer is likely to be human” (i.e., *based on the second analysis value meeting a second analysis predetermined criteria*—e.g., the probability or confidence that the client is human is high), “the system redirects the web viewer’s web browser to” (i.e., *the client computer is granted access to*) “the advertiser’s designated web site” (*the protected page—see supra §VI.E.2 (claim 17)*). Broder, [0058].

EX1001, 1:47-53. POSAs thus understood why Broder teaches to “consider a large number of different factors” and render an “only probabilistic” judgment even when the intermediate page is a CAPTCHA. Broder, [0043], [0057].

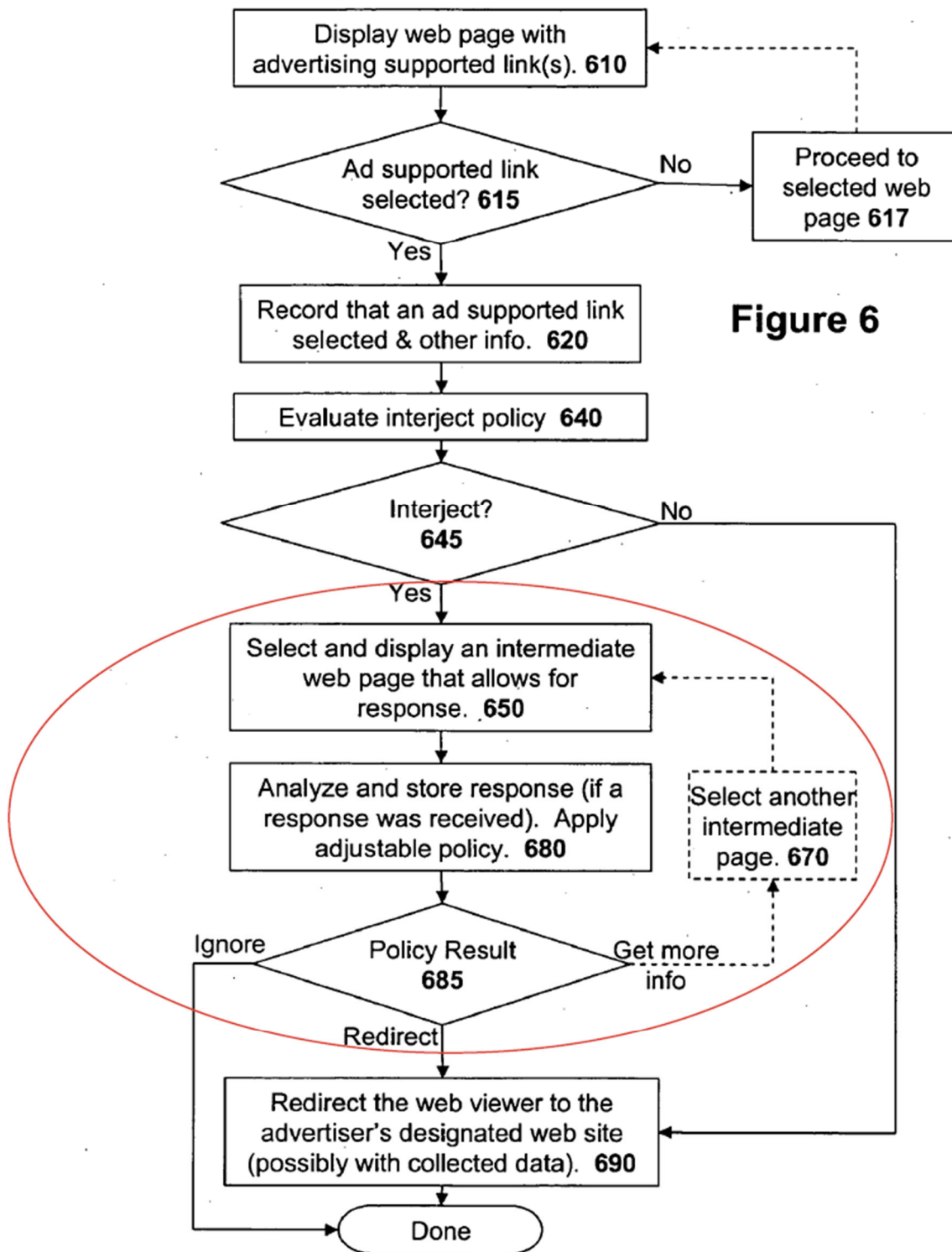
8. Claim 2:

- a. [2A] provide an additional CAPTCHA test to the client computer based on the determination that the second analysis value fails to meet the second analysis predetermined criteria;**

Broder teaches that, following the analysis and judgment of the client's response to the first intermediate webpage, "the adjustable policy may request that *additional* information be collected from the web viewer in order to make a more accurate determination." Broder, [0059]. POSAs would have known that one situation warranting "a more accurate determination" is when the probabilistic judgment from the first intermediate webpage response does not reflect high confidence that the client is human (i.e., *based on the determination that the second analysis value fails to meet the second analysis predetermined criteria*), because the "judgment is only probabilistic and is not a final authoritative determination as to whether the activity is robotic." Broder, [0057]; *see also* EX1016 ("Emigh"), 19:65-20:3 (corroborating POSAs' knowledge to "issue an additional challenge" to address "uncertainty" in the determination). For example, POSAs knew that a CAPTCHA can receive an incorrect response even if the user is actually human, because humans can make mistakes. Lopresti-Decl., [0145]. Additionally, POSAs would have had reason to request additional information if the probabilistic judgment is accurate that the client is actually a bot, because requesting additional information would beneficially "slow down the automated

program and make it less efficient” at attempting fraud. Lopresti-Decl., [0146] (quoting corroborating EX1007 (“O’Connell”), [0049]; EX1008 (“Meek”), [0008]).

