

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

DECLARATION OF DANIEL P. LOPRESTI, PH.D.

Google Exhibit 1003 Google v. Nobots

CONDENSED TABLE OF CONTENTS

I.	PERSONAL AND PROFESSIONAL BACKGROUND	2
II.	MATERIALS REVIEWED AND CONSIDERED	10
III.	MY UNDERSTANDING OF PATENT LAW	11
	A. Anticipation	13
	B. Obviousness.....	14
IV.	PERSON OF ORDINARY SKILL IN THE ART (“POSA”).....	16
V.	THE ’014 PATENT	19
	A. Described Embodiments.....	19
	B. Prosecution History of the ’014 Patent.....	21
VI.	CLAIM INTERPRETATION	24
	A. “active data”	25
	B. “passive data”	27
VII.	PRIOR-ART REFERENCES	28
	A. Willner (EX1005).....	28
	B. Kitts (EX1009)	29
	C. Broder (EX1011)	30
	D. Tanzer (EX1012).....	30
	E. Meek (EX1008)	31
	F. Farahat (EX1022)	32
VIII.	THE ’014 PATENT’S CLAIMS WOULD HAVE BEEN OBVIOUS OVER THE PRIOR ART	32
	A. Ground 1: Claims 1-8, 10-12, 14, and 16-29 of the ’014 Patent Would Have Been Obvious over Willner in View of Kitts and Broder	33
	1. Discussion of Willner (EX1005).....	33
	2. Discussion of Kitts (EX1009)	40
	3. Discussion of Broder (EX1011).....	41
	4. Discussion of Willner-Kitts-Broder Combination	42

5. Mapping of Willner-Kitts-Broder Combination to Claims 1-8, 10-12, 14, and 16-29 of the '014 Patent.....	50
B. Ground 2: Claims 4, 19, and 23 of the '014 Patent Would Have Been Obvious over Willner in view of Kitts, Broder, and Tanzer.....	104
1. Discussion of Tanzer (EX1012).....	104
2. Discussion of Willner-Kitts-Broder-Tanzer Combination.....	106
3. Mapping of Willner-Kitts-Broder-Tanzer Combination to Claims 4, 19, and 23 of the '014 Patent	107
C. Ground 3: Claims 9, 15, and 30 of the '014 Patent Would Have Been Obvious over Willner in View of Kitts, Broder, and Meek.....	107
1. Discussion of Meek (EX1008).....	108
2. Discussion of Willner-Kitts-Broder-Meek Combination.....	109
3. Mapping of Willner-Kitts-Broder-Meek Combination to Claims 9, 15, and 30 of the '014 Patent.....	111
D. Ground 4: Claim 13 Would Have Been Obvious over Willner in View of Kitts, Broder, and Farahat	116
1. Discussion of Farahat (EX1022).....	117
2. Discussion of Willner-Kitts-Broder-Farahat Combination.....	118
3. Mapping of Willner-Kitts-Broder-Farahat Combination to Claim 13 of the '014 Patent.....	118
IX. CLAIM LISTING APPENDIX	121

FULL TABLE OF CONTENTS

I.	PERSONAL AND PROFESSIONAL BACKGROUND	2
II.	MATERIALS REVIEWED AND CONSIDERED	10
III.	MY UNDERSTANDING OF PATENT LAW	11
	A. Anticipation	13
	B. Obviousness.....	14
IV.	PERSON OF ORDINARY SKILL IN THE ART (“POSA”).....	16
V.	THE ’014 PATENT	19
	A. Described Embodiments.....	19
	B. Prosecution History of the ’014 Patent.....	21
VI.	CLAIM INTERPRETATION	24
	A. “active data”	25
	B. “passive data”	27
VII.	PRIOR-ART REFERENCES	28
	A. Willner (EX1005).....	28
	B. Kitts (EX1009)	29
	C. Broder (EX1011).....	30
	D. Tanzer (EX1012).....	30
	E. Meek (EX1008).....	31
	F. Farahat (EX1022).....	32
VIII.	THE ’014 PATENT’S CLAIMS WOULD HAVE BEEN OBVIOUS OVER THE PRIOR ART	32
	A. Ground 1: Claims 1-8, 10-12, 14, and 16-29 of the ’014 Patent Would Have Been Obvious over Willner in View of Kitts and Broder	33
	1. Discussion of Willner (EX1005).....	33
	2. Discussion of Kitts (EX1009)	40
	3. Discussion of Broder (EX1011).....	41
	4. Discussion of Willner-Kitts-Broder Combination	42

a.	Passive Data	43
b.	Further Testing, Including CAPTCHA.....	45
5.	Mapping of Willner-Kitts-Broder Combination to Claims 1-8, 10-12, 14, and 16-29 of the '014 Patent.....	50
a.	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:	51
i.	[16A] provide data collection data requesting active and passive data of the client computer;.....	54
ii.	[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;	59
iii.	[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;.....	60
iv.	[16D] determine that the first analysis value fails to meet a first analysis predetermined criteria; and	65
v.	[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.	66
b.	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.....	68

- c. 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. 70
- d. 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. 71
- e. 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: 72
 - i. [20A] receive further data from the client computer in response to the request for further data; 72
 - ii. [20B] perform a second level of analyzing on the received further data; and 73
 - iii. [20C] provide a second analysis value based on the second level of analyzing.....73
- f. 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. 73
- g. 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: 74
 - i. [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;	75
ii.	[1B] receive at least some of the collected active data from the client computer and at least some passive data from the client computer;	76
iii.	[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;	77
iv.	[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;	77
v.	[1E] determine that the first analysis value fails to meet the first analysis predetermined criteria;	78
vi.	[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;	78
vii.	[1G] receive a response of the client computer to the CAPTCHA test;	79
viii.	[1H] perform a second analysis comprising assessing accuracy of the response of the client computer to the CAPTCHA test; and	79
ix.	[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.	80
h.	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:	82

i.	[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;	82
ii.	[2B] receive a response of the client computer to the additional CAPTCHA test;	85
iii.	[2C] perform a third analysis comprising assessing the accuracy of the client computer's response to the additional CAPTCHA test; and	85
iv.	[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.	86
i.	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.....	86
j.	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.....	87
k.	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.....	87
l.	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.	87
m.	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.....	88

- n. 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. 90
- o. 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.....93
- p. 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. 93
- q. 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.....94
- r. 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. 94
- s. 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:	95
i. [22A] provide instructions that allow client computer interactions with a website of the server to be remotely monitored;.....	95
ii. [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;	95
iii. [22C] analyze the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including:.....	97
iv. [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;	97
v. [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	99
vi. [22F] provide a second-level analysis value when the second-level analysis meets a second-level analysis predetermined criteria.	100
t. 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.	101
u. 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.....	101
v. 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.	102
w. 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:	102
i. [26A] receive further data from the client computer in response to the request for further data;	102
ii. [26B] perform a third-level of analyzing on the received further data; and	102
iii. [26C] provide a third-level analysis value after completion of the third-level of analyzing.	103
x. Claim 27: The non-transitory machine readable medium of claim 26, wherein the request for further data includes a CAPTCHA test.	103
y. 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.	103
z. Claim 29: The non-transitory machine readable medium of claim 28, wherein the received monitored data includes manual device input activity.	103
B. Ground 2: Claims 4, 19, and 23 of the '014 Patent Would Have Been Obvious over Willner in view of Kitts, Broder, and Tanzer.....	104
1. Discussion of Tanzer (EX1012).....	104
2. Discussion of Willner-Kitts-Broder-Tanzer Combination.....	106
3. Mapping of Willner-Kitts-Broder-Tanzer Combination to Claims 4, 19, and 23 of the '014 Patent	107

C. Ground 3: Claims 9, 15, and 30 of the '014 Patent Would Have Been Obvious over Willner in View of Kitts, Broder, and Meek.....	107
1. Discussion of Meek (EX1008).....	108
2. Discussion of Willner-Kitts-Broder-Meek Combination.....	109
3. Mapping of Willner-Kitts-Broder-Meek Combination to Claims 9, 15, and 30 of the '014 Patent.....	111
a. 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.	111
b. 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.	114
c. Claim 30: The non-transitory machine readable medium of claim 29, wherein the manual device input activity comprises mouse movement and key strokes.	116
D. Ground 4: Claim 13 Would Have Been Obvious over Willner in View of Kitts, Broder, and Farahat	116
1. Discussion of Farahat (EX1022).....	117
2. Discussion of Willner-Kitts-Broder-Farahat Combination.....	118
3. Mapping of Willner-Kitts-Broder-Farahat Combination to Claim 13 of the '014 Patent.....	118
IX. CLAIM LISTING APPENDIX	121

I, Daniel P. Lopresti, declare:

[0001] I have been retained by Wolf, Greenfield & Sacks, P.C., counsel for Petitioner Google LLC, to assess all claims 1-30 of U.S. Patent No. 11,810,014 (“the ’014 patent”). I am being compensated for my time at my standard rate of \$500.00 per hour, plus actual expenses. My compensation is not dependent in any way upon any outcome in the above-captioned proceeding concerning the ’014 patent.

[0002] I previously provided declaration testimony in two *inter partes* reviews filed by the same Petitioner concerning patents that are related to and share the same specification as the ’014 patent: IPR2022-00940 concerning U.S. Patent No. 9,595,008 (“the ’008 patent”) and IPR2022-00941 concerning U.S. Patent No. 10,423,885 (“the ’885 patent”). I have been informed that the PTAB held all claims of the ’885 patent unpatentable in IPR2022-00941, and held claims 1-17 and 20 of the ’008 patent unpatentable in IPR2022-00940. I have been informed that Petitioner appealed to the U.S. Court of Appeals for the Federal Circuit concerning claim 19 of the ’008 patent, and that claim was held unpatentable in that appeal. I have been informed that dependent claim 18 of the ’008 patent was not held unpatentable.

I. PERSONAL AND PROFESSIONAL BACKGROUND

[0003] My qualifications for forming the opinions set forth in this declaration are summarized below and explained in more detail in my current curriculum vitae, provided as Exhibit 1004. Exhibit 1004 also includes a list of my publications and patents.

[0004] I am a Full Professor in the Department of Computer Science & Engineering (“CSE”) at Lehigh University in Bethlehem, PA, and have been since May 2009. From July 2009 through June 2019, I also served as Chair of the CSE Department, except for a period from July 2014 to June 2015 when I served as the interim Dean of Engineering and another person served as interim Chair of the CSE Department. In July 2015, I was named Director of the Lehigh Data X strategic initiative focused on interdisciplinary data science, a role I held until June 2020. From 2003 to 2009, I was an Associate Professor in the CSE Department. The courses that I have taught at Lehigh include big data analytics, artificial intelligence theory and practice, AI for social good, software product management, issues in cybersecurity, data mining, research methods, and operating system design. My research areas include computer security, biometric security, pattern and optical character recognition, document image analysis, machine learning, and electronic voting systems.

[0005] From December 2002 to June 2003, I held a courtesy appointment as a Visiting Research Scientist at the Palo Alto Research Center, and from February 2003 to June 2003 I also held courtesy appointments as a Research Fellow in the Information Security Institute at Johns Hopkins University, and as a Visiting Research Associate Professor at Rensselaer Polytechnic Institute.

[0006] From October 1997 to December 2002, I was a Member of Technical Staff at Bell Labs/Lucent Technologies, conducting research in the areas of computer security, document image analysis, optical character recognition, and pen computing, and where I also collaborated with colleagues on the development of text-to-speech (“TTS”) technologies. I also worked on audio Completely Automated Public Turing Tests to Tell Computers and Humans Apart (“CAPTCHA”), speech biometrics, and handwriting biometrics.

[0007] From June 1991 to October 1997, I was a Principal Scientist at the Matsushita Information Technology Laboratory in Princeton, NJ, conducting research in the areas of optical character recognition, pen computing, document analysis, and document processing systems.

[0008] From September 1986 to May 1991, I was an Assistant Professor of Computer Science at Brown University in Providence, RI, conducting research in parallel computing and computer-aided design of VLSI. The courses that I taught

at Brown included VLSI design, parallel computer architecture, discrete math, and computational molecular biology.

[0009] From 2009 through 2013, I served as Chair of Technical Committee 11 of the International Association for Pattern Recognition (“IAPR”). Technical Committee 11 is known as the “Reading Systems” committee and its goal is to understand and develop systems that can analyze media containing character symbols and return an encoded representation of the text content and structure. From 2018 through 2021, I served as Treasurer of IAPR, and in 2021 I was elected President of IAPR, a role that I held through 2022. I then served for two more years as IAPR Past President. I served as a member of the IAPR Executive Committee from 2018 through 2024, and now serve as a member of the IAPR Advisory Committee.

[0010] From 2015 through 2025, I served as an appointed member on the Council for the Computing Community Consortium (“CCC”) of the Computing Research Association (“CRA”). I assumed the role of CCC Council Vice Chair effective July 2020, and served as CCC Council Chair from July 2022 through July 2024, and then as CCC Council Chair Emeritus until July 2025. The role of the CCC is to catalyze the United States computing research community to pursue high-impact research, conduct activities that strengthen the research community, articulate compelling research visions, and align those visions with key national

and global challenges. While on the CCC Council, I served on, and also co-chaired, the Cybersecurity and Cybercrime Task Force. I also served on the Security, Integrity, and Trust Task Force, in addition to other CCC Task Forces. Over the years of my service on CCC, working with other leading researchers in the field, I co-authored numerous whitepapers and responses to requests for information (RFIs) from US government agencies on topics relating to computer security.

[0011] Between 2014 and 2026, I served as an Editor-in-Chief of the International Journal of Document Analysis and Recognition which is a scholarly journal published by Springer-Nature and generally concerns all areas related to document analysis and recognition. This includes research dealing with computer recognition of characters, symbols, text, lines, graphics, images, handwriting, signatures, as well as automatic analyses of the overall physical and logical structures of documents, with the ultimate objective of a high-level understanding of their semantic content. Over a period of more than 20 years, I have served as a technical program co-chair for many of the major international conferences in the fields of document analysis, including the latest upcoming International Conference on Document Analysis and Recognition which will be held in Vienna, Austria in August-September 2026.

[0012] In May 2005, I co-chaired and organized the Second International Workshop on Human Interactive Proofs (“HIPs”) at Lehigh University. This workshop brought together top researchers in the area, with proceedings that were published by Springer. HIPs are a similar, overlapping concept to CAPTCHAs. Both HIPs and CAPTCHAs deal with completely automated systems and methods to determine whether an entity interacting with a computing device is in fact human, or is instead a computer. This concept is also sometimes called a “Reverse Turing Test.” The May 2005 workshop was one of very few conferences focused specifically on HIPs, CAPTCHAs, and related concepts. More generally, these concepts concern a particular problem in computer security that was becoming more prevalent with the wider spread of the Internet in the 2000s: how to tell whether a computing device that is interacting with another device (e.g., a server) is being operated by a human or instead by an automated program (a.k.a. “bot”).

[0013] I received a B.A. in Mathematics and Engineering Science from Dartmouth College in 1982, an M.S.E. in Electrical Engineering and Computer Science from Princeton University in 1983, an M.A. in Electrical Engineering and Computer Science from Princeton University in 1984, and a Ph.D. in Computer Science from Princeton University in 1987.

[0014] My areas of expertise encompass the fields of computer security and authentication, access control, biometric security, document image analysis

techniques, optical character recognition technology, other artificial intelligence techniques (*e.g.*, machine learning), and electronic voting systems.

[0015] I have authored or co-authored over 180 publications in peer-reviewed conferences and journals. I am also a named inventor on 24 United States patents, many of which are related to or in the field of document image analysis, and several of which cover audio CAPTCHA technology and pen computing.

[0016] I have authored or co-authored many publications involving computer security, biometric security, and related concepts. While they are fully set forth in my CV, some examples include “Evaluating Biometric Security: Understanding the Impact of Wolves in Sheep’s Clothing,” D. Lopresti, F. Monroe, and L. Ballard, *Proceedings of the First Korea-Japan Joint Workshop on Pattern Recognition*, November 2006, Jeju, Korea, pp. 15-24 (invited keynote paper); “Forgery Quality and its Implications for Behavioral Biometric Security,” L. Ballard, D. Lopresti, and F. Monroe, *IEEE Transactions on Systems, Man and Cybernetics*, Part B, vol. 37, no. 5, October 2007, pp. 1107-1118; “On the Usability and Security of Pseudo-Signatures,” J. Chen and D. Lopresti, *Proceedings of Document Recognition and Retrieval XVII (IS&T/SPIE International Symposium on Electronic Imaging)*, January 2010, San Jose, CA, pp.

7534-08.01 - 7534-08.10; and “Human/Machine Differentiation,” H. Baird and D. Lopresti, *2005 McGraw-Hill Yearbook of Science and Technology*, pp. 144-147.

[0017] I have also authored or co-authored several publications involving computer security, access control, CAPTCHAs, HIPs, Reverse Turing Tests, and related concepts. These publications include “Leveraging the CAPTCHA Problem,” D. Lopresti, *Proceedings of the Second International Workshop on Human Interactive Proofs*, May 2005, Bethlehem, PA, pp. 97-110; “A Reverse Turing Test Using Speech,” G. Kochanski, D. Lopresti, and C. Shih, *Proceedings of the Seventh International Conference on Spoken Language Processing*, September 2002, Denver, CO, pp.1357-1360; *Human Interactive Proofs*, Lecture Notes in Computer Science Vol. 3517, H. Baird and D. Lopresti (editors), Springer-Verlag, May 2005; and “Human Interactive Proofs for Spoken Language Interfaces,” D. Lopresti, C. Shih and G. Kochanski, *Proceedings of the Workshop on Human Interactive Proofs*, January 2002, Palo Alto, CA, pp. 30-34.

[0018] I have also received grants to do research on computer and biometric security, authentication, access control, and CAPTCHAs: “Using Generative Models to Evaluate and Strengthen Biometrically Enhanced Systems,” Co-Principal Investigator (with F. Monroe and M. Reiter), NSF, \$287,950, 2004 – 2008; and “Implicit and Multi-Modal CAPTCHAs,” Co-Principal Investigator (with H. Baird), Avaya Labs Research, \$30,000, 2005 – 2006.

[0019] I have also taught many courses that covered the basic technical concepts underlying computer security, biometric security, authentication, access control, CAPTCHAs, HIPs, Reverse Turing Tests, and related concepts, at both the undergraduate and graduate level, over the course of the past two decades.

[0020] I have also been a member of the Institute of Electrical and Electronics Engineers (“IEEE”) since 1982. I became an IEEE Senior Member in 2003, and was named an IEEE Life Member in 2024. During my career, I have authored or co-authored approximately 17 refereed papers or proceedings that were published in IEEE technical publications.

[0021] I have also been active in other IEEE activities. For example, I served as program co-chair for the Eleventh International Conference on Document Analysis and Recognition in 2011, whose proceedings were published on the IEEE Explore website. I have received two awards from IEEE organizations. I was an Associate Editor of *IEEE Transactions on Pattern Analysis and Machine Intelligence* between 2005 and 2010. I have been a member of conference program committees for several IEEE conferences, I have served as an invited reviewer for a number of different IEEE journals and several IEEE conferences, all as listed in my CV.

[0022] I am also a member of several other technical associations, and have conducted various activities for them, attended their conferences, and published

papers and proceedings in their technical publications. These include the Association for Computing Machinery (“ACM”), the International Association for Pattern Recognition (“IAPR”), and the Association for the Advancement of Artificial Intelligence (“AAAI”).

II. MATERIALS REVIEWED AND CONSIDERED

[0023] My findings, as explained below, are based on my years of education, research, experience, and background in the field of computer security, as well as my investigation and study of relevant materials for this declaration. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth in Section IV below. In forming my opinions, I have studied and considered the materials identified in the list below.

Exhibit	Description
1001	U.S. Patent No. 11,810,014 (“the ’014 patent”)
1002	Prosecution History of U.S. Patent No. 11,810,014
1005	U.S. Patent Application Publication No. 2009/0024971 (“Willner”)
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”)

Exhibit	Description
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”)

III. MY UNDERSTANDING OF PATENT LAW

[0024] In developing my opinions, I discussed various relevant legal principles with Petitioner’s attorneys. Though I do not purport to have prior knowledge of such principles, I understood them when they were explained to me and have relied upon such legal principles, as explained to me, in the course of forming the opinions set forth in this declaration. My understanding in this respect is as follows:

[0025] I understand that “*inter partes* review” (IPR) is a proceeding before the United States Patent & Trademark Office for evaluating the patentability of an issued patent’s claims based on prior-art patents and printed publications.

[0026] I understand that, in this proceeding, Petitioner has the burden of proving that the challenged claims of the ’014 patent are unpatentable by a

preponderance of the evidence. I understand that “preponderance of the evidence” means that a fact or conclusion is more likely true than not true.

[0027] I understand that, in IPR proceedings, claim terms in a patent are given their ordinary and customary meaning as understood by a person of ordinary skill in the art (“POSA”) in the context of the entire patent and the prosecution history pertaining to the patent. If the specification provides a special definition for a claim term that differs from the meaning the term would otherwise possess, the specification’s special definition controls. If a claim element is expressed as a “means” for performing a specified function, I understand that it covers the corresponding structure described in the specification and equivalents of the described structure. I have applied these standards in preparing the opinions in this declaration.

[0028] I understand that determining whether a particular patent or printed publication constitutes prior art to a challenged patent claim can require determining the effective filing date (also known as the priority date) to which the challenged claim is entitled. I understand that for a patent claim to be entitled to the benefit of the filing date of an earlier application to which the patent claims priority, the earlier application must have described the claimed invention in sufficient detail to convey with reasonable clarity to the POSA that the inventor had possession of the claimed invention as of the earlier application’s filing date. I

understand that a disclosure that merely renders the claimed invention obvious is not sufficient written description for the claim to be entitled to the benefit of the filing date of the application containing that disclosure.

[0029] I understand that for an invention claimed in a patent to be patentable, it must be, among other things, new (novel—*i.e.*, not anticipated) and not obvious from the prior art. My understanding of these two legal standards is set forth below.

A. Anticipation

[0030] I understand that, for a patent claim to be “anticipated” by the prior art (and therefore not novel), each and every limitation of the claim must be found, expressly or inherently, in a single prior-art reference. I understand that a claim limitation is disclosed for the purpose of anticipation if a POSA would have understood the reference to disclose the limitation based on inferences that a POSA would reasonably be expected to draw from the explicit teachings in the reference when read in light of the POSA’s knowledge and experience.

[0031] I understand that a claim limitation is inherent in a prior art reference if that limitation is necessarily present when practicing the teachings of the reference, regardless of whether a person of ordinary skill recognized the presence of that limitation in the prior art.

B. Obviousness

[0032] I understand that a patent claim may be unpatentable if it would have been obvious in view of a single prior-art reference or a combination of prior-art references.

[0033] I understand that a patent claim is obvious if the differences between the subject matter of the claim and the prior art are such that the subject matter as a whole would have been obvious to a person of ordinary skill in the relevant field at the time the invention was made. Specifically, I understand that the obviousness question involves a consideration of:

- the scope and content of the prior art;
- the differences between the prior art and the claims at issue;
- the knowledge of a person of ordinary skill in the pertinent art; and
- if present, objective factors indicative of non-obviousness, sometimes referred to as “secondary considerations.” To my knowledge, the Patent Owner has not asserted any such secondary considerations with respect to the ’014 patent.

[0034] I understand that in order for a claimed invention to be considered obvious, a POSA must have had a reason for combining teachings from multiple prior-art references (or for modifying a single prior-art reference or

implementing its teachings in a given manner, in the case of obviousness in view of a single reference) in the fashion proposed.

[0035] I further understand that in determining whether a prior-art reference would have been combined with other prior art or with other information within the knowledge of a POSA, the following are examples of approaches and rationales that may be considered:

- combining prior-art elements according to known methods to yield predictable results;
- simple substitution of one known element for another to obtain predictable results;
- use of a known technique to improve similar devices in the same way;
- applying a known technique to a known device ready for improvement to yield predictable results;
- applying a technique or approach that would have been “obvious to try,” i.e., choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.
- known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;

- some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference, to implement it in a given way, or to combine prior-art reference teachings to arrive at the claimed invention. I understand that this teaching, suggestion or motivation may come from a prior-art reference or from the knowledge or common sense of one of ordinary skill in the art.

[0036] I understand that for a single reference or a combination of references to render the claimed invention obvious, a POSA must have been able to arrive at the claimed invention by modifying, implementing, and/or combining the teachings of the applied references.

IV. PERSON OF ORDINARY SKILL IN THE ART (“POSA”)

[0037] I have been informed and understand that for purposes of assessing whether prior-art references disclose every element of a patent claim (thus “anticipating” the claim) and/or would have rendered the claim obvious, the patent and the prior-art references must be assessed from the perspective of a person having ordinary skill in the art (“POSA”) to which the patent is related, based on the understanding of that person at the time of the patent claim’s priority date. I have been informed and understand that a POSA is presumed to be aware

of all pertinent prior art and the conventional wisdom in the art, and is a person of ordinary creativity. I have applied this standard throughout my declaration.

[0038] The '014 patent involves technology in the field of computer security or cybersecurity in general, and in more specific embodiments detecting automated systems (“bots”) attempting to access services that may be intended for human users. I have been asked to provide my opinions as to the state of the art in these areas by 2007. I use this timeframe because the face of the '014 patent indicates an earliest claimed priority date of November 19, 2007. Whenever I offer an opinion in this declaration about the knowledge of a POSA, the manner in which a POSA would have understood the claims of the '014 patent or its description, the manner in which a POSA would have understood the prior art, or what a POSA would have been led to do based on the prior art, I am referencing the 2007 timeframe, even if I do not say so specifically in each case.

Demonstrating that the '014 patent's claims were anticipated or would have been obvious in 2007 demonstrates that they remained so any time after 2007 (including as of the November 19, 2008, filing date of the '014 patent's first non-provisional parent; the March 13, 2017, filing date of the '014 patent's second non-provisional parent; the September 23, 2019, filing date of the '014 patent's third non-provisional parent; and the August 5, 2022 filing date of the application that issued as the '014 patent), because the POSA's knowledge only increases over time.

[0039] I understand that the Patent Owner may attempt to prove that the alleged invention recited in the challenged claims was conceived at some time prior to the earliest claimed priority date on the face of the patent. At the time of this declaration, I am unaware of any evidence produced by the Patent Owner to establish any earlier conception date.

[0040] In my opinion, a person of ordinary skill in the art in the 2007 timeframe (“POSA”) would have had a bachelor’s degree in computer science or in a related field with coursework relating to computer science, plus two years of academic and/or industry experience in computer security. More education could substitute for experience, and vice versa. This person would have been capable of understanding and applying the teachings of the ’014 patent and the prior-art references discussed in this declaration.

[0041] By 2007, I held two different master’s degrees in Electrical Engineering and Computer Science, a Ph.D. in Computer Science, and was a professor in Computer Science and Engineering at Lehigh University in Bethlehem, Pennsylvania. Before those degrees, I obtained my bachelor’s degree in Mathematics and Engineering Science from Dartmouth College, which at that time (1982) did not have a department called “Computer Science,” but did offer courses in computer science subjects. My bachelor’s degree involved significant computer science coursework, including a course titled “Introduction to Computer

Science” and more advanced courses in digital electronics, program system design and development, computer architecture, programming languages, etc. By 2007, I had over twenty years of academic and industry experience in computer science, working as a Principal Scientist at the Matsushita Information Technology Laboratory and a technical staff member at Bell Labs/Lucent Technologies, as well as various visiting professorships and research fellowships at other universities. I also had over fifteen years of academic and industry experience in computer security, including experience with HIPs and CAPTCHA, including the experience listed in Section I above. Therefore, I was a person of more than ordinary skill in the art during the relevant timeframe. However, I worked with many people who fit the characteristics of the POSA, and I am familiar with their level of skill.

When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

V. THE '014 PATENT

A. Described Embodiments

[0042] 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. The '014 patent notes that 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.

[0043] The '014 patent attempts to avoid requiring all users to answer 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.

[0044] Such techniques were not new in the '014 patent. For example, Willner (EX1005, discussed further below) 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, discussed further below) had disclosed detecting “click fraud” perpetrated by “various automated methods” by analyzing “attributes” including the “internet protocol (IP) address of the client-computing device [],...geographic location,...web history,...etc.” via “statistical models” to determine “a probability that the request is originating from an automated system.” Kitts, [0003]-[0005], [0021], [0046], [0049]. Indeed, the prior art discussed in this declaration provided far greater detail than the '014 patent does regarding *how* to use biometrics and other collected data to distinguish human users from bots.

B. Prosecution History of the '014 Patent

[0045] I have reviewed the '014 patent's specification, the patent's prosecution history, and the provisional application listed on the patent's face. The application that ultimately issued as the '014 patent was filed on August 5, 2022, as a continuation of a chain of parent applications. One of those parent

applications had issued as the '008 patent, and another of those parent applications had issued as the '885 patent. The '014 patent's application's filing in August 2022 was after the petitions in IPR2022-00940 ('008 patent) and IPR2022-00941 ('885 patent) had been filed in April 2022. Together with the '014 patent's application, the applicant filed an information disclosure statement that cited, among other things, the two IPR petitions and the prior-art references that were discussed in those petitions. EX1002 at 17-25.

[0046] In October 2022, the Examiner issued an Office Action that rejected the '014 patent's application's claims over a combination of references called Afergan, McNair, and Farahat. EX1002 at 117. In January 2023, the applicant addressed this rejection by arguing that Afergan and McNair did not teach various claim limitations. EX1002 at 309-323. By this time in January 2023, the PTAB had already issued institution decisions in December 2022 granting institution of IPR2022-00940 ('008 patent) and IPR2022-00941 ('885 patent). However, I find no indication in the '014 patent's prosecution history of the applicant ever informing the Examiner of these institutions or providing copies of the institution decisions for the prosecution record.

[0047] The Examiner issued a Notice of Allowance on March 8, 2023. EX1002 at 407-413. The notice included "an examiner's statement of reasons for allowance," stating that "the examiner agrees that the combination of the cited

prior art would not make it obvious for one of ordinary skill in the art, prior to the instant effective filing date, 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.” EX1002 at 412. The notice also included a “References Cited” section stating that “Gusler et al., USPN 2008/0263636, discloses a method of determining a likelihood that a user is actually a bot (0025), but does not disclose using collected passive data to make the determination.” EX1002 at 412.

[0048] However, I find no discussion by the Examiner of the Willner, Kitts, or Broder references, even though they were discussed in the IPR petitions that the applicant cited in the August 2022 information disclosure statement. The petition in IPR2022-00940 had discussed how Willner combined with Kitts satisfies analyzing collected passive data together with active data in conjunction with model data based on human interactions from a prior session with the same website. The petition in IPR2022-00941 had discussed how Broder supplies teachings to afterwards challenge the user with a CAPTCHA. The Examiner in the ’014 patent’s prosecution did not provide any reasoning to explain why he did not apply these teachings of Willner, Kitts, and Broder to the ’014 patent’s claims, as these teachings directly contradict the stated reasons for allowance.