Broder teaches that in this scenario, the system “select[s] another intermediate web page that will be used to obtain *additional* information from the web viewer.” Broder, [0059]. As with the first intermediate webpage, one selectable option for the second intermediate webpage is *an additional CAPTCHA test*. Broder, [0039]-[0041]. “The system will then repeat the steps of displaying the newly selected intermediate web page (step 250), analyzing and storing the web viewer’s response to the newly selected web page with the adjustable policy (step 280), and implementing the output of the adjustable policy determination (step 285).” Broder, [0059]. Broder illustrates this process as a “Get more info” loop in Figure 6 (annotated below):



For example, in a scenario where *the second analysis value fails to meet the second analysis predetermined criteria* because the client responded incorrectly to the first CAPTCHA, POSAs would have found it obvious to *provide an additional CAPTCHA test to the client computer* in order to delay and withhold access, while providing a second chance in case the client is actually human who made a mistake, as discussed above. Lopresti-Decl., [0147]-[0151].

b. [2B] receive a response of the client computer to the additional CAPTCHA test;

Broder teaches receiving “the web viewer’s response to the newly selected web page.” Broder, [0059].

c. [2C] perform a third analysis comprising assessing the accuracy of the client computer’s response to the additional CAPTCHA test; and

Broder teaches “*analyzing* and storing the web viewer’s response to the newly selected web page with the adjustable policy.” Broder, [0059], Fig. 6 box 680 (reproduced above). This *comprises assessing the accuracy of the client computer’s response to the CAPTCHA* in the manner discussed *supra* §VI.E.7.h ([1H]).

- d. **[2D] generate a third analysis value based on the third analysis, wherein the client computer is granted access to the protected page based on the third analysis value meeting a third analysis predetermined criteria.**

Broder ([0059]) teaches “*analyzing*” the response “with the adjustable policy...and implementing the output of the adjustable policy determination,” which *generates an analysis value and grants access based on that analysis value meeting a predetermined criteria* in the manner discussed *supra* §VI.E.7.i ([11]).

9. **Claim 3: ...when the first analysis value meets a first analysis predetermined criteria, the client computer is not presented with a CAPTCHA test prior to the client computer being granted access to the protected page.**

As discussed *supra* §VI.E.7.d ([1.D]), Willner-Kitts-Broder does not present an intermediate webpage (i.e., *the client computer is not presented with a CAPTCHA test*) prior to the client computer being granted access to the protected page when the first analysis value meets a first analysis predetermined criteria (high confidence level/factor suggests no click fraud based on analysis of active and passive data). Lopresti-Decl., [0152].

10. **Claim 4: ...decrypt the received active data and the received passive data.**

See supra §VI.E.4 (claim 19).

11. **Claim 5: ...the model data is based on human interaction from a prior session with the same given page.**

See supra §VI.E.1.c ([16C]).

12. Claim 6: ...the ability of the client computer to collect active data is only active while the client computer is visiting a web page enabled with data collection data.

As discussed *supra* §VI.E.1.a ([16A]), Willner’s “server...downloads [to the client] *the web page*” that the client *is visiting*, “which may include markup that *enables* the cursor tracking,” and/or downloads “code (e.g., applets, activeX, Javascript, etc.)” together with the webpage. Willner, [0042], [0054]. Therefore, because the cursor-tracking markup and/or code (*data collection data*) is provided in or with the webpage, *the ability of the client computer to collect active data* (track cursor movements) *is only active while the client computer is visiting a web page enabled with data collection data*. Lopresti-Decl., [0155] (citing corroborating EX1021 (“Nir”), [0007]-[0009]).

13. Claim 7: ...receive the first or second analysis predetermined criteria from an operator or administrator of the website.

Broder teaches that “the advertiser’s preference” may “specify” how to “determin[e] how often to interject” with an intermediate webpage, and for which “web viewers” to interject. Broder, [0065]. POSAs would have understood and found obvious from this disclosure that the advertiser can specify *the first analysis predetermined criteria* setting the threshold level of suspicion that will trigger interjection (discussed *supra* §VI.E.1.e ([16E])). Lopresti-Decl., [0156].

Broder likewise teaches that “the advertiser’s preference” may factor into whether access is withheld or granted based on the client’s response to an intermediate webpage. Broder, [0048]. POSAs would have understood and found obvious from this disclosure that the advertiser can specify *the second analysis predetermined criteria* setting the threshold analysis value for approving the client’s response (discussed *supra* §VI.E.7.i ([1I])). Lopresti-Decl., [0157].

Broder also teaches that the advertiser “may also provide its own web content and thus also be the web publisher” of the webpage, and thus *an operator or administrator of the website*. Broder, [0025]; *see supra* §VI.E.2 (claim 17).

Therefore, POSAs would have found it obvious based on Broder’s disclosures to implement Willner-Kitts-Broder *to receive the first and/or second analysis predetermined criteria from an operator or administrator of the website*. Kitts similarly teaches that “the advertiser can specify a threshold quality score that a page request must have before an advertisement can be displayed.” Kitts, [0060], [0031], [0068], [0071]. Lopresti-Decl., [0158]-[0159].

14. Claim 8: ...receive from an operator or administrator of the website a number of CAPTCHA tests that will be provided to a client computer after the second analysis value fails to meet the second analysis predetermined criteria.

Broder discloses that “[t]he intermediate web page may be provided by the web publisher, the advertising network, or the advertiser.” Broder, [0031]. One

type of intermediate webpage is a *CAPTCHA test* as discussed *supra* §VI.E.6 (claim 21). Broder, [0039]-[0041]. As discussed *supra* §VI.E.2 (claim 17), the publisher and advertiser “may be the same entity” that hosts the website. Broder, [0025]. Thus, Broder teaches *receiving the CAPTCHA tests from an operator or administrator of the website*.

As discussed *supra* §VI.E.8.a ([2A]), Willner-Kitts-Broder *provides* such a *CAPTCHA test* to the *client computer after the second analysis value fails to meet the second analysis predetermined criteria*, based on Broder’s teaching to “repeat” providing “another intermediate web page...to obtain additional information from the web viewer.” Broder, [0059]. Broder’s Figures 2 and 6 illustrate that this can be performed in a loop, which can present a third intermediate page after analyzing the response to the second intermediate page, and so on:

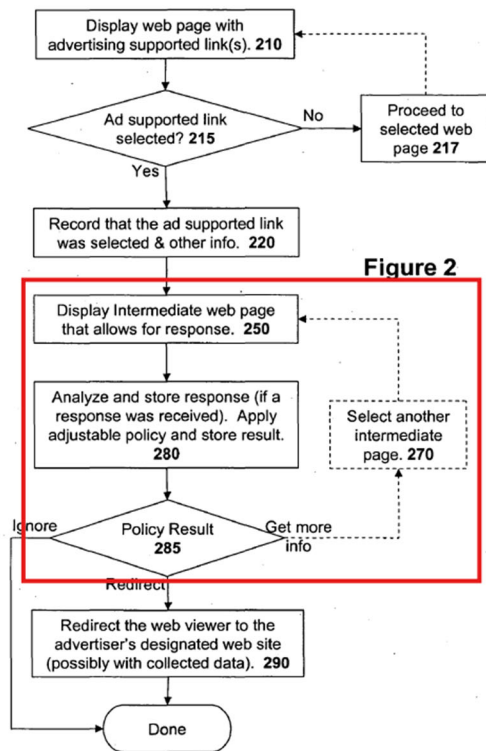


Figure 2

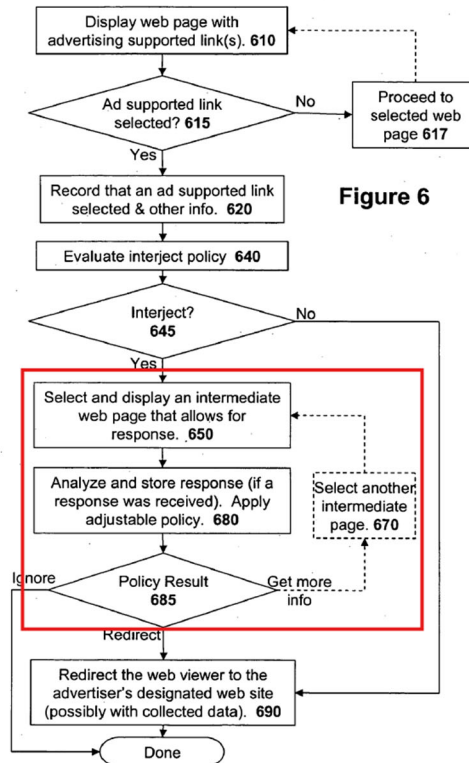


Figure 6

Broder, Figs. 2 and 6 (annotated)

Each of these intermediate pages can be a *CAPTCHA test*. Broder, [0039]-[0041]. Thus, POSAs would have understood and found obvious from Broder's disclosure that *a number of CAPTCHA tests can be provided to a client computer after the second analysis value fails to meet the second analysis predetermined criteria*. For the reasons discussed *supra* §VI.E.8.a ([2A]), POSAs would have found it obvious to *provide a number of additional CAPTCHA tests sequentially after a first CAPTCHA has received an incorrect response, in order to delay and withhold access by prolonging the loop if the client is a bot, and to provide*

additional chances to answer correctly in case the client is actually human.

Lopresti-Decl., [0160]-[0162].

Additionally, POSAs would have understood that the choice of how many additional *CAPTCHA tests to provide* would be a design choice, balancing between how much an advertiser wishes to avoid rejecting legitimate human customers who make mistakes versus admitting a fraudulent bot that could make a lucky guess if given enough tries. *See, e.g.,* Broder, [0041]. POSAs knew that “a retry limit may be predefined or user-defined” for how many times “another challenge should be sent” following an incorrect response to the previous CAPTCHA. Lopresti-Decl., [0163] (quoting corroborating EX1016 (“Emigh”), 20:41-58). POSAs would therefore have found it obvious to allow the advertiser to specify the number of CAPTCHA tests to provide (i.e., *receive from an operator or administrator of the website a number of CAPTCHA tests*), which is also consistent with Broder’s teaching to allow “advertiser’s preference” to specify how to “determin[e] how often to interject.” Broder, [0065]; Lopresti-Decl., [0163].

15. Claim 10: ...the data collection data comprises JavaScript code that causes a browser of the client computer to collect the active data.

Willner’s *data collection data* (*supra* §VI.E.1.a ([16A]) can include “downloaded *code* (e.g.,...*Javascript*, etc.).” Willner, [0042]. This “*browser code*” is “installed on the *client* device” and “track[s] cursor movement.” Willner,

[0054], [0009]-[0011] (cursor tracking performed “by the browser”). Lopresti-Decl., [0164].

- 16. Claim 11: ...analyzing the at least one browser cookie and the at least one IP address in conjunction with the model data.**

See supra §VI.E.3 (claim 18).

- 17. Claim 12: ...analyzing manual device input activity of the client computer in conjunction with the model data based on human interaction with the same given page.**

See supra §VI.E.1.c ([16C]) and §VI.E.3 (claim 18).

- 18. Claim 14: ...the human interaction...includes human interaction of another client computer from the prior session with the same given page.**

Willner-Kitts-Broder meets claim 14 for the reasons discussed *supra* §VI.E.1.c ([16C]). The combination’s *model data* includes prior cursor click paths by “**different users** (or the same user).” Willner, [0037]-[0038]. POSAs would have understood that different users’ previously stored data *includes human interaction of another client computer from the prior session with the same given page* discussed *supra* §VI.E.1.c ([16C]). Lopresti-Decl., [0167].

- 19. Claim 22:**

[22Pre] is identical to [16Pre] and satisfied as discussed *supra* §VI.E.1.

- a. **[22A] provide instructions that allow client computer interactions with a website of the server to be remotely monitored;**

See supra §§VI.E.1.a—VI.E.1.b ([16A]-[16B]). Willner’s cursor-movement-monitoring markup and/or code, and Kitts’s and/or Broder’s cookies, *provide instructions that allow client computer interactions with a website of the server to be remotely monitored* by sending cursor-movement data and passive data associated with the webpage request to the server hosting the website. Lopresti-Decl., [0169].

- b. **[22B] receive monitored data originating with the client computer, ...comprising active data relating to interactions of the client computer with the website and passive data of the client computer;**

Willner-Kitts-Broder *receives active data relating to interactions of the client computer with the website and passive data of the client computer, originating with the client computer*, for the reasons discussed *supra* §§VI.E.1.a—VI.E.1.b ([16A]-[16B]).

The ’014 patent defines “*monitored data*” at 3:43-51. Willner-Kitts-Broder satisfies this definition because, as discussed *supra* §§VI.E.1.a—VI.E.1.b ([16A]-[16B]), Willner-Kitts-Broder obtains its active data (which is acquired) and its passive data (which is available) from the client computing device, and as a result of the client’s external interactions with the server, after generation of the webpage for download (with the webpage being “issued data” because it is generated by the

publisher's server, which is not the same as the client computing device).

Lopresti-Decl., [0170]-[0171].

- c. **[22C] analyze the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including:**

See supra §VI.E.1.c ([16C]).