VI. CLAIM INTERPRETATION

[0049] In accordance with the standards for interpreting patent claim terms discussed in Section III (paragraph [0027]) above, I have applied the meanings of “model data” and “monitored data” discussed in the ’014 patent at 2:64-3:56. The ’014 patent’s specification further defines the terms “available data,” “acquired data,” “issued data,” and “interest data,” but those terms do not appear in the ’014 patent’s claims.

[0050] I understand that Petitioner has proposed in district court that the preambles of the ’014 patent’s independent claims are limiting, and has proposed the constructions of “active data” and “passive data” discussed in the subsections below. I have applied these constructions to these claim terms in my analysis in this declaration. While I have not personally formed an opinion as to whether the independent claims’ preambles are limiting, I discuss in this declaration how the prior art satisfies the preambles’ recitations, to demonstrate how the claims are unpatentable regardless of whether the preambles are limiting or not. As to “active data” and “passive data,” I agree that Petitioner’s proposed constructions are reasonable as discussed in the subsections below. It is not necessary for me to form an opinion as to whether Petitioner’s proposed constructions or Patent Owner’s proposed constructions are correct for these terms, because Petitioner’s proposed constructions are narrower than Patent Owner’s

proposed constructions (as discussed further in the subsections below). Therefore, by demonstrating in this declaration how the prior art satisfies Petitioner’s narrower proposed constructions, I am also demonstrating how the prior art satisfies Patent Owner’s broader proposed constructions. In other words, because the claims are unpatentable under either construction, it is not necessary for me to form an opinion as to which construction is correct.

[0051] For all other claim terms, I have interpreted the terms in accordance with their ordinary and customary meaning as understood by a POSA in the context of the patent (including the descriptions in the specification) and its prosecution history, in accordance with the standards set forth in Section III above.

A. “active data”

[0052] I have been informed by counsel that Patent Owner Nobots and Petitioner Google propose the following constructions of “active data” in district court:

Nobots’s Proposed Construction	Google’s Proposed Construction
Plain and ordinary meaning with the explanation that “active data includes, without limitation, pointing device vector movements and/or cadence, key stroke combinations and/or cadence, time differentials between stimulus (e.g., display of dialog box, radio button, form field, etc., and/or generation of sound) and user response (e.g., input into dialog box, selection of radio button, completion of form field, new page display request rates, etc., and/or input response to sound), and similar metrics.”	“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, including, without limitation, pointing device vector movements and/or cadence, key stroke combinations and/or cadence, time differentials between stimulus (e.g., display of dialog box, radio button, form field, etc., and/or generation of sound) and user response (e.g., input into request rates, etc., and/or input response to sound), and similar metrics”

[0053] I note that Petitioner Google’s proposed construction is composed of text from the ’014 patent’s discussion of “active model data” at 3:3-15. Patent Owner Nobots’s proposed construction contains the examples listed following “includes, without limitation” in the specification, but omits the “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” portion. The text of Patent Owner’s construction is a subset of the text of Petitioner’s construction, and therefore the scope of the claim term under Patent Owner’s construction is a superset of the scope of the claim term under Petitioner’s construction. In other words, Patent Owner’s construction is broader and Petitioner’s construction is narrower. In this declaration, I explain below how the prior art satisfies Petitioner’s narrower construction, which necessarily also demonstrates how the prior art satisfies Patent Owner’s broader construction. Therefore, it is not necessary for me to form an opinion as to which construction is correct, because my opinion regarding the claims’ unpatentability is the same either way.

[0054] In my opinion, Petitioner’s proposed construction is a reasonable construction of “active data” in the context of the ’014 patent. The specification does not define the phrase “active data” separately or differently from

“active model data,” and its discussion of “active data” (3:34-42) is consistent with the definition of “active model data.”

B. “passive data”

[0055] I have been informed by counsel that Patent Owner Nobots and Petitioner Google propose the following constructions of “passive data” in district court:

Nobots’ Proposed Construction	Google’s Proposed Construction
Plain and ordinary meaning with the explanation that “passive data includes, 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.”	“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, including, 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.”

[0056] I note that Petitioner Google’s proposed construction is composed of text from the ’014 patent’s discussion of “passive model data” at 3:19-27. Patent Owner Nobots’s proposed construction contains the examples listed following “includes, without limitation” in the specification, but omits the “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” portion. The text of Patent Owner’s construction is a subset of the text of Petitioner’s construction, and therefore the scope of the

claim term under Patent Owner’s construction is a superset of the scope of the claim term under Petitioner’s construction. In other words, Patent Owner’s construction is broader and Petitioner’s construction is narrower. In this declaration, I explain below how the prior art satisfies Petitioner’s narrower construction, which necessarily also demonstrates how the prior art satisfies Patent Owner’s broader construction. Therefore, it is not necessary for me to form an opinion as to which construction is correct, because my opinion regarding the claims’ unpatentability is the same either way.

VII. PRIOR-ART REFERENCES

[0057] I briefly introduce in this Section below various prior-art references discussed in this declaration.

A. Willner (EX1005)

[0058] According to the face of the document, Willner is a published U.S. patent application, filed on July 16, 2007, as Application No. 11/778,140, and published on January 22, 2009, as Publication No. 2009/0024971. I have been informed by counsel that Willner meets the requirements to be prior art to the ’014 patent, based at least on Willner’s filing date.

[0059] Willner is titled “Cursor Path Vector Analysis for Detecting Click Fraud,” and relates to “[a] system and method for detecting click fraud where data is received corresponding to a tracking of movement of a cursor on a web

page,” and “[a] confidence level useable in the determination of click fraud is determined...responsive to analysis of...the cursor movement.” Willner, Abstract. I discuss Willner further in each of Grounds 1-4 (Sections VIII.A – VIII.D) below, which detail how each of the ’014 patent’s claims would have been obvious over Willner in combination with other references.

B. Kitts (EX1009)

[0060] According to the face of the document, Kitts is a published U.S. patent application, filed on November 13, 2006, as Application No. 11/559,291, and published on May 15, 2008, as Publication No. 2008/0114624. I have been informed by counsel that Kitts meets the requirements to be prior art to the ’014 patent, based at least on Kitts’s filing date.

[0061] Kitts is titled “Click-Fraud Protector,” and relates to “[d]etermining the probability that a user or program fraudulently initiated a web-page request” by “determin[ing] attributes associated with the web-page request” and “calculat[ing] a probability” wherein “the attributes and other parameters are fed into a statistical model.” Kitts, Abstract. I discuss Kitts further in each of Grounds 1-4 (Sections VIII.A – VIII.D) below, which detail how each of the ’014 patent’s claims would have been obvious over Willner in combination with Kitts and other references.

C. Broder (EX1011)

[0062] According to the face of the document, Broder is a published U.S. patent application, filed on December 19, 2006, as Application No. 11/642,098, and published on June 19, 2008, as Publication No. 2008/0147456. I have been informed by counsel that Broder meets the requirements to be prior art to the '014 patent, based at least on Broder's filing date.

[0063] Broder is titled "Methods of Detecting and Avoiding Fraudulent Internet-Based Advertisement Viewings," and relates to "interject[ing] an intermediate web page after a web viewer selects an advertising link but before the web viewer is sent to the advertiser's designated web site," to "analyze[] the web viewer's response to the intermediate web page (if any) along with other information using an adjustable testing policy to make a determination as to whether the web viewer is a human or non-human entity." Broder, Abstract. I discuss Broder further in each of Grounds 1-4 (Sections VIII.A – VIII.D) below, which detail how each of the '014 patent's claims would have been obvious over Willner in combination with Kitts and Broder (plus other references for certain dependent claims).

D. Tanzer (EX1012)

[0064] According to the face of the document, Tanzer is a published U.S. patent application, filed on April 29, 2006, as Application No. 11/380,921,

and published on November 1, 2007, as Publication No. 2007/0255818. I have been informed by counsel that Tanzer meets the requirements to be prior art to the '014 patent, based on Tanzer's filing and publication dates.

[0065] Tanzer is titled "Method of Detecting Unauthorized Access to a System or an Electronic Device," and relates to "captur[ing] and stor[ing]" "[c]haracteristics of a user's behavior on an electronic device" so that "[t]hese stored characteristics are compared to the characteristics of a subsequent user" and "an alert is activated" "[i]f the differences in the characteristics are such that fraud is suspected." Tanzer, Abstract. I discuss Tanzer further in Ground 2 (Section VIII.B) below, which details how claims 4, 19, and 23 of the '014 patent would have been obvious over Willner in combination with Kitts, Broder, and Tanzer.

E. Meek (EX1008)

[0066] According to the face of the document, Meek is a published U.S. patent application, filed on June 15, 2004, as Application No. 10/868,116, and published on December 15, 2005, as Publication No. 2005/0278253. I have been informed by counsel that Meek meets the requirements to be prior art to the '014 patent, based on Meek's filing and publication dates.

[0067] Meek is titled "Verifying Human Interaction to a Computer Entity by Way of a Trusted Component on a Computing Device or the Like," and relates to "monitor[ing]" various "indicia...that can be employed to detect that the

user is in fact expending effort.” Meek, Abstract. I discuss Meek further in Ground 3 (Section VIII.C) below, which details how claims 9, 15, and 30 of the ’014 patent would have been obvious over Willner in combination with Kitts, Broder, and Meek.

F. Farahat (EX1022)

[0068] According to the face of the document, Farahat is a published U.S. patent application, filed on December 19, 2003, as Application No. 10/742,380, and published on June 30, 2005, as Publication No. 2005/0144067. I have been informed by counsel that Farahat meets the requirements to be prior art to the ’014 patent, based on Farahat’s filing and publication dates.

[0069] Farahat is titled “Identifying and Reporting Unexpected Behavior in Targeted Advertising Environment,” and relates to “detecting non-conforming behavior associated with pay-per-click advertising in a keyword searching environment.” Farahat, Abstract. I discuss Farahat further in Ground 4 (Section VIII.D) below, which details how claim 13 of the ’014 patent would have been obvious over Willner in combination with Kitts, Broder, and Farahat.

VIII. THE ’014 PATENT’S CLAIMS WOULD HAVE BEEN OBVIOUS OVER THE PRIOR ART

[0070] I have been asked to provide my opinion concerning whether claims 1-30 of the ’014 patent would have been obvious to a POSA in light of the

prior-art references identified above. For the reasons explained below, it is my opinion that each of claims 1-30 would have been obvious to a POSA.

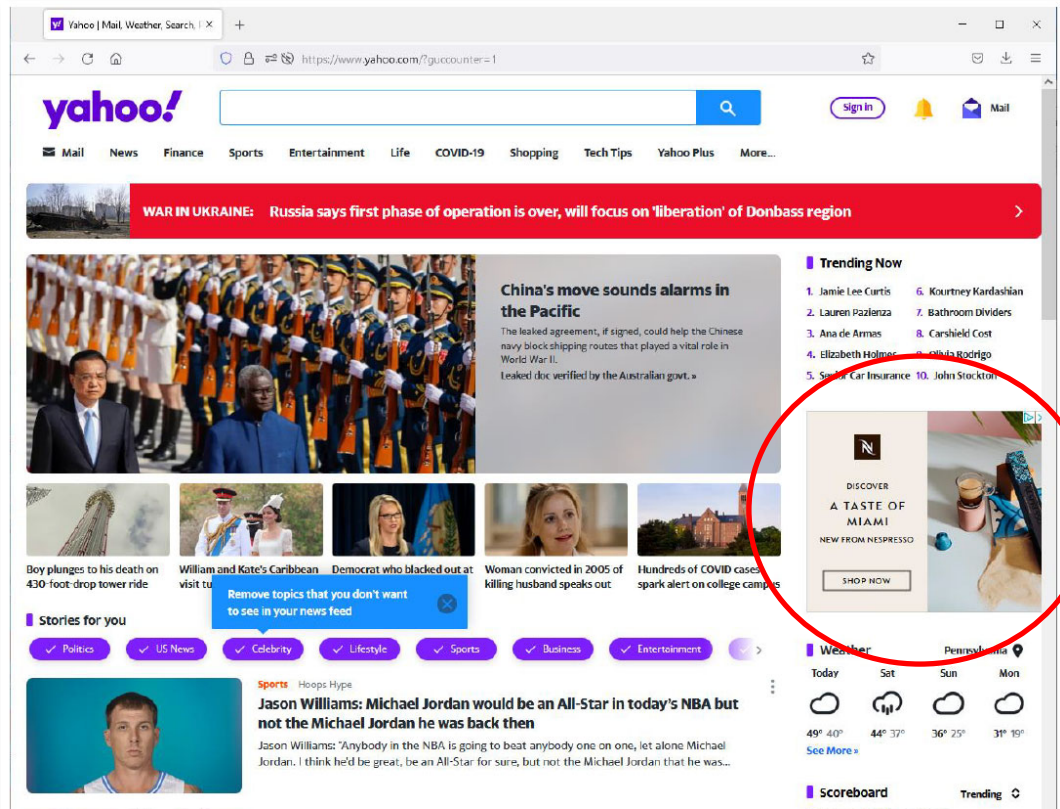
A. Ground 1: Claims 1-8, 10-12, 14, and 16-29 of the '014 Patent Would Have Been Obvious over Willner in View of Kitts and Broder

[0071] After reviewing Willner, Kitts, Broder, and claims 1-8, 10-12, 14, and 16-29 of the '014 patent, it is my opinion that each of these claims would have been obvious to a POSA in view of the combined teachings of Willner, Kitts, and Broder. A POSA would have had reasons to combine the collective teachings of these references to result in a combination that meets all limitations of each of claims 1-8, 10-12, 14, and 16-29, and would have reasonably expected success in doing so. In the alternative, to the extent the Board finds that the references do not expressly or inherently disclose certain limitations of these claims, a POSA would have had reasons to implement the teachings of these references in a typical, conventional, and obvious way that meets those limitations, as I discuss in the corresponding sections below. The bases for my opinion and the details of my analysis are below.

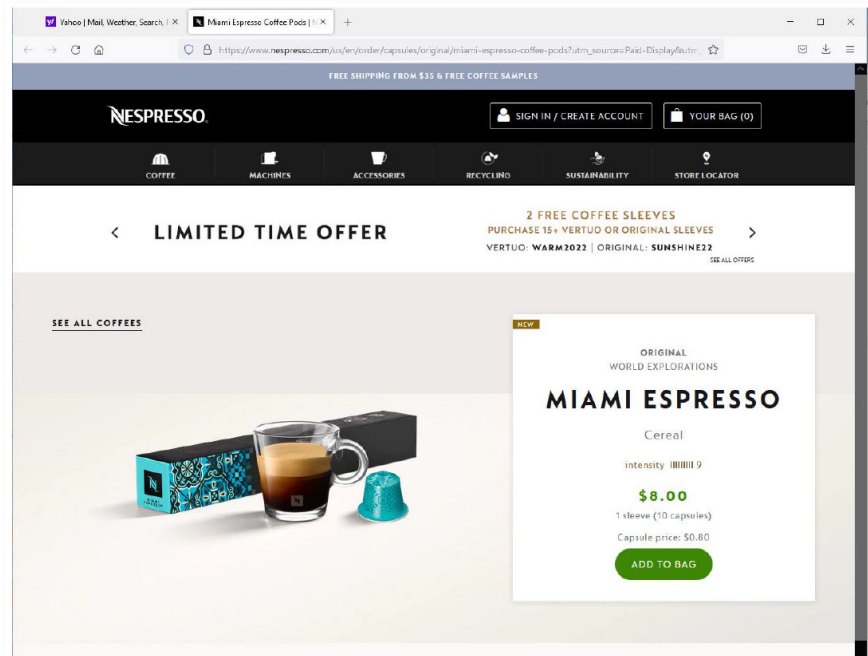
1. Discussion of Willner (EX1005)

[0072] 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

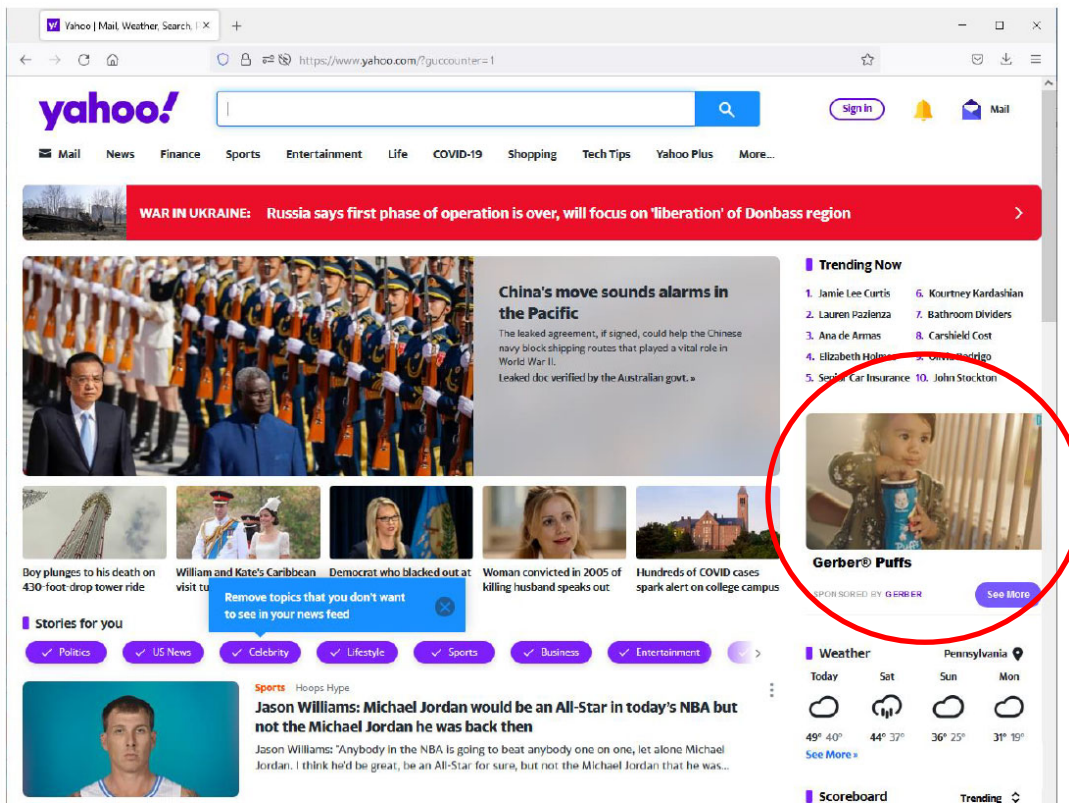
publisher's website (e.g., Yahoo), and pay the publisher for each "click through" whereby a user clicks on the advertisement and is referred to the advertiser's website. Willner, [0002]. I have created some example screenshots from interacting with Yahoo's website, <https://www.yahoo.com>, as shown below, where I have added red circles around advertisements in the screenshots:



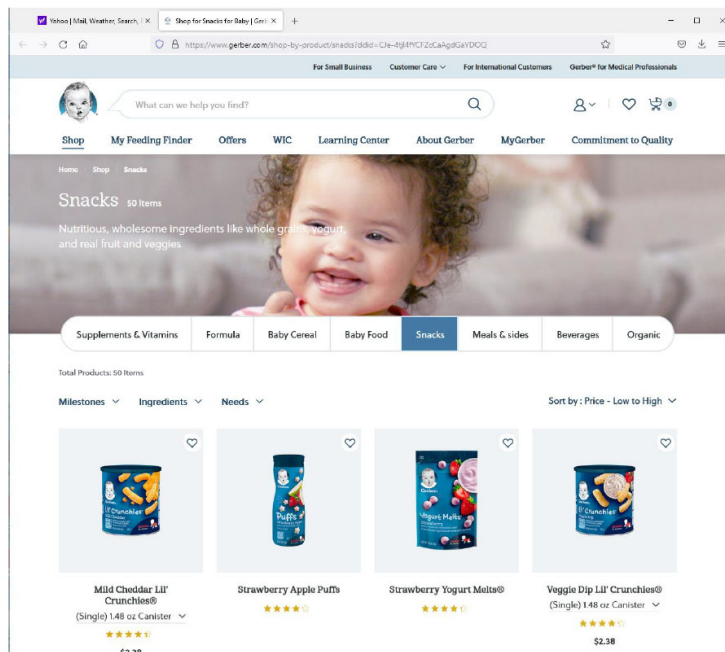
(Yahoo website with Nespresso advertisement)



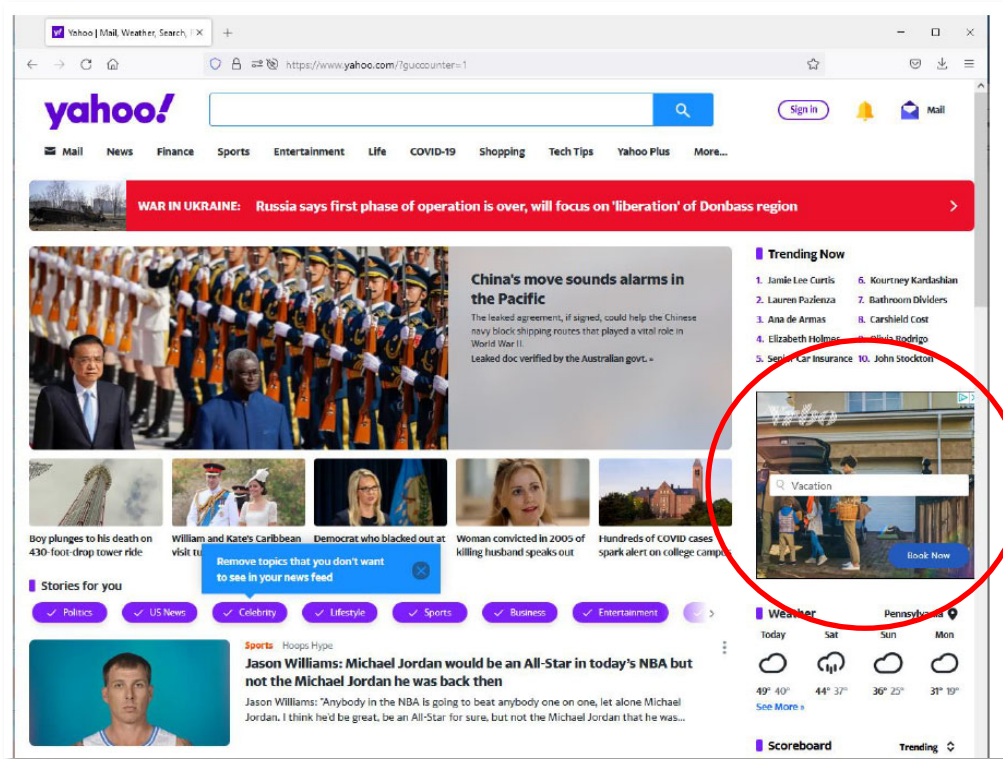
(Nespresso website displayed on click of advertisement)



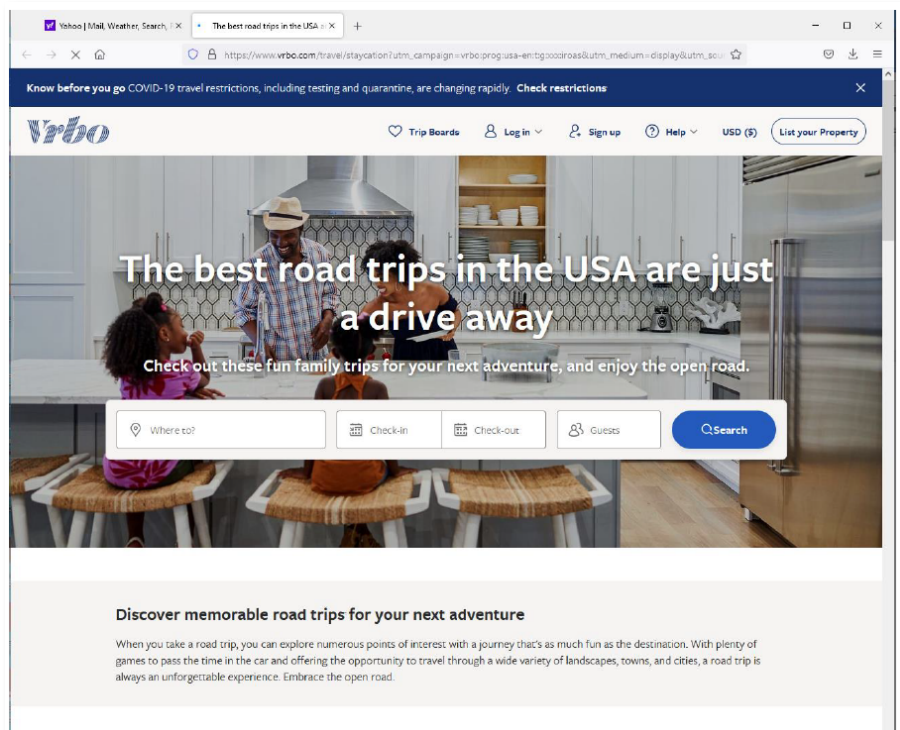
(Yahoo website with Gerber advertisement)



(Gerber website displayed on click of advertisement)



(Yahoo website with Vrbo advertisement)



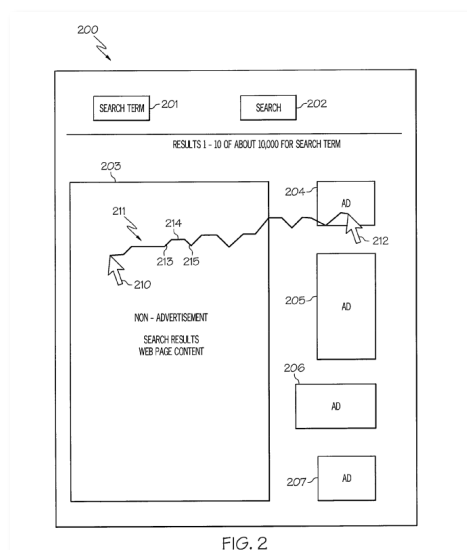
(Vrbo website displayed on click of advertisement)

[0073] I created the above images using the following steps. First, I opened a new window in my Firefox web browser. Second, I navigated to the web address <https://www.yahoo.com>. Third, I used the Windows print active window function (Ctrl-Alt-Print Screen) to capture the active window. Fourth, I pasted the captured window to create its screenshot. Fifth, I went back to the Yahoo homepage and clicked on the banner ad on the right side of the webpage. Clicking on the advertisement caused the browser to open a new tab and navigate to the website that the advertisement linked to. Sixth, I captured the resulting webpage that opened in the new tab, using the Windows print active window function (Ctrl-Alt-Print Screen). Seventh, I pasted the captured window to create its screenshot. Eighth, I repeated the prior steps twice more to capture the interactions with three different banner ads total. The banner ad on the Yahoo homepage changes to a different ad at intervals of several seconds, so repeating the steps after some seconds had passed resulted in interactions with different advertisements linking to different advertisers' websites. Finally, in reproducing these images in this declaration, I added the red circles shown above to indicate where the banner ads on which I clicked are located on the Yahoo webpage.

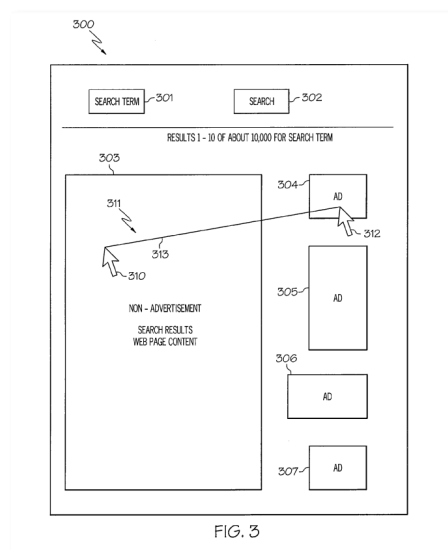
[0074] Returning to Willner: Willner explains that "Click Fraud may be accomplished via automated scripts (clickbots)" that "repeatedly generate[] clicks to a PPC advertisement with the intent of generating an improper charge to the

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].

[0075] 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 (reproduced below) illustrates a “human-like cursor movement” path 211 which “includes a series of multiple vectors,” unlike the “perfectly straight line” 311 in Figure 3 (also reproduced below) which indicates “click fraud cursor movement...generated by software...or...automation tool.” Willner, [0046]-[0048].



(FIG. 2, human movement)



(FIG. 3, clickbot movement)

[0076] 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.

[0077] 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].

2. Discussion of Kitts (EX1009)

[0078] 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].

[0079] The “attributes” that Kitts analyzes include “an internet protocol (IP) address of the client-computing device 202, date, time, geographic location, metadata, key words, HTML tags, or other characteristics associated with the page request,...the user’s gender, ethnicity, age, web history, residence, etc.” Kitts, [0046]-[0048], [0067]. The ’014 patent refers to such data as “passive model data.” EX1001, 3:19-27 (“Passive model data...includes, without limitation,...originating IP address,...originating IP address physical location,...etc.”).

3. Discussion of Broder (EX1011)

[0080] Like Willner and Kitts, Broder relates to detecting and avoiding fraudulent internet-based advertisement viewings by “[n]on human entities such as automated web crawlers or malicious click-fraud programs.” Broder, Title, Abstract. In relevant part, Broder teaches to “consider a large number of different factors depending on what information is collected from the web viewer and the desires of the advertiser” 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].

[0081] Broder also 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 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].

4. Discussion of Willner-Kitts-Broder Combination

[0082] A POSA having access to Willner’s teachings in conjunction with Kitts’s and Broder’s teachings would have been motivated and would have reasonably expected success to extend and/or modify Willner’s system in various ways, which I discuss in two subsections below. First, I discuss collecting and

analyzing what the '014 patent calls “passive data” in addition to what the '014 patent calls “active data.” Second, I discuss performing further testing based on results of the active/passive data analysis.

a. Passive Data

[0083] In view of Kitts’s teachings, a POSA would have been motivated to add Kitts’s statistical model analysis and use of passive model data (Kitts’s “attributes”) to determining the confidence level in Willner’s method. Willner and Kitts address the same problem of preventing automated click fraud on webpage advertisements (*see* above Sections VIII.A.1 and VIII.A.2 (Discussions of Willner and Kitts)), 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 (at [0068]) teaches that “[a]dditionally, other user or program parameters may also be used in conjunction with the attributes to determine the probability,” and a POSA would have been motivated to improve Willner’s performance in detecting automated click fraud by analyzing passive data as Kitts teaches, in addition to active data as Willner teaches. Kitts (at [0047]) teaches that “[s]uch information can be an important tool in determining whether the user requesting the web page has a propensity for click fraud,” and it was well known to POSAs that analyzing

passive data could help differentiate humans from bots. For corroborating evidence of the POSA's background knowledge in this regard, *see*, e.g., the following references which describe analyzing passive data to help differentiate humans from bots: Ge (EX1014), [0082]-[0083]; English (EX1015), 3:17-29.