- d. **[22D] perform a first level of analyzing on the received monitored data for any indication that a human may be operating the client computer to obtain a first-level analysis;**

As discussed *supra* §VI.D, Broder teaches to “consider a large number of different factors” in “determin[ing] whether the web viewer is human or not,” and it would have been obvious to incorporate consideration of any of those factors in Willner-Kitts-Broder. Broder, [0042]-[0043]. Exemplary factors include whether “no input is received from the web viewer within a particular time limit,” or whether “a response is received nearly instantaneously,” either of which suggest the client may not be human. Broder, [0044]-[0045]. Each of these is *analyzing the received monitored data for any indication that a human may be operating the client computer*. If no input is received or essentially no time elapses in which movement could have occurred before a response, there is no *indication that a human may be operating the client computer*, because there has been no detected human activity (e.g., no cursor movement). Lopresti-Decl., [0173].

POSAs would have found it obvious to incorporate this analysis as *a first level of analyzing to obtain a first-level analysis*—e.g., before analyzing cursor-movement vector patterns using Willner’s techniques as discussed *supra* §VI.E.1.c ([16C])—because if there is no detected human activity then there would be no vector patterns warranting analysis. Lopresti-Decl., [0174].

- e. **[22E] perform a second level of analyzing to obtain a second-level analysis, when the first-level analysis does not meet a first-level analysis predetermined criteria, the second level of analyzing comprising analyzing the received monitored data in conjunction with previously recorded data relating to human interactions from a prior session with the same website; and**

Willner-Kitts-Broder *performs* [22E]’s *second level of analyzing* by the analysis of cursor movements and passive data discussed *supra* §VI.E.1.c (discussing [16C]’s “*first*” analysis). As discussed *supra* §VI.E.19.d ([22D]), this *second level of analyzing* (including analyzing cursor-movement vectors) is performed *when the first-level analysis does not meet a first-level analysis predetermined criteria* (e.g., when the *first-level analysis* does not conclude that there has been no input or that an instantaneous click has been received with no cursor movement).

- f. **[22F] provide a second-level analysis value when the second-level analysis meets a second-level analysis predetermined criteria.**

The second-level analysis in [22F] meets a second-level analysis predetermined criteria in Willner-Kitts-Broder when “a high confidence level/factor [is] determined, suggesting no click fraud,” in the analysis discussed *supra* §VI.E.1.c (discussing [16C]’s “*first*” analysis). Willner, [0051]. For example, Willner teaches *predetermined criteria* for deciding whether current and previously recorded cursor movements are “deemed analogous”—“if they have the same slope and overlap by a minimum number of pixels.” Willner, [0052]. If they “are not analogous” (i.e., *the second-level analysis meets a second-level analysis predetermined criteria*), “a high confidence level/factor may be determined” (*providing a second-level analysis value*). Willner, [0051]. In Willner-Kitts-Broder, the *predetermined criteria* also account for passive data, as discussed *supra* §VI.E.1.c ([16C]). Lopresti-Decl., [0175]-[0177].

20. Claim 23: ...decrypt the received monitored data.

See supra §VI.E.4 (claim 19).

21. Claim 24: ...the monitored data comprises active data relating to interactions of the client computer with a given page of the website and passive data of the client computer, and the recorded data relates to human interaction from a prior session with the same given page.

See supra §VI.E.1.c ([16C]).

- 22. Claim 25: ...provide a request for further data from the client computer based on the determination that the second-level analysis does not meet the second level analysis predetermined criteria.**

See supra §VI.E.1.e ([16E]) (where claim 25's *second-level analysis* corresponds to claim 16's *first analysis*).

- 23. Claim 26:**

- a. [26A] receive further data from the client computer in response to the request for further data;**

See supra §VI.E.5.a ([20A]).

- b. [26B] perform a third-level of analyzing on the received further data; and**

See supra §VI.E.5.b ([20B]) (where claim 26's *third-level of analyzing* corresponds to claim 20's *second level of analyzing*).

- c. [26C] provide a third-level analysis value after completion of the third-level of analyzing.**

See supra §VI.E.5.c ([20C]) (where claim 26's *third-level analysis value* corresponds to claim 20's *second analysis value*).

- 24. Claim 27: ...the request for further data includes a CAPTCHA test.**

See supra §VI.E.6 (claim 21).

- 25. Claim 28: ...the received monitored data includes at least one browser cookie and at least one IP address.**

See supra §VI.E.3 (claim 18).

26. Claim 29: ...the received monitored data includes manual device input activity.

See supra §VI.E.3 (claim 18).

VII. GROUND 2: CLAIMS 4, 19, AND 23 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND TANZER

Like Willner, Kitts, and Broder, Tanzer (EX1012) relates to comparing “characteristics” of “a user’s behavior on an electronic device” to “characteristics of a subsequent user” to determine whether “fraud is suspected.” Tanzer, Abstract, [0017] (“capturing user attributes” and comparing to “previously-recorded data”). Like Willner-Kitts-Broder, Tanzer’s techniques operate in “a client-server computing system” where a “customer...accesses [a server’s] web page” and “[e]ach client’s attributes are captured on their local machine and then uploaded to a server” for analysis, using “JavaScript...executed by the user’s Web client browser” to “capture[] the user activity.” Tanzer, [0020]-[0023], [0041].

Tanzer monitors and analyzes the same types of active data as Wilner-Kitts-Broder, including mouse “dither (slight variations in the path when moving from one point to another on the screen).” Tanzer, [0024]-[0025], [0039]. Like Willner, Tanzer analyzes whether “the difference between the historical [movement data] and the current [movement data]” is “so minor as to suggest that a fraud involving copying of behaviors is taking place.” Tanzer, [0033], [0054]. Tanzer also teaches that “[a]ny” additional “attribute or combination of attributes available can...be

examined to determine the suspicion level,” including “IP address,” etc., consistent with Willner-Kitts-Broder’s analysis of both active and passive data. Tanzer, [0035], [0038].

In this context, Tanzer teaches that the client-side “script and applet” should “compress[], optimiz[e] and encrypt[]” the collected “attributes” before “transmission of [the] data” to the server. Tanzer, [0062], [0059].

In the Willner-Kitts-Broder-Tanzer combination, POSAs would therefore have been motivated to transmit the collected data to the server in encrypted form, per Tanzer’s teaching to do so for the same types of data collected and transmitted in the same way for the same type of comparison to previously recorded data. Lopresti-Decl., [0188]-[0191]. POSAs would have reasonably expected success based on Tanzer’s teachings, and because encrypting/decrypting data transmissions were routine activities within POSAs’ ordinary skill.