[0084] POSAs would have reasonably expected success in the above-discussed implementation 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.

[0085] When Willner's teachings are combined with Broder's, the obviousness of collecting and analyzing both active and passive data is alternatively and additionally further supported by Broder's teachings. As discussed above in Section VIII.A.3 (Discussion of Broder), 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].

[0086] POSAs would have been motivated by the above-discussed teachings to collect and analyze both what the '014 patent calls "active data" (as Willner and Broder both disclose) and what the '014 patent calls "passive data" (as

Kitts and Broder both disclose) in assessing whether the client computer is being operated by a human or a bot. 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 nothing more than ordinary programming skill to implement such data collection and analysis. As the '014 patent itself admits, passive data is already "normally stored (logged) or transmitted to a remote location" and "is readily harvestable by query." EX1001, 3:19-27, 4:9-11. And both Kitts and Broder teach that such data can be analyzed using modeling techniques that POSAs knew were old and well understood, such as, e.g., "Bayesian" classifiers. Kitts, [0049], [0068]; Broder, [0074].

b. Further Testing, Including CAPTCHA

[0087] As discussed above in Section VIII.A.3 (Discussion of Broder), Broder teaches benefits of "interjecting an intermediate web page between the display of the original web page wherein the advertisement was selected by the web viewer and the advertiser's designated web page," to "test for and reduce non human web site traffic." Broder, [0029]. "The intermediate page may take many different forms and may be used to help determine if the entity that selected the advertisement link was a human or non human entity." Broder, [0029]. One type

of intermediate page that can be interjected is “a CAPTCHA page” that presents “a challenge-response test used to determine whether or not the web viewer is human.” 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].

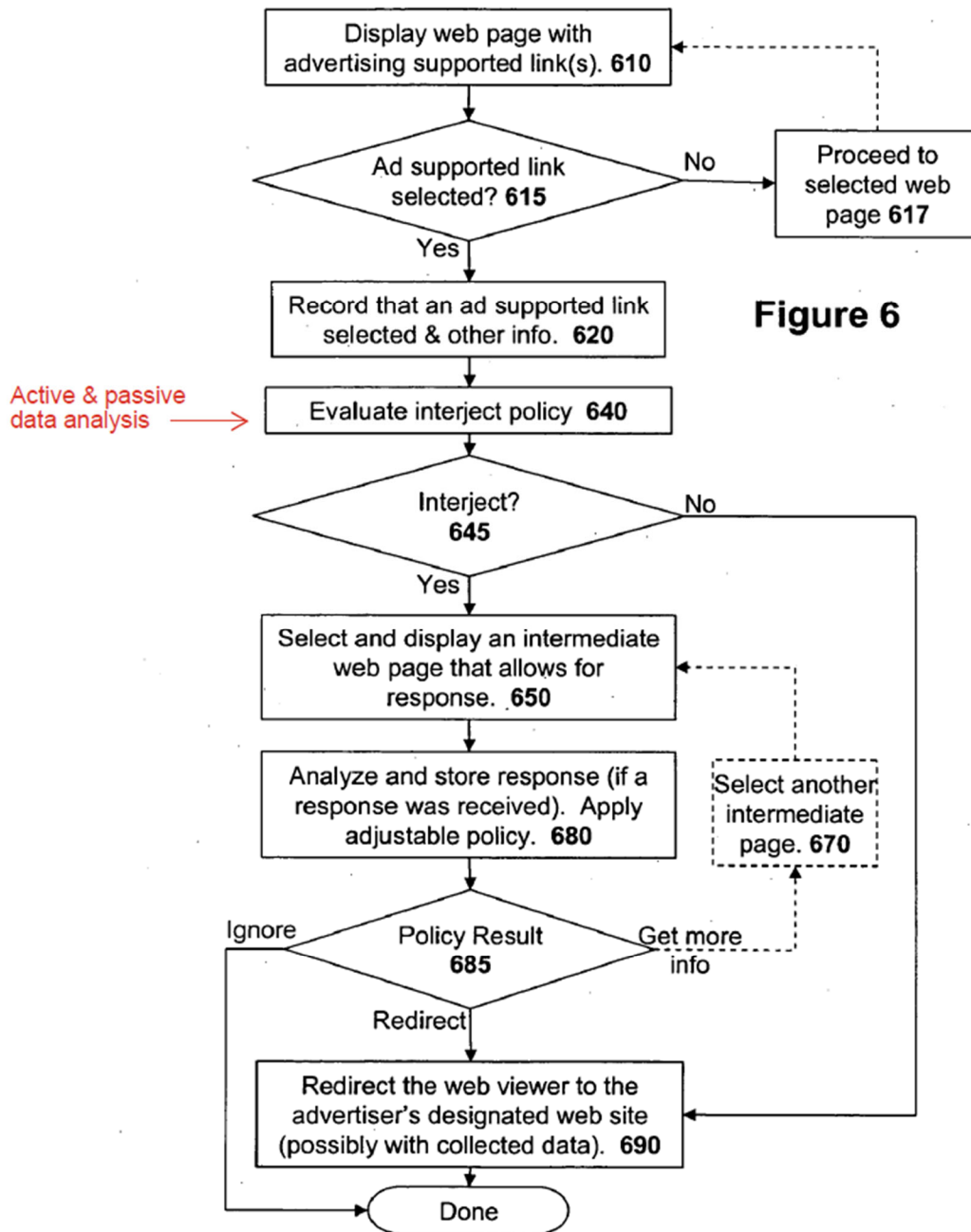
[0088] Broder recognizes that “[a]lthough a CAPTCHA intermediate web page presents the best system for determining if a web viewer is a human or non human entity,...the annoyance of having to complete a CAPTCHA task will tend to drive many web viewers away.” Broder, [0041]. “Consumers that browse the web can be notoriously impatient and easily alienated,” so “one may not wish to interject an intermediate web page every time that a web viewer selects an advertising link.” Broder, [0060]. Therefore, Broder teaches to “evaluate[] an adjustable interject policy” to “determine[] whether or not an intermediate web page should be displayed to the web viewer for the purpose of helping to determine if the web viewer is a human or non human entity.” Broder, [0061]-[0062].

[0089] “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 that may be considered” 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].

[0090] As discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data), Broder itself discusses analyzing active and passive data as part of the “adjustable policy” applied in box 680 of Fig. 6 after an intermediate page has been presented and responded to. Broder, [0042]-[0053]. In the Willner-Kitts-Broder combination, POSAs would have also found it obvious to analyze active and passive data as part of an “adjustable interject policy” for determining whether to present an intermediate page in the first place, such as in box 640 of Broder’s Fig. 6. Broder, [0060]-[0072]. POSAs would have understood that the analysis of active and passive data performed by the Willner-Kitts-Broder combination (as discussed in the Section just above this one) is a suitable type of adjustable interject policy for determining whether “the level of suspicion” as to whether the client may be a bot 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” (which could beneficially include Willner’s active data) as Broder discusses. Broder, [0063]-[0070]. This can be illustrated by annotation of Broder’s Figure 6 as follows:



Broder, Figure 6 (annotated)

[0091] In situations where the Willner-Kitts-Broder combination's 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 then interject an intermediate page, such as a CAPTCHA page, 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 the Willner-Kitts-Broder combination) "to make a determination as to whether the web viewer is a human or non-human entity." 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." EX1007 ("O'Connell"), [0032]. For further evidence corroborating POSAs' background knowledge in this regard, *see also* Emigh (EX1016), 9:64-66 ("If it is determined that there is a high likelihood that the incoming message is spam, the message may be retained pending the results of a challenge."), 10:21-42 (discussing comparing "a spam likelihood value p" to a "suspicion threshold" and a "junk threshold," where "[i]f the spam likelihood value is greater than the suspicion threshold" but

“less than the junk threshold,...a challenge may be issued...to determine whether the message is spam or is legitimate”), 11:7-9 (“If the likelihood value p is less than the junk threshold, the message may be retained pending the outcome of a challenge operation.”), 14:47-62 (the “challenge” can be a “captcha”).

[0092] 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. Corroborating evidence of this background knowledge of POSAs can be found, for example, in EX1007 (O’Connell) at [0049] (discussing how “slow[ing] down the automated program” helps to “make it less efficient (and thus useful)”).

[0093] POSAs would have reasonably expected success in implementing the above-discussed features based on Broder’s teachings of successfully interjecting intermediate webpages in the same context of detecting click fraud that concern Willner and Kitts, and because it would have required nothing more than POSAs’ ordinary programming skill to implement such an intermediate page.

5. Mapping of Willner-Kitts-Broder Combination to Claims 1-8, 10-12, 14, and 16-29 of the ’014 Patent

[0094] Of the ’014 patent’s three independent claims (claims 1, 16, and 22), claim 16 is the broadest claim. Therefore, in the sections below, I first address claim 16 and its dependent claims (Sections VIII.A.5.a – VIII.A.5.f below), then

independent claim 1 and its dependent claims (Sections VIII.A.5.g – VIII.A.5.r below), and then independent claim 22 and its dependent claims (Sections VIII.A.5.s – VIII.A.5.z below). In the sections below in this declaration, uses of italic font designate claim language. All uses of bold emphasis below (including bold italics to emphasize words that match claim language) are added unless otherwise indicated.

- a. **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:**

[0095] 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 claim elements [16A]-[16E] as Sections VIII.A.5.a.i – VIII.A.5.a.v below demonstrate. Willner, [0028]-[0030], claims 17-19. Willner teaches that 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).

[0096] The Willner-Kitts-Broder combination’s functionality *performs* a “**method** for detecting click fraud,” whereby “[a] confidence level useable in the determination of click fraud is determined.” Willner, Abstract, [0049], claims 8-9 (“*providing* a confidence factor *indicative* of click fraud”). POSAs would have understood that the provided 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 or not occurring. Willner, [0050]-[0051], [0043] (Willner’s analysis is used to “**judge** whether or not this was click fraud”).

[0097] 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” (i.e., it is not likely click fraud), while “not” human-like movement produces “a low confidence factor” (i.e., it is likely clickbot fraud). 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.*

[0098] Broder likewise teaches to output “a ***judgment*** as to whether the web viewer is human or not,” with the “***judgment***” being a “probabilistic” value. Broder, [0054], [0057]. Further, providing the confidence level/factor as *a value indicating the judgment* would also have been obvious to a POSA in view of 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]. “Embodiments are not limited to actual percentages or proportions. Rather, any ***value***, such as a numeric, binary, hexadecimal, or the like may be used.” Kitts, [0032]. Alternatively, a POSA would also have understood generating a value to be a straightforward, conventional, and obvious way of representing the confidence level to indicate the human/bot judgment in Willner’s computer-implemented system. For corroborating evidence in this regard, see, e.g., Afergan (EX1013), which corroborates that it was within the POSA’s

background knowledge that a score “that represents a confidence value” regarding whether “the user agent is associated with a human user or an automated agent” “may be represented as a number, a percentage, a code, or in any other convenient symbol, character or representation.” Afergan, [0040], [0155].

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

[0099] The '014 patent's specification never uses the term “*data collection data*.” It does say that both “[a]ctive and passive data” can be “collected” (FIG. 4), and it discusses collecting passive data the way such data is “normally...transmitted to a remote location,” 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, as well as the listed browser cookies, etc., to be examples of *data collection data*.

[0100] 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 prior to the advertisement on the web page being clicked.” Willner, [0010]. The code can be “downloaded” to the client 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.

[0101] As discussed above in Section VI.A, I understand that Petitioner in district court has proposed construing “*active data*” based on the ’014 patent’s discussion of “active model data” at 3:3-15, 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, including, without limitation, **pointing device vector movements** and/or cadence, key stroke combinations and/or cadence, time differentials between stimulus (e.g., display of dialog box, radio button, form field, etc., and/or generation of sound) and user response (e.g., input into dialog box, selection of radio button, completion of form field, new page display request rates, etc., and/or input response to sound), and similar metrics.” I understand that Patent Owner proposes a broader “[p]lain and ordinary meaning” construction that includes the listed examples. As discussed above in Section VI.A, it is not necessary to my opinions for me to decide which construction is correct, because the prior art satisfies the claim element either way, because by satisfying Petitioner’s narrower construction it also satisfies Patent Owner’s broader construction. But, in my

opinion, Petitioner’s construction is at least reasonable for the reasons discussed above in Section VI.A.

[0102] In Willner’s disclosure, the “cursor **movement vectors**”—made “by a **pointing device** such as a mouse”—that Willner’s webpage markup/code requests and collects are one of the examples of *active data* discussed in the ’014 patent. Willner, [0033], [0046] (“The path traveled 211 by a cursor, which may be controlled by a **pointing device** such as a mouse, controlled by software, or an automation tool, may be mapped into one or more **vectors** that define the path 211 from the first position 210 to the location of the advertisement 212.”). 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]. Therefore, Willner’s collected cursor-movement data satisfy both parties’ constructions of “*active data*,” and Willner’s *data collection data* thus *requests active data of the client computer*.

[0103] As to *passive data*, as discussed above in Section VI.B, I understand that Petitioner in district court has proposed construing “*passive data*” based on the ’014 patent’s discussion of “passive model data” at 3:19-27, 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, including, 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.” I understand that Patent Owner proposes a broader “[p]lain and ordinary meaning” construction that includes the listed examples. As discussed above in Section VI.B, it is not necessary to my opinions for me to decide which construction is correct, because the prior art satisfies the claim element either way, because by satisfying Petitioner's narrower construction it also satisfies Patent Owner's broader construction. But, in my opinion, Petitioner's construction is at least reasonable for the reasons discussed above in Section VI.B.

[0104] As discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data), the Willner-Kitts-Broder combination 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]. Attributes may also be retrieved via browser cookies. Kitts, [0047]. Kitts thus teaches collecting *passive data of the client computer* under either party's construction of "*passive data*," including via cookies which satisfy *providing data collection data requesting passive data*, as discussed above (paragraph [0099])). POSAs would have been motivated and reasonably expected success to incorporate such *passive data* collection and analysis for the reasons discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data).

[0105] Alternatively or additionally, POSAs would have been motivated and reasonably expected success to incorporate such *passive data* collection and analysis for the reasons discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data) related to Broder's teachings, including Broder's teaching to "consider a large number of different factors," including both *active data* and *passive data*, in differentiating humans from clickbots. Broder, [0043]-[0052], [0063]-[0070]. In addition to *active data* such as data related to mouse clicks (Broder, [0045]-[0046]), Broder teaches to additionally collect and analyze *passive data* such as IP address ([0051], [0068]), physical geographic origin ([0052], [0069]), and/or information provided via browser cookies ([0027]), which are examples of *passive data requested by data collection data* in the '014 patent as discussed above (paragraph [0099])).

- ii. **[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;**

[0106] 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 above in Section VIII.A.5.a.i (discussing claim element [16A]). Willner, [0042]-[0043]. As discussed above in Section VIII.A.5.a (discussing the preamble [16Pre]), the cursor movement data *relate to interactions of the client computer with a website of the server*. Willner, [0041] (client computer is "access[ing] the *website hosted on the server*"), [0042]-[0048], [0054].

[0107] The Willner-Kitts-Broder combination also *receives passive data responsive to the data collection data* (e.g., via cookies) as discussed above in Section VIII.A.5.a.i (discussing claim element [16A]).

- iii. [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;

[0108] Willner's method "detects a click fraud based on an *analysis of the received data*." Willner, [0012]-[0014]. "[A] confidence factor may be determined based on the *analysis*." Willner, [0036]. And the confidence factor is *a value* as discussed above in Section VIII.A.5.a (discussing the preamble [16Pre]). Thus, the confidence factor is *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 as discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data), the Willner-Kitts-Broder combination 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].

[0109] 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 similarly discusses (EX1001, 5:9-23). Willner detects this type of bot fraud 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].

[0110] 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 (at [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 in [0037]-[0038] and FIG. 1. 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, and meet the '014 patent’s above-discussed definition of “*model data*.”

[0111] 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. As Willner explains, “different screen types,...different start positions, different trajectories,” etc., will all produce different movement vectors (Willner, [0037]); therefore, in order to detect duplication, POSAs would have known to compare cursor movements for the same given page on which a cursor might start from the same position (e.g., a search input field on that page) and travel the same path to the same end position (e.g., an advertisement on that page). POSAs knew that 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.”). See Mak (EX1017), [0047], corroborating this background knowledge.

[0112] The Willner-Kitts-Broder combination thus *analyzes the received active data in conjunction with model data based on human interactions from a prior session with the same website*, for the above-discussed reasons.

[0113] In view of Kitts’s and/or Broder’s teachings, the Willner-Kitts-Broder combination also *analyzes the received passive data* as discussed above in

this section and others. 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* and same webpage. 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 that 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); Emigh (EX1016), 18:31-67 (similarly corroborating the same background knowledge). 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*.

[0114] 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 (Broder, [0073]), which includes active and passive data as discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data).

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

[0115] 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 the Willner-Kitts-Broder combination, passive data also contributes to the confidence level based on Kitts’s and/or Broder’s teachings, as discussed above in Section VIII.A.4.a (Discussion of Willner-Kitts-Broder Combination as to Passive Data). “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].

[0116] POSAs knew that 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]. For further evidence corroborating POSAs’ background knowledge in this regard, *see also* Emigh (EX1016), 10:57-60 (“A binary decision mechanism” for deciding whether a received communication

is unwanted spam may “be implemented using” a “classifier tool that generates a scalar ‘likelihood of spam’ metric combined with a threshold test.”) POSAs would have understood and found it obvious, therefore, that the threshold value that the Willner-Kitts-Broder confidence factor must surpass in order to not be considered “low” and be disallowed access to the advertised webpage is *a predetermined criteria*. The Willner-Kitts-Broder combination 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 to be “low.”

- v. **[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.**

[0117] As discussed above in Section VIII.A.4.b (Discussion of Willner-Kitts-Broder Combination as to Further Testing), the Willner-Kitts-Broder combination 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, to *request further data from the client computer*. Broder, [0062]-[0063]. It was also background knowledge for POSAs that “request[ing] additional authentication information” is “appropriate course of action” based on “fraud detection results.” *See* O’Connell (EX1007), [0032], which is corroborating evidence of this background knowledge.

The analysis to determine whether to interject an intermediate page can consider any “click fraud indicators” that may “raise the level of suspicion” that the client may be a bot. Broder, [0070]-[0072]. In the Willner-Kitts-Broder combination, as discussed above in Section VIII.A.4.b (Discussion of Willner-Kitts-Broder Combination as to Further Testing), this analysis includes the active and passive data analysis discussed above in Sections VIII.A.5.a.i – VIII.A.5.a.iv (discussing claim elements [16A]-[16D]). When *the first analysis value fails to meet the first analysis predetermined criteria* (i.e., when the determined confidence value is lower than a pre-specified threshold, which raises the level of suspicion of click fraud as discussed above in Section VIII.A.5.a.iv (discussing claim element [16D])), the Willner-Kitts-Broder combination “selects and displays an intermediate web page for testing the web viewer” as Broder ([0072]) teaches.

[0118] “The intermediate page may take many different forms” which “may vary widely depending on the circumstances.” Broder, [0029], [0032]. Various options for the intermediate page may “require[] a web viewer to click a specified location,” and/or may “*request*[]” “demographic information,” or may request that the user submit 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.*

- b. **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.**

[0119] 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 that the advertisement links to is *a protected page*.

[0120] 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 user 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.

[0121] 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. This is discussed further in Sections VIII.A.5.e – VIII.A.5.f below (discussing claims 20-21 of the '014 patent).

- c. **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.**

[0122] 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]. The *manual input device activity is analyzed in conjunction with model data based on human interactions from a prior session with the same website*, as discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]). Willner, [0037]-[0039].

[0123] The Willner-Kitts-Broder combination's *received passive data includes at least one browser cookie and at least one IP address* based on 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 above in Section VIII.A.5.a.iii (discussing claim element [16C]). Kitts, [0047]-[0049]; Broder, [0073]-[0074].

- d. 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.**

[0124] At the time of the '014 patent's claimed priority date in 2007, 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. *See* Swanson (EX1018), [0039], which corroborates this background knowledge. *See also* Swanson at [0006]-[0007] (showing that Swanson is discussing a "Pay-per-click" advertising environment, which is the same type of environment that Willner, Kitts, and Broder relate to), [0058] (further discussing HTTPS as a known, commonly used option for network communications). For further evidence corroborating this background knowledge, *see also* Ling (EX1019), 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 (showing that Ling likewise is discussing an advertising environment with paid advertisements on a search engine webpage, like Willner's environment).

[0125] 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 in general. In obvious implementations, this would include *the received active data and the received passive data*, and the server would then *decrypt* that *received data* in order to be able to analyze it.

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

[0126] When the Willner-Kitts-Broder combination interjects an intermediate page as discussed in Section VIII.A.5.a.v above (discussing claim element [16E]) (*the request for further data*), *the client computer responds* by providing *further data* corresponding to the request. Broder, [0042] (“[A]fter displaying the intermediate web page...if any **response** was **received** from the web viewer,” the “system then stores and analyzes the web viewer’s response to the intermediate page...to determine whether the web viewer is a human or not and how the system should proceed.”).

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

[0127] The Willner-Kitts-Broder combination *performs a second level of analyzing on the received further data* when it “*analyzes* the web viewer’s response to the intermediate page.” Broder, [0042].

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

[0128] In analyzing the response to the intermediate page, Broder teaches that the “output” of this *second level of analyzing* includes “a judgment as to whether the web viewer is human or not,” wherein the “judgment is only probabilistic.” Broder, [0054], [0057]. POSAs would have found it obvious to implement such a probabilistic judgment by *providing a 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 probability” for human versus bot). This value may be considered *a second analysis value* because the value is provided from the *second level of analyzing*.

- f. **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.**

[0129] As discussed above in Section VIII.A.5.a.v (discussing claim element [16E]), one option Broder teaches 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].

In other words, Broder’s CAPTCHA is a test to determine if a computer user is a human or a bot. One example CAPTCHA “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.*

[0130] Claim 21 of the ’014 patent depends from claim 20, which recites providing *a second analysis value* based on the *second level of analyzing*, which is performed on *the received further data*. In Section VIII.A.5.g.ix below (discussing claim element [1I]), I provide further discussion on the *second analysis value* in the case where Broder’s intermediate page includes *a CAPTCHA test*.

- g. 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:**

[0131] The preamble of claim 1 ([1Pre]) shares much of the same language as the preamble of claim 16 ([16Pre]). All of the shared language is satisfied by the Willner-Kitts-Broder combination for the reasons already discussed above in Section VIII.A.5.a (discussing [16Pre]).

[0132] As to the few words that differ between [1Pre] and [16Pre]:

The Willner-Kitts-Broder combination’s *method generates* a confidence level/factor (which is the *value* discussed above in Section VIII.A.5.a (discussing [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 above in Section VIII.A.5.b (discussing claim 17).

- i. **[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;**

[0133] Willner discloses *providing data collection data that causes the client computer to collect active data*, as discussed above in Section VIII.A.5.a.i (discussing claim element [16A]). 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 prior to the advertisement on the web page being clicked.” Willner, [0010]. The code can be “downloaded” to the client 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 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 above in Section VIII.A.5.b (discussing 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.

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

[0134] The Willner-Kitts-Broder combination satisfies claim element [1B] for the reasons discussed above in Section VIII.A.5.a.ii (discussing claim element [16B]). The *active* and *passive data* are *received from the client computer*. Willner, [0043] (receiving active data “*from the* workstation/*client* device”); Kitts, [0047]-[0048] (receiving passive data in cookies and/or page request from “client-computing device”); Broder, [0043] (receiving active and passive data “from the web viewer”), [0063].

- iii. **[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;**

[0135] The Willner-Kitts-Broder combination *performs a first analysis* satisfying claim element [1C] in the manner discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]).

- iv. **[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;**

[0136] The Willner-Kitts-Broder combination *generates a first analysis value* (a confidence factor/level) *based on the first analysis* as discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]).

[0137] 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...related to the advertisement 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, like the threshold discussed

above in Section VIII.A.5.a.iv (discussing claim element [16D])). As discussed above in Section VIII.A.4.b (Discussion of Willner-Kitts-Broder Combination as to Further Testing), 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].

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

[0138] The Willner-Kitts-Broder combination satisfies claim element [1E] for the reasons discussed above in Section VIII.A.5.a.iv (discussing claim element [16D]).

vi. [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;

[0139] The Willner-Kitts-Broder combination satisfies claim element [1F] for the reasons discussed above in Sections VIII.A.5.a.v (discussing claim element [16E]) and VIII.A.5.f (discussing 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* Emigh (EX1016), 10:21-42, which corroborates POSAs’ background knowledge to issue a CAPTCHA challenge based on whether a “spam likelihood value” crosses a “threshold.”

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

[0140] The Willner-Kitts-Broder combination satisfies claim element [1G] for the reasons discussed above in Sections VIII.A.5.e – VIII.A.5.f (discussing claims 20-21).

viii. [1H] perform a second analysis comprising assessing accuracy of the response of the client computer to the CAPTCHA test; and

[0141] The Willner-Kitts-Broder combination satisfies claim element [1H] for the reasons discussed above in Sections VIII.A.5.e – VIII.A.5.f (discussing 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 from the web viewer is not logical then the response may be from a computer program.” Broder, [0046]. POSAs would have known that in the case where the intermediate page is a *CAPTCHA test* (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*.

Broder ([0040]) also incorporates by reference “U.S. Pat. No. 6,195,698” (EX1020, “Lillibridge”) for “[a]dditional information on CAPTCHAs,” and Lillibridge’s Abstract explains that, in response to a CAPTCHA, “the client computer sends an answer to the server,” which “determines if the guess is the correct answer.”

- ix. **[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.**

[0142] 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” and can be made using, e.g., “a Bayesian classifier.” Broder, [0057], [0074]. 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. 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].

[0143] 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 a human or a bot. *See* Kitts, [0031]-[0032] (“any indicative **value** may be used” to designate a score that “refer[s] to the probability that a web page request...is initiated from a user or by software attempting to induce click fraud”). *See also* Emigh (EX1016), 26:55-57, which corroborates POSAs’ background knowledge that “a Bayesian...classifier may be used to create a numeric value that corresponds to an estimated likelihood” that the received input belongs to a particular classification being decided upon. In Emigh’s specific case, the classifier is deciding whether a “received message is spam.” Emigh, 26:57. In Broder’s case, the “Bayesian classifier” is deciding whether a received web request is from a “non human web viewer.” Broder, [0074].

[0144] 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* as discussed above in Section VIII.A.5.b (discussing claim 17)). Broder, [0058].

h. 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:

i. [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;

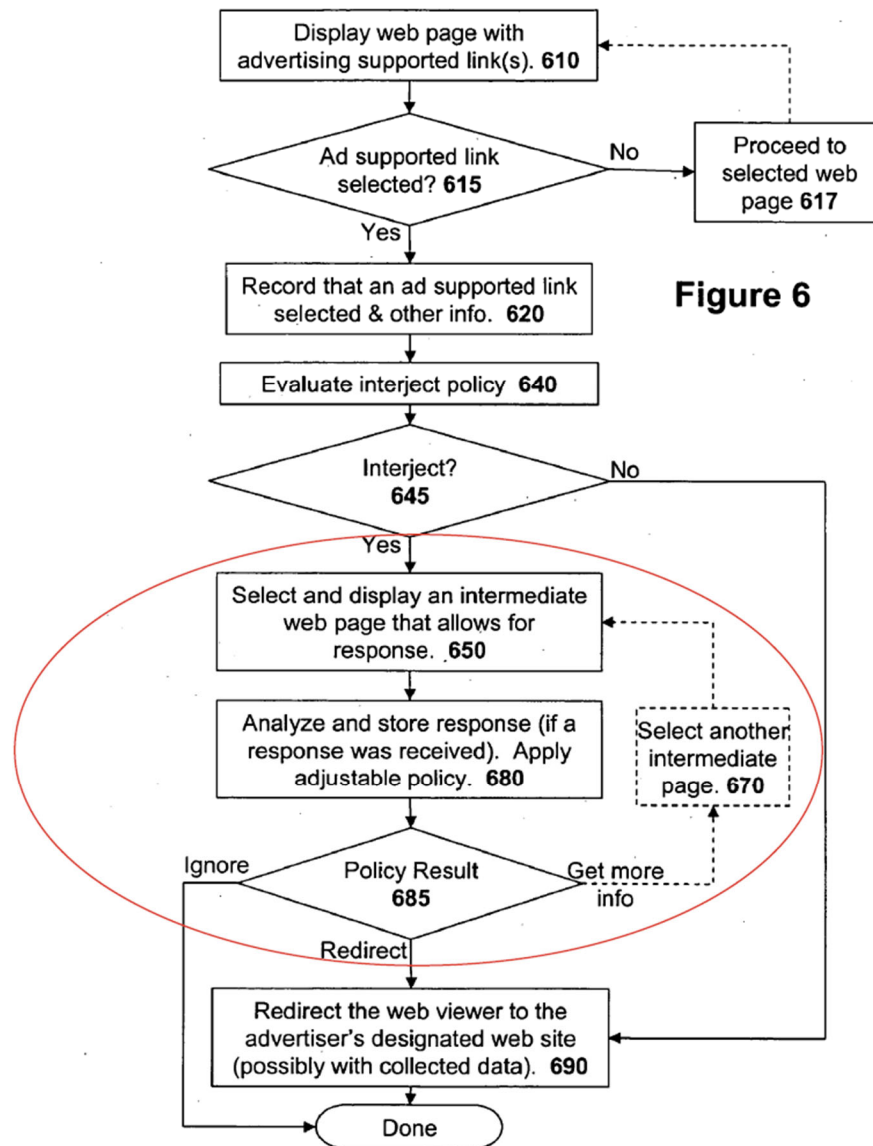
[0145] Broder teaches that, following the analysis and judgment of the client’s response to the first intermediate webpage, “the adjustable policy may request that *additional* information be collected from the web viewer in order to make a more accurate determination of whether the web viewer is a human or non human entity.” Broder, [0059]. POSAs would have known that one situation warranting “a more accurate determination” would be 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]. For additional evidence corroborating POSAs’ background knowledge in this regard, *see* Emigh

(EX1016), 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.

[0146] POSAs also would have had reason to request additional information if the probabilistic judgment is accurate that the client is actually a bot, because requiring the client to provide additional information would slow down the bot. POSAs knew this was beneficial to "slow down the automated program and make it less efficient" at attempting fraud. *See* O'Connell (EX1007), [0049], which is corroborating evidence of this background knowledge. For additional evidence corroborating POSAs' background knowledge in this regard, *see* Meek (EX1008), [0008] ("the effort" of attempting a CAPTCHA "imposes a cost on the computing device [bot]..., either in terms of monetary value, capacity, time, or the like").

[0147] In this scenario where additional information is to be requested after a first intermediate webpage has been presented, Broder teaches that 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):



Broder, Figure 6 (annotated)

[0148] For example, in a scenario where *the second analysis value fails to meet the second analysis predetermined criteria* because the client provided an incorrect response 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 and merely made a mistake on the first CAPTCHA.