Willner-Kitts-Broder-Tanzer satisfies claims 4 and 19 (“*decrypt[ing] the received active data and the received passive data*”) and claim 23 (“*decrypt[ing] the received monitored data*”), because the data are encrypted for transmission to the server, which would then *decrypt the received data* to analyze it. Lopresti-Decl., [0192].

VIII. GROUND 3: CLAIMS 9, 15, AND 30 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND MEEK

A. Willner-Kitts-Broder-Meek Combination

Like Willner, Kitts, and Broder, Meek (EX1008) relates to “prevention of fraudulent click-through in an advertising setting” by employing techniques “to ensure that the send item [e.g., web request] originated from a human at a computing device performing human-type actions.” Meek, [0005]. Like Willner, Meek “recognize[s] that a human in sending an item expends...natural efforts that a computer cannot likewise expend, such as...moving a cursor by way of a mouse device, etc, and that by detecting” such active data the system can differentiate humans from bots without “requir[ing] the human to...jump[] through a hoop” like a CAPTCHA. Meek, [0009].

Meek extends upon Willner’s teachings by recognizing that, in addition to mouse movement, “typing on a keyboard” is also suitable active data to detect human effort in differentiating humans from bots. Meek, [0009], [0026], [0035], [0038], [0045].

POSAs would therefore have found it obvious to extend Willner-Kitts-Broder to monitor active data including not only mouse cursor activity as Willner teaches, but also keyboard activity as Meek teaches. Lopresti-Decl., [0194]-[0196]. POSAs would have been motivated by Meek’s above-discussed teachings

that doing so is useful in detecting human effort, in the same click-fraud-prevention context that Willner, Kitts, and Broder relate to. POSAs would have been further motivated by Broder's teachings to "consider a large number of different factors" in developing a "probabilistic" "judgment," including "other additional factors" beyond those mentioned in a single reference, and by Kitts's similar teachings to consider any "other parameters associated with the user or program initiating the request." Broder, [0043], [0057], [0063]; Kitts, [0049], [0068]. POSAs would have reasonably expected success based on Meek's teachings that mouse and keyboard activity can be successfully monitored (e.g., via browser application) and transmitted with a webpage request (e.g., in the advertising context), and because programming software to do so was within POSAs' ordinary skill. Meek, [0005], [0009], [0029], [0037]-[0038], [0043], [0045]. Lopresti-Decl., [0196]-[0197].

B. Mapping to Challenged Claims

- 1. Claim 9: ...analyzing mouse and keyboard activity of the client computer in conjunction with mouse and keyboard activity from human interactions from a prior session with the same website.**

Willner-Kitts-Broder-Meek *analyzes mouse and keyboard activity of the client computer*, as discussed *supra* §VIII.A. POSAs knew, for example, that the click fraud detected by Willner, Kitts, Broder, and Meek often occurs on a webpage that presents advertisements together with search results returned for a

search string that is input via *keyboard activity*. Willner, [0046]; Kitts, [0001], [0041]; EX1022 (“Farahat”), [0003]-[0004]. For example, Willner illustrates an input field 201 for providing a “search term,” which POSAs would have understood was typically input by keyboard:

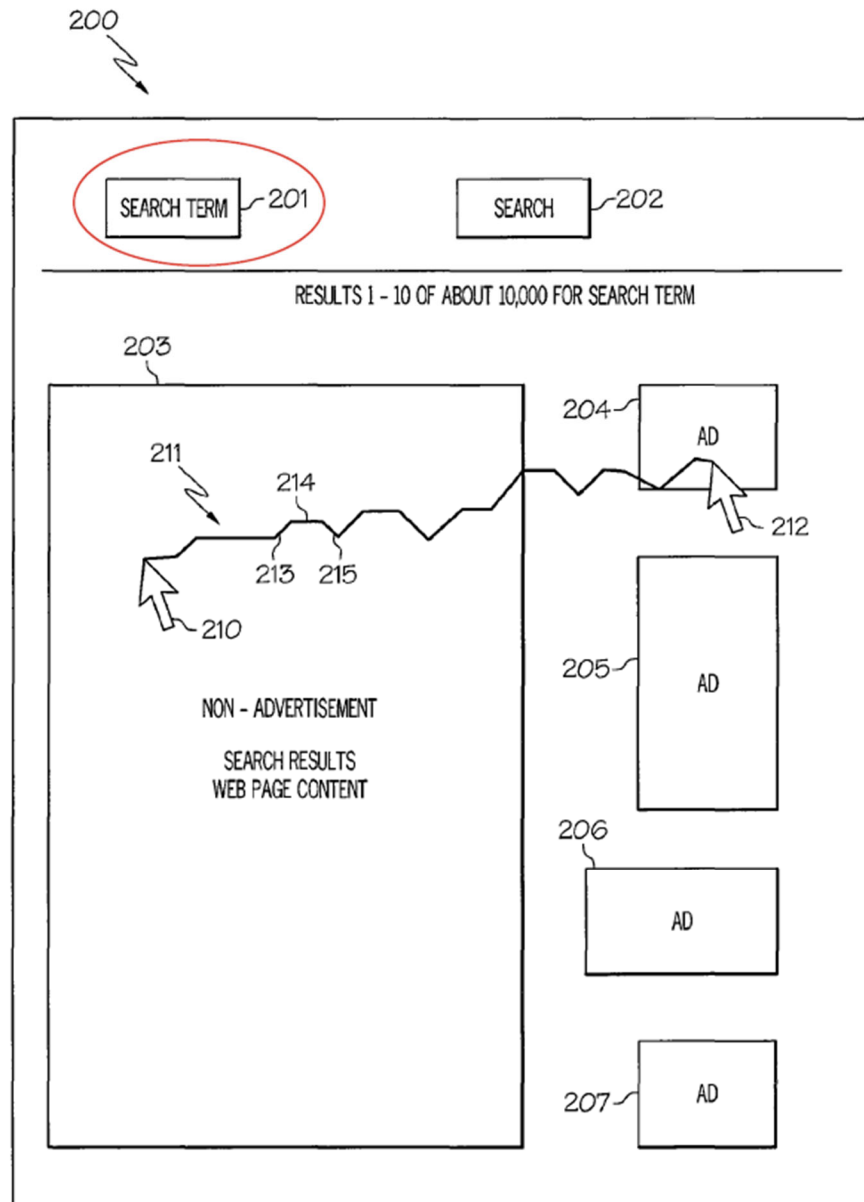


FIG. 2

Willner, FIG. 2 (annotated)

Based on this knowledge and Meek’s teachings, POSAs would have found it obvious to monitor and analyze the client’s *keyboard activity* in entering search terms into the *website*, in addition to monitoring and analyzing the *mouse activity* leading to the client clicking on an advertisement on that *website* as Willner teaches. Lopresti-Decl., [0198]-[0199].