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

[0149] Broder teaches “analyzing and storing the web viewer’s response to the newly selected web page,” satisfying claim element [2B]. Broder, [0059].

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

[0150] 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. This *comprises assessing the accuracy of the client computer’s response to the CAPTCHA* in the manner discussed above in Section VIII.A.5.g.viii (discussing claim element [1H]).

- iv. **[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.**

[0151] Broder teaches “*analyzing* and storing the web viewer’s response to the newly selected web page 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 above in Section VIII.A.5.g.ix (discussing claim element [1I]).

- i. **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.**

[0152] As discussed above in Section VIII.A.5.g.iv (discussing claim element [1D]), the Willner-Kitts-Broder combination 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* (e.g., when a high confidence level/factor suggests no click fraud based on analysis of active and passive data).

- j. **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.**

[0153] It would have been obvious to POSAs for the Willner-Kitts-Broder combination *to decrypt the received active data and the received passive data* for the reasons discussed in Section VIII.A.5.d above (discussing claim 19).

- k. **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.**

[0154] The Willner-Kitts-Broder combination's *model data is based on human interaction from a prior session with the same given page* for the reasons discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]).

- l. **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.**

[0155] As discussed above in Section VIII.A.5.a.i (discussing claim element [16A]), Willner's "server...downloads [to the client] *the web page*" that the client *is visiting*, "which may include markup [*data collection data*] that *enables* the cursor tracking," and/or downloads "code (e.g., applets, activeX, Javascript, etc.)" (*data collection data*) 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*. For evidence corroborating POSAs' knowledge in this regard, *see, e.g., Nir (EX1021), [0007]* ("executable code" that "comes as part of a requested Web page" is "typically referred to as an applet" and "typically developed using the Java programming environment"), [0009] ("When the Web page is downloaded to the network browser of the client system the page is appropriately processed by the browser according to the various tags appearing in the body of the Web page. When the browser identifies the APPLET tag within the Web page the downloading of the applet is effected. Subsequently the applet initializes itself and commences running.... . Furthermore when the user closes a Web page the applet's execution is stopped....").

- m. **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.**

[0156] 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 (i.e., the level of suspicion discussed above in Section VIII.A.5.a.v (discussing claim element [16E])).

[0157] 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 (e.g., the threshold probability/confidence/score or similar value for considering the client to be likely human as discussed above in Section VIII.A.5.g.ix (discussing claim element [1I])).

[0158] 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* the discussion of this aspect in Section VIII.A.5.b above (discussing claim 17).

[0159] Therefore, POSAs would have found it obvious based on Broder’s disclosures to implement the Willner-Kitts-Broder combination *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

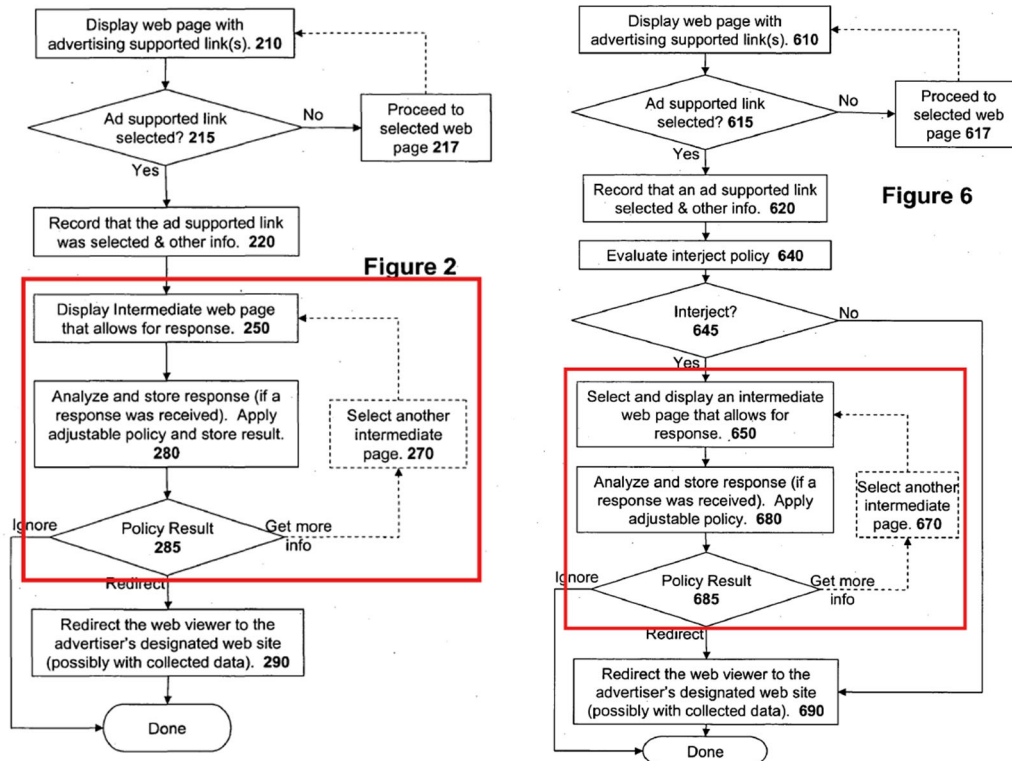
specify a threshold quality score that a page request must have before an advertisement can be displayed.” Kitts, [0060], [0031], [0068], [0071].

- n. **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.**

[0160] Broder further 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 above in Section VIII.A.5.f (discussing claim 21). Broder, [0039]-[0041]. As discussed above in Section VIII.A.5.b (discussing 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*.

[0161] As discussed above in Section VIII.A.5.h.i (discussing claim element [2A]), the Willner-Kitts-Broder combination *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, in which the system can decide to present a third intermediate page after analyzing the response to the second intermediate page, and so on:



Broder, Figs. 2 and 6 (annotated)

[0162] 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 above in Section VIII.A.5.h.i (discussing claim element [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 and merely made initial mistakes.

[0163] Additionally, POSAs would have understood that the choice of how many additional *CAPTCHA tests* to *provide* to a client that has failed a first test would be a design choice, balancing between how much an advertiser wishes to avoid rejecting legitimate human customers who make mistakes versus how much the advertiser wishes to avoid admitting a fraudulent bot that could make a lucky guess if given enough tries. *See, e.g.*, Broder, [0041] (“Annoying web viewers that may be potential customers is clearly not the goal of a web advertiser. However,” advertisers also wish “to filter out all of the accesses by [a] malicious robot program.”). 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. *See* Emigh (EX1016), 20:41-58, corroborating this background knowledge. 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].

- o. 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.**

[0164] Willner's *data collection data* (i.e., the *data collection data* discussed in Section VIII.A.5.a.i above (discussing claim element [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 on the web page displaying the advertisement." Willner, [0054], [0009]-[0011] (cursor tracking performed "by the browser"). Thus, *the data collection data comprises JavaScript code that causes a browser of the client computer to collect the active data.*

- p. 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.**

[0165] The Willner-Kitts-Broder combination satisfies claim 11 for the reasons discussed above in Section VIII.A.5.c (discussing claim 18).

- q. **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.**

[0166] The Willner-Kitts-Broder combination satisfies claim 12 for the reasons discussed above in Sections VIII.A.5.a.iii (discussing claim element [16C]) and VIII.A.5.c (discussing claim 18).

- r. **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.**

[0167] The Willner-Kitts-Broder combination satisfies claim 14 for the reasons discussed above in Section VIII.A.5.a.iii (discussing claim element [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* (i.e., the prior session discussed above in Section VIII.A.5.a.iii (discussing claim element [16C])).

- s. **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:**

[0168] The Willner-Kitts-Broder combination satisfies [22Pre] in the same way it satisfies [16Pre] as discussed above in Section VIII.A.5.a.

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

[0169] See the discussion in Sections VIII.A.5.a.i – VIII.A.5.a.ii above (discussing claim elements [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.

- ii. **[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;**

[0170] The Willner-Kitts-Broder combination *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

above in Sections VIII.A.5.a.i – VIII.A.5.a.ii (discussing claim elements [16A]-[16B]).

[0171] As to the term “*monitored data*” which appears in claim element [22B], the ’014 patent defines “*monitored data*” as “compris[ing] active or passive data, whether available or acquired, obtained from the computing device, or as a result of its external interactions, after the generation of issued data,” where “issued data...comprises data generated by a server or other computing device that is not the same as the computing device for which the assessment as to user status is being performed.” EX1001, 3:43-51. As discussed above in Sections VIII.A.5.a.i – VIII.A.5.a.ii (discussing claim elements [16A]-[16B]), the Willner-Kitts-Broder combination obtains its active data (which is acquired) from the client computing device, and obtains its passive data (which is available) from the client computing device. Both types of data are obtained as a result of the client computing device’s external interactions with the server, after generation of the webpage that the client computing device downloads from the publisher’s server and interacts with. The webpage is generated by the publisher’s server, and the publisher’s server is not the same as the client computing device.

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

[0172] The Willner-Kitts-Broder combination satisfies claim element [22C] for the reasons discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]).

- iv. **[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;**

[0173] As discussed above in Section VIII.A.4 (Discussion of Willner-Kitts-Broder Combination), 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 the Willner-Kitts-Broder combination. Broder, [0042]-[0043]. Exemplary factors to consider include whether “no input is received from the web viewer within a particular time limit,” or whether “a response is received nearly instantaneously.” Broder, [0044]-[0045]. Broder explains that “[i]f no response is received, this may be a non human entity that does not know how to deal with the...page,” and “[i]f a response is received nearly instantaneously then the web viewer may be a computer program since humans generally cannot react instantaneously.” Broder, [0044]-[0045]. Each of these is an example of *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., there has been no cursor movement, or the only input is a response entered much too quickly to have been human).

[0174] While Broder discusses this no-input/instantaneous-input scenario in the context of testing for a response to an intermediate webpage, POSAs would have known that the generic teaching—that a lack of expected input or a nearly instantaneous input can be indicative of a bot—is applicable more generally to testing/analyzing any webpage response. POSAs would have found it obvious to apply this type of analysis also when assessing the client’s interaction with the webpage containing the advertisement (e.g., testing whether the click on the advertisement was too instantaneous to have been made by a human, or occurred without any mouse movement). 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 above in Section VIII.A.5.a.iii (discussing claim element [16C])—because if there is no detected human activity then there would be no vector patterns to analyze. (Or, if any vector patterns were input too

instantaneously, they would not be trusted and would not be appropriate to analyze further.)

- v. **[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**

[0175] The Willner-Kitts-Broder combination *performs* claim element [22E]’s *second level of analyzing* by the analysis of cursor movements and passive data discussed above in Section VIII.A.5.a.iii (discussing the “*first*” analysis in [16C]). (In other words, what is called the *second level of analyzing* in claim element [22E] can be satisfied by the same analysis as what is called the *first* analysis in claim element [16C].) As discussed above in Section VIII.A.5.s.iv (discussing claim element [22D]), this *second level of analyzing* in the Willner-Kitts-Broder combination (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* discussed above for claim element [22D] does not conclude that there has been no input or that an instantaneous click has been received with no cursor movement). For example, if the Willner-Kitts-Broder system concludes in a *first-level analysis* that there has been elapsed time and cursor movement before an advertisement is selected, then

the system performs a *second level of analyzing* on the vector patterns of the cursor movement (as well as passive data).

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

[0176] *The second-level analysis* recited in claim element [22F] is the *second-level analysis* recited in claim element [22E], which can be the same analysis as the “*first*” analysis recited in claim element [16C], as discussed in the section above on [22E].

[0177] In the Willner-Kitts-Broder combination, this analysis *meets a second-level analysis predetermined criteria* when “a high confidence level/factor [is] determined, suggesting no click fraud,” in the analysis of active and passive data discussed above in Section VIII.A.5.a.iii (discussing the “*first*” analysis in claim element [16C]). 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 the Willner-Kitts-Broder combination, the

predetermined criteria also account for passive data, as discussed above in Section VIII.A.5.a.iii (discussing the “*first*” analysis in claim element [16C]).

- t. **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.**

[0178] It would have been obvious to POSAs for the Willner-Kitts-Broder combination *to decrypt the received monitored data* for the reasons discussed in Section VIII.A.5.d above (discussing claim 19).

- u. **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.**

[0179] The Willner-Kitts-Broder combination satisfies claim 24 for the reasons discussed above in Section VIII.A.5.a.iii (discussing claim element [16C]).

- v. **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.**

[0180] The Willner-Kitts-Broder combination satisfies claim 25 for the reasons discussed above in Section VIII.A.5.a.v (discussing claim element [16E]) (with claim 25's *second-level analysis* corresponding to claim 16's *first analysis*).

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

[0181] The Willner-Kitts-Broder combination satisfies claim element [26A] for the reasons discussed above in Section VIII.A.5.e.i (discussing claim element [20A]).

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

[0182] The Willner-Kitts-Broder combination satisfies claim element [26B] for the reasons discussed above in Section VIII.A.5.e.ii (discussing claim element [20B]) (with claim 26's *third-level of analyzing* corresponding to claim 20's *second level of analyzing*).

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

[0183] The Willner-Kitts-Broder combination satisfies claim element [26C] for the reasons discussed above in Section VIII.A.5.e.iii (discussing claim element [20C]) (with claim 26's *third-level analysis value* corresponding to claim 20's *second analysis value*).

x. Claim 27: The non-transitory machine readable medium of claim 26, wherein the request for further data includes a CAPTCHA test.

[0184] The Willner-Kitts-Broder combination satisfies claim 27 for the reasons discussed above in Section VIII.A.5.f (discussing claim 21).

y. 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.

[0185] The Willner-Kitts-Broder combination satisfies claim 28 for the reasons discussed above in Section VIII.A.5.c (discussing claim 18).

z. Claim 29: The non-transitory machine readable medium of claim 28, wherein the received monitored data includes manual device input activity.

[0186] The Willner-Kitts-Broder combination satisfies claim 29 for the reasons discussed above in Section VIII.A.5.c (discussing claim 18).

B. Ground 2: Claims 4, 19, and 23 of the '014 Patent Would Have Been Obvious over Willner in view of Kitts, Broder, and Tanzer

[0187] After reviewing Willner, Kitts, Broder, Tanzer, and claims 4, 19, and 23 of the '014 patent, it is my opinion that each of these claims would have been obvious to a POSA in view of the combined teachings of Willner, Kitts, Broder, and Tanzer. A POSA would have had reasons to combine the collective teachings of these references to result in a combination that meets all limitations of each of claims 4, 19, and 23, and would have reasonably expected success in doing so. In the alternative, to the extent the Board finds that the references do not expressly or inherently disclose certain limitations of these claims, a POSA would have had reasons to implement the teachings of these references in a typical, conventional, and obvious way that meets those limitations, as I discuss in the corresponding sections above and below. The bases for my opinion and the details of my analysis are below.

1. Discussion of Tanzer (EX1012)

[0188] Like Willner, Kitts, and Broder, Tanzer relates to comparing “stored characteristics” of “a user’s behavior on an electronic device” to “the characteristics of a subsequent user” to determine whether “fraud is suspected.” Tanzer, Abstract, [0017] (“capturing user attributes on a system or electronic device and comparing the attributes to corresponding attributes from previously-

recorded data”). Like the Willner-Kitts-Broder combination, Tanzer’s techniques operate in “a client-server computing system” where a “customer...accesses [a server’s] web page through their computers...which are known as clients,” and “[e]ach client’s attributes are captured on their local machine and then uploaded to a server” for analysis, using “client-side scripting” with “JavaScript...executed by the user’s Web client browser” to “capture[] the user activity.” Tanzer, [0020]-[0023], [0041].