Additionally, Willner teaches to protect against “an automation tool attempting to simulate the actions of a user” by replaying recorded activity patterns that humans produced previously. Willner, [0037]-[0038]. For cursor movements, Willner recognizes that “repeated cursor movements” by true humans “will be different from each other” without “duplication.” Willner, [0037]. Willner therefore protects against replay attacks by bots by comparing “[s]ubsequent” cursor-movement vectors with those “previously stored” from prior movements to detect if they are too “analogous,” thus *analyzing mouse activity of the client computer in conjunction with mouse activity from human interactions from a prior session with the same website* as discussed *supra* §VI.E.1.c ([16C]). Willner, [0038], [0051], [0056].

POSAs knew the same considerations apply to *keyboard activity*, because a “human is not that consistent in typing” and will exhibit “variance among the key space times and key depression times for each letter,” and therefore “[a] computer fraud” replay attack can be detected by “look[ing] for a given variance” between

prior and subsequent keyboard activity typing the same input string. Lopresti-Decl., [0200]-[0201] (quoting corroborating EX1010 (“Kroll”), 8:17-34; EX1012 (“Tanzer”), [0024]. POSAs would therefore have found it obvious, in *analyzing* the *keyboard activity* in Willner-Kitts-Broder-Meek as discussed above, to compare the keyboard activity (e.g., keystroke timings) with previously recorded *keyboard activity from human interactions from a prior session with the same website*, like Willner already does with cursor activity (discussed *supra* §VI.E.1.c ([16C])). Lopresti-Decl., [0201].

- 2. Claim 15: ...the received active data comprises keyboard activity of the client computer on the given page and...the step of analyzing...further includes analyzing the keyboard activity in conjunction with the model data.**

Willner-Kitts-Broder-Meek meets claim 15 for the reasons discussed *supra* §VIII.B.1 (claim 9). POSAs would have understood that the search webpage into which the client inputs a search string via *keyboard activity* can be the same *given page* on which the client clicks an advertisement. Lopresti-Decl., [0202]; *see* Willner, Figure 2 (showing “search term” text field 201 and “ad” click target 204 on same page):

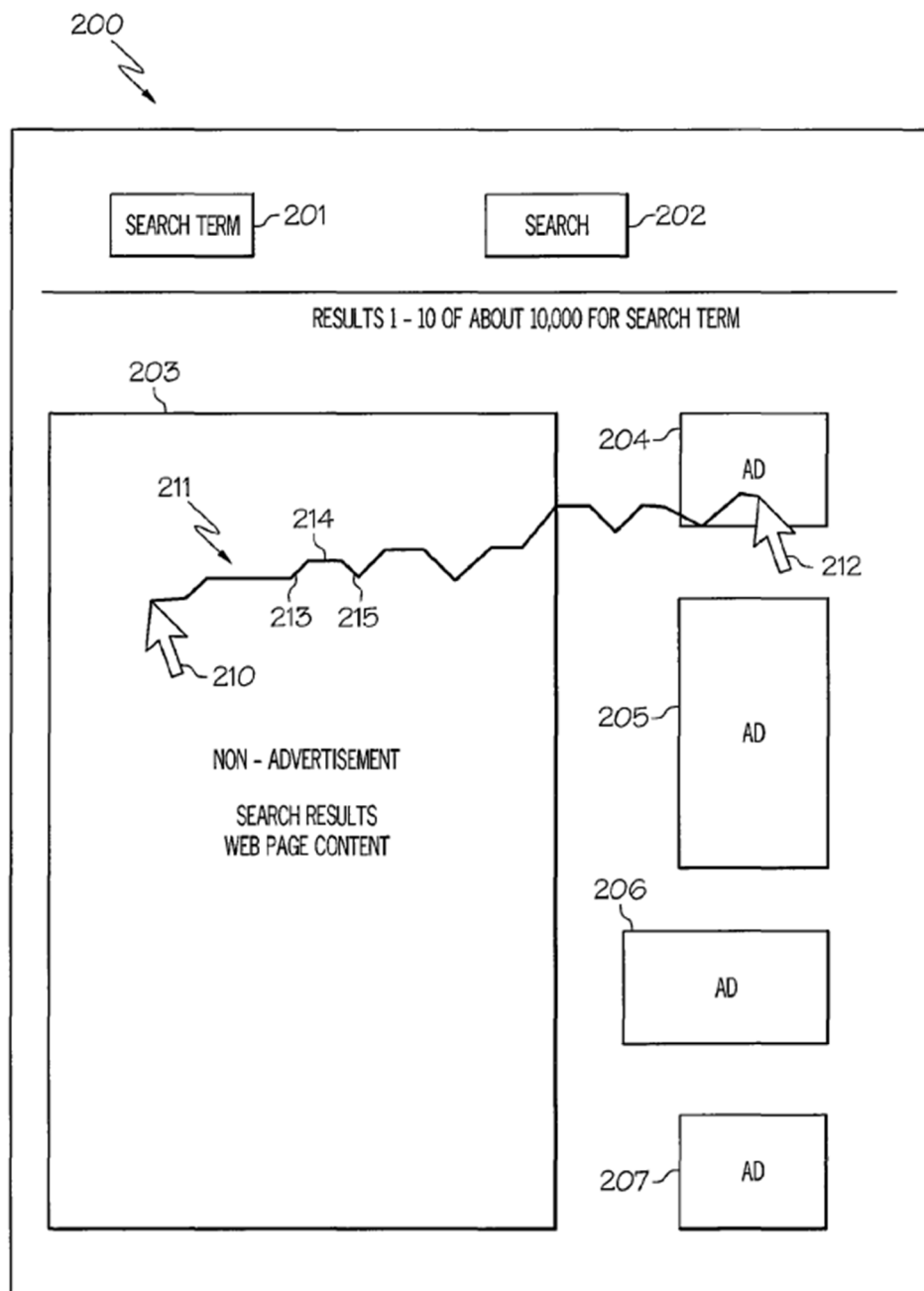


FIG. 2

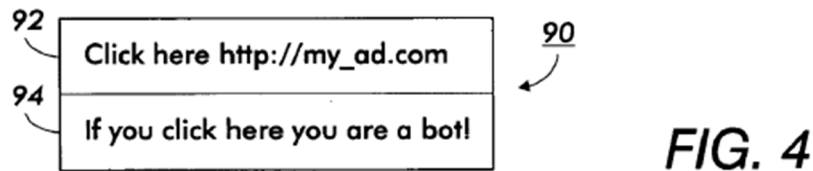
It would have been obvious to compare *keyboard activity* with prior activity from the same page to compare keystroke timings for the same input strings (e.g., same search terms), to detect suspicious duplication. Lopresti-Deci., [0203].

3. Claim 30: ...the manual device input activity comprises mouse movement and key strokes.

See supra §§VIII.A—VIII.B.1.

IX. GROUND 4: CLAIM 13 WOULD HAVE BEEN OBVIOUS OVER WILLNER IN VIEW OF KITTS, BRODER, AND FARAHAT

Like Willner, Kitts, and Broder, Farahat (EX1022) relates to detecting “fraudulent” “automated clicks” on “pay-per-click (PPC)...advertising.” Farahat, [0019], [0014], [0005]. Farahat teaches that one way of “detect[ing] automated agents clicking on sponsored PPC links” is to pair a true clickable advertisement with a dummy ad displaying “images of text” saying to “not click on this image.” Farahat, [0053], FIG. 4:



Farahat explains that an “automated agent may not be able to read text embedded in an image object (i.e., images of text),” whereas humans will see the text and immediately know not to click the dummy ad. Farahat, [0055]-[0056]. Therefore, a client that selects the dummy ad is likely a bot. Farahat, [0057]-[0058]. This is also consistent with Broder’s teachings to present “a variable click location” using “image files” so “a non human entity...would have difficulty in determining where to click on the screen.” Broder, [0034]-[0035], [0046].

POSAs would have been motivated by these teachings to incorporate a dummy ad like Farahat's FIG. 4 into clickable advertisement location(s) on Willner's webpage in Willner-Kitts-Broder, to provide an additional trap for detecting bots, and consistent with Broder's teaching to "consider a large number of different factors" in detection. Broder, [0043], [0063]; Lopresti-Decl., [0206]-[0208]. POSAs would have reasonably expected success based on Farahat's teachings of successfully implementing dummy ads in the same click-fraud-detection context in which Willner, Kitts, and Broder operate, and because it would have required only ordinary programming skill. Lopresti-Decl., [0208].

This Willner-Kitts-Broder-Farahat combination satisfies claim 13 ("*the manual device input activity comprises mouse movement over a CAPTCHA test prompt*"). Willner's techniques monitor *mouse movement* leading to a click, which in the combination can traverse *over* dummy ad 94 on the way to click on either dummy ad 94 or the true ad 92. Because it tells a human that it is testing for bots ("If you click here you are a bot!"), the dummy ad's text is *a CAPTCHA test prompt*. However, humans will immediately know where (not) to click without having to *decipher a CAPTCHA test* (as [1D] recites), because the text is a plain instruction with nothing concealed. Lopresti-Decl., [0209].

X. CONCLUSION

The Board should institute review and cancel claims 1-30.

Dated: 2026-07-29

/Elisabeth Hunt/
Elisabeth Hunt, Reg. #67,336

XI. CLAIM LISTING APPENDIX

Claim 1
[1Pre] A non-transitory machine readable medium having stored thereon instructions for performing a method for generating a value indicative of a likelihood that a human or autonomic computer application is operating a client computer attempting access to a protected page of a website, which when executed by at least one machine, causes the at least one machine to perform operations comprising:
[1A] provide data collection data that causes the client computer to collect active data relating to interactions of the client computer with a given page of the website;
[1B] receive at least some of the collected active data from the client computer and at least some passive data from the client computer;
[1C] perform a first analysis comprising analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data based on human interactions from a prior session with the same website;
[1D] generate a first analysis value based on the first analysis, wherein the client computer is allowed to access the protected page without requiring an operator of the client computer to decipher a CAPTCHA test if the first analysis value meets a first analysis predetermined criteria;
[1E] determine that the first analysis value fails to meet the first analysis predetermined criteria;
[1F] provide a CAPTCHA test to the client computer based on the determination that the first analysis value fails to meet the first analysis predetermined criteria;
[1G] receive a response of the client computer to the CAPTCHA test;
[1H] perform a second analysis comprising assessing accuracy of the response of the client computer to the CAPTCHA test; and
[1I] generate a second analysis value based on the second analysis, wherein the client computer is granted access to the protected page based on the second analysis value meeting a second analysis predetermined criteria.

Claim 2
[2Pre] The non-transitory machine readable medium of claim 1, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to:
[2A] provide an additional CAPTCHA test to the client computer based on the determination that the second analysis value fails to meet the second analysis predetermined criteria;
[2B] receive a response of the client computer to the additional CAPTCHA test;
[2C] perform a third analysis comprising assessing the accuracy of the client computer's response to the additional CAPTCHA test; and
[2D] generate a third analysis value based on the third analysis, wherein the client computer is granted access to the protected page based on the third analysis value meeting a third analysis predetermined criteria.
Claim 3
The non-transitory machine readable medium of claim 1, wherein when the first analysis value meets a first analysis predetermined criteria, the client computer is not presented with a CAPTCHA test prior to the client computer being granted access to the protected page.
Claim 4
The non-transitory machine readable medium of claim 1, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to decrypt the received active data and the received passive data.
Claim 5
The non-transitory machine readable medium of claim 1, wherein the model data is based on human interaction from a prior session with the same given page.
Claim 6
The non-transitory machine readable medium of claim 1, wherein the ability of the client computer to collect active data is only active while the client computer is visiting a web page enabled with data collection data.

Claim 7

The non-transitory machine readable medium of claim 1, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to receive the first or second analysis predetermined criteria from an operator or administrator of the website.

Claim 8

The non-transitory machine readable medium of claim 1, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to receive from an operator or administrator of the website a number of CAPTCHA tests that will be provided to a client computer after the second analysis value fails to meet the second analysis predetermined criteria.

Claim 9

The non-transitory machine readable medium of claim 1, wherein the step of analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data further comprises analyzing mouse and keyboard activity of the client computer in conjunction with mouse and keyboard activity from human interactions from a prior session with the same website.

Claim 10

The non-transitory machine readable medium of claim 1, wherein the data collection data comprises JavaScript code that causes a browser of the client computer to collect the active data.

Claim 11

The non-transitory machine readable medium of claim 10, wherein the received passive data comprises at least one browser cookie and at least one Internet Protocol (IP) address associated with the client computer, and wherein the step of analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data further includes analyzing the at least one browser cookie and the at least one IP address in conjunction with the model data.

Claim 12
The non-transitory machine readable medium of claim 11, wherein the step of analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data includes analyzing manual device input activity of the client computer in conjunction with the model data based on human interaction with the same given page.
Claim 13
The non-transitory machine readable medium of claim 12, wherein the manual device input activity comprises mouse movement over a CAPTCHA test prompt.
Claim 14
The non-transitory machine readable medium of claim 12, wherein the human interaction from a prior session with the same website includes human interaction of another client computer from the prior session with the same given page.
Claim 15
The non-transitory machine readable medium of claim 14, wherein the received active data comprises keyboard activity of the client computer on the given page and wherein the step of analyzing at least some of the received active data and at least some of the received passive data in conjunction with model data further includes analyzing the keyboard activity in conjunction with the model data.
Claim 16
[16Pre] A non-transitory machine readable medium having stored thereon instructions for performing a method for providing a value indicating a judgment of whether a human or an autonomic computer application operating a client computer is interacting with a server, which when executed by at least one machine, causes the at least one machine to perform operations comprising:
[16A] provide data collection data requesting active and passive data of the client computer;
[16B] receive active and passive data responsive to the data collection data, the received active data relating to interactions of the client computer with a website of the server;

[16C] analyze the received active data and the received passive data for indication of a human or an autonomic computer application operating the client computer, wherein the analyzing includes analyzing the received active data and the received passive data in conjunction with model data based on human interactions from a prior session with the same website and developing a first analysis value;

[16D] determine that the first analysis value fails to meet a first analysis predetermined criteria; and

[16E] provide a request for further data from the client computer based on the determination that the first analysis value fails to meet the first analysis predetermined criteria.

Claim 17

The non-transitory machine readable medium of claim 16, wherein the first analysis value failing to meet the first analysis predetermined criteria indicates that the client computer should not be allowed access to a protected page of the website.

Claim 18

The non-transitory machine readable medium of claim 16, wherein the received active data includes manual input device activity and the received passive data includes at least one browser cookie and at least one IP address, and the analyzing includes analyzing the at least one browser cookie, the at least one IP address, and the manual input device activity in conjunction with model data based on human interactions from a prior session with the same website.

Claim 19

The non-transitory machine readable medium of claim 16, further comprising instructions, when executed by the at least one machine to decrypt the received active data and the received passive data.

Claim 20
[20Pre] The non-transitory machine readable medium of claim 16, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to:
[20A] receive further data from the client computer in response to the request for further data;
[20B] perform a second level of analyzing on the received further data; and
[20C] provide a second analysis value based on the second level of analyzing.
Claim 21
The non-transitory machine readable medium of claim 20, wherein the received further data includes the response of the client computer to a CAPTCHA test provided to the client computer.
Claim 22
[22Pre] A non-transitory machine readable medium having stored thereon instructions for performing a method for providing a value indicating a judgment of whether a human or an autonomic computer application operating a client computer is interacting with a server, which when executed by the at least one machine, causes the at least one machine to perform operations comprising:
[22A] provide instructions that allow client computer interactions with a website of the server to be remotely monitored;
[22B] receive monitored data originating with the client computer, the monitored data comprising active data relating to interactions of the client computer with the website and passive data of the client computer;
[22C] analyze the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including:
[22D] perform a first level of analyzing on the received monitored data for any indication that a human may be operating the client computer to obtain a first-level analysis;
[22E] perform a second level of analyzing to obtain a second-level analysis, when the first-level analysis does not meet a first-level analysis predetermined criteria, the second level of analyzing comprising analyzing the received monitored data in conjunction with previously recorded data relating to human interactions from a prior session with the same website; and

[22F] provide a second-level analysis value when the second-level analysis meets a second-level analysis predetermined criteria.
Claim 23
The non-transitory machine readable medium of claim 22, further comprising instructions, when executed by the at least one machine, that cause the at least one machine to decrypt the received monitored data.
Claim 24
The non-transitory machine readable medium of claim 22, wherein the monitored data comprises active data relating to interactions of the client computer with a given page of the website and passive data of the client computer, and the recorded data relates to human interaction from a prior session with the same given page.
Claim 25
The non-transitory machine readable medium of claim 22, the analyzing further comprising instructions, when executed by the at least one machine, that cause the at least one machine to: provide a request for further data from the client computer based on the determination that the second-level analysis does not meet the second level analysis predetermined criteria.
Claim 26
[26Pre] The non-transitory machine readable medium of claim 25, the analyzing further comprising instructions, when executed by the at least one machine, that cause the at least one machine to:
[26A] receive further data from the client computer in response to the request for further data;
[26B] perform a third-level of analyzing on the received further data; and
[26C] provide a third-level analysis value after completion of the third-level of analyzing.
Claim 27
The non-transitory machine readable medium of claim 26, wherein the request for further data includes a CAPTCHA test.
Claim 28
The non-transitory machine readable medium of claim 22, wherein the received monitored data includes at least one browser cookie and at least one IP address.

Claim 29

The non-transitory machine readable medium of claim 28, wherein the received monitored data includes manual device input activity.

Claim 30

The non-transitory machine readable medium of claim 29, wherein the manual device input activity comprises mouse movement and key strokes.

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

I certify that on July 29, 2026, a copy of the foregoing document, including any exhibits or appendices filed therewith, is being served via Overnight FedEx at the following correspondence address of record for the patent:

K-T Legal, PLLC
315 W. Riverside Ave. Ste 603
Spokane, WA 99201

Date: July 29, 2026

/Dara Del Rosario/
Dara Del Rosario
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 13,999 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: July 29, 2026

/Dara Del Rosario/
Dara Del Rosario
Paralegal
WOLF, GREENFIELD & SACKS, P.C.