[0189] Tanzer monitors and analyzes the same types of active data as the Wilner-Kitts-Broder combination, including “input device dither (slight variations in the path when moving from one point to another on the screen).” Tanzer, [0024], [0025] (“user’s dither in mouse movement”), [0039]. Like Willner, Tanzer teaches to analyze “the difference between the historical [movement data] and the current [movement data],” to detect whether the difference is “so minor as to suggest that a fraud involving copying of behaviors is taking place.” Tanzer, [0033], [0054]. Although Tanzer is interested in whether a specific human’s past movements are being copied while Willner is interested in whether any human’s past movements are being copied, the type of data being monitored (e.g., mouse movement), the way it is monitored (e.g., via browser-downloaded JavaScript), and the use of comparison to previously recorded data are the same. 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 the Willner-Kitts-Broder combination’s analysis of both active and passive data. Tanzer, [0035], [0038] (“A user’s attributes are those attributes associated with the electronic device utilized by the user and his or her behaviors”).

[0190] 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] (“Monitoring software requires some system resources to perform computations (encryption, compression, optimization, etc.) and store the collected data.”).

2. Discussion of Willner-Kitts-Broder-Tanzer Combination

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

3. Mapping of Willner-Kitts-Broder-Tanzer Combination to Claims 4, 19, and 23 of the '014 Patent

[0192] Claims 4 and 19 of the '014 patent each recite “*decrypt[ing] the received active data and the received passive data,*” and claim 23 recites “*decrypt[ing] the received monitored data.*” The above-discussed Willner-Kitts-Broder-Tanzer combination satisfies these recitations because the data are encrypted for transmission to the server, and POSAs would have understood that the server would then *decrypt the received data* to analyze it after receiving it.

C. Ground 3: Claims 9, 15, and 30 of the '014 Patent Would Have Been Obvious over Willner in View of Kitts, Broder, and Meek

[0193] After reviewing Willner, Kitts, Broder, Meek, and claims 9, 15, and 30 of the '014 patent, it is my opinion that each of these claims would have been obvious to a POSA in view of the combined teachings of Willner, Kitts, Broder, and Meek. A POSA would have had reasons to combine the collective teachings of these references to result in a combination that meets all limitations of each of claims 9, 15, and 30, and would have reasonably expected success in doing so. In the alternative, to the extent the Board finds that the references do not expressly or inherently disclose certain limitations of these claims, a POSA would have had reasons to implement the teachings of these references in a typical, conventional, and obvious way that meets those limitations, as I discuss in the

corresponding sections above and below. The bases for my opinion and the details of my analysis are below.

1. Discussion of Meek (EX1008)

[0194] Like Willner, Kitts, and Broder, Meek 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, and not merely the computing device performing programmed 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].

[0195] In this respect, Meek extends upon Willner’s teachings by recognizing that, in addition to mouse cursor movement, “typing on a keyboard” is also suitable active data to monitor to detect human effort in differentiating humans from bots. Meek, [0009], [0026] (“sufficient human effort detected may for example include a keystroke, a mouse click, a minimum number of keystrokes or mouse clicks, a minimum composition time,...etc.”), [0035] (“detected expended human effort, such as for example a number of keystrokes”), [0038]

(“the application...could monitor for substantial keyboard activity and/or mouse activity”), [0045] (“monitored data such as a number of keyboard taps and/or a number of mouse clicks”).

2. Discussion of Willner-Kitts-Broder-Meek Combination

[0196] POSAs would therefore have found it obvious to extend the Willner-Kitts-Broder system to monitor active data including not only mouse cursor activity as taught by Willner, but also keyboard activity as taught by Meek. POSAs would have been motivated to do so by Meek’s above-discussed teachings that monitoring both mouse and keyboard activity are useful in detecting human effort for differentiating humans from bots, in the same context of preventing click fraud that Willner, Kitts, and Broder are directed to. POSAs would have been further motivated by Broder’s teachings to “consider a large number of different factors” in arriving at a “probabilistic” “judgment” of whether the client is a human or a bot, 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].

[0197] POSAs would have reasonably expected success based on Meek’s teachings that both mouse and keyboard activity can be successfully monitored (e.g., via a browser application) and transmitted to the server in

connection with a webpage request (e.g., in the advertising context), and because programming software to do so was well within a POSA's ordinary skill. Meek, [0005] (teaching that the "Human Interactive Proofs" Meek is directed to "are employed" in "prevention of fraudulent click-through in an advertising setting," like Willner-Kitts-Broder's setting), [0009] (teaching to detect "typing on a keyboard, moving a cursor by way of a mouse device, etc.," because "by detecting expending of such passive efforts a Human Interactive Proof need not in fact require the human to expend an active or specific effort in the manner of 'jumping through a hoop'"), [0029] (the "recipient" of the web request and monitored data "is typically an application running on a server," like in Willner-Kitts-Broder), [0037]-[0038] ("a computer browser" is a "sending application" that "could monitor for substantial keyboard activity and/or mouse activity"), [0043] ("all information necessary for the recipient" server to make the human/bot determination can be "include[d]" with the web request sent to the server), [0045] ("the relevant information" sent to the server "likely includes monitored data such as a number of keyboard taps and/or a number of mouse clicks," etc.).

3. Mapping of Willner-Kitts-Broder-Meek Combination to Claims 9, 15, and 30 of the '014 Patent

- a. 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.**

[0198] In the Willner-Kitts-Broder-Meek combination, as discussed in the section just above this one, *the step of analyzing* includes *analyzing mouse and keyboard activity of the client computer*. POSAs knew, for example, that the type of click fraud being detected by Willner, Kitts, Broder, and Meek often occurs on a webpage that presents advertisements together with search results that were returned for a search string that a human would input via *keyboard activity*. Willner, [0046]; Kitts, [0001], [0041]; *see also* Farahat (EX1022), [0003]-[0004]. For example, Willner illustrates an input field 201 for a user to provide a “search term,” and POSAs would have understood this was typically input by keyboard:

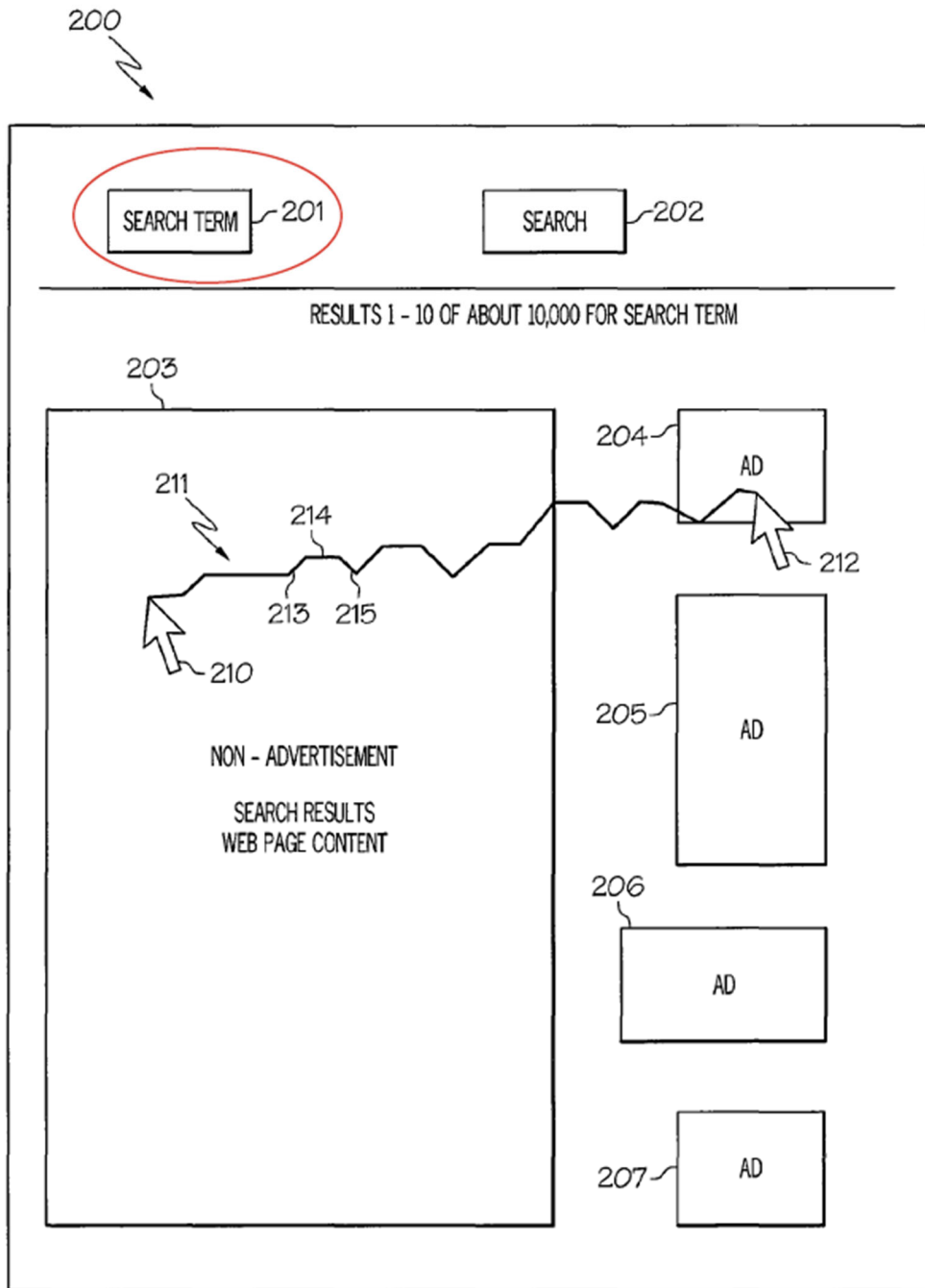


FIG. 2

Willner, FIG. 2 (annotated)

[0199] Thus, in view of 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.

[0200] Additionally, Willner teaches to protect against “an automation tool attempting to simulate the actions of a user” by simply replaying a recorded activity pattern that a human 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 above in Section VIII.A.5.a.iii (discussing claim element [16C]). Willner, [0038], [0051], [0056].

[0201] POSAs knew that the same considerations apply to *keyboard activity*, because a “human is not that consistent in typing” and instead will exhibit “variance among the key space times and key depression times for each letter” being typed, 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. *See* Kroll (EX1010), 8:17-34, which is corroborating evidence of this background knowledge. For further evidence corroborating POSAs’ background knowledge in this regard, *see also* Tanzer (EX1012), [0024] (“key stroke rate and rhythm” are “key elements of [a] user’s behavior” that should differ between users). POSAs would therefore have found it obvious, in *analyzing* the *keyboard activity* in the Willner-Kitts-Broder-Meek combination 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 (as discussed above in Section VIII.A.5.a.iii (discussing claim element[16C])).

- b. 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.**

[0202] The Willner-Kitts-Broder-Meek combination satisfies claim 15 for the reasons discussed above in Section VIII.C.3.a (discussing 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. See Willner, Figure 2 (showing “search term” text field 201 and “ad” click target 204 on same page):

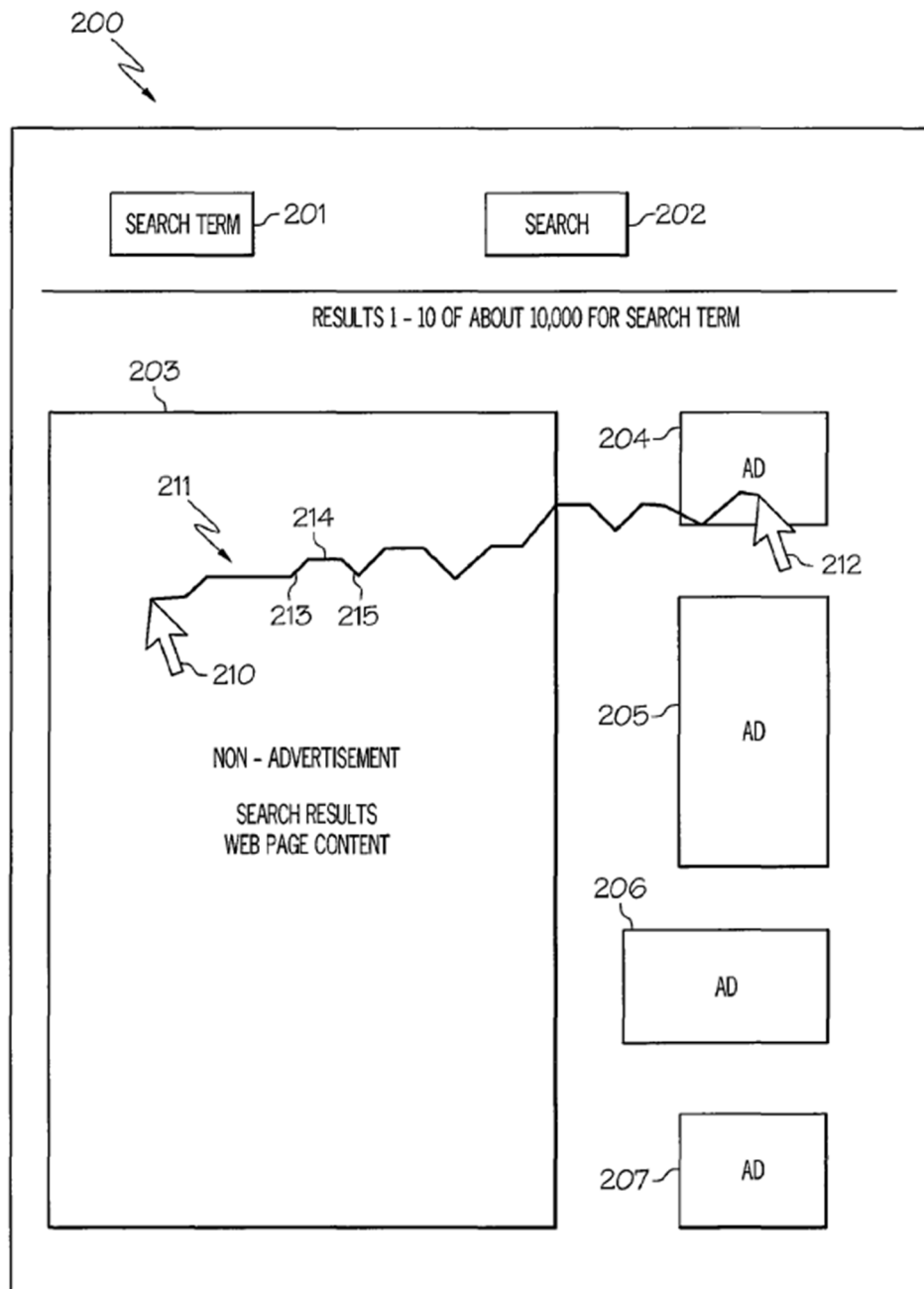


FIG. 2

Willner, FIG. 2

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

c. Claim 30: The non-transitory machine readable medium of claim 29, wherein the manual device input activity comprises mouse movement and key strokes.

[0204] In the Willner-Kitts-Broder-Meek combination, *the manual device input activity comprises mouse movement and key strokes* for the reasons discussed above in Sections VIII.C.2 – VIII.C.3.a (discussing the combination and claim 9).

D. Ground 4: Claim 13 Would Have Been Obvious over Willner in View of Kitts, Broder, and Farahat

[0205] After reviewing Willner, Kitts, Broder, Farahat, and claim 13 of the '014 patent, it is my opinion that claim 13 would have been obvious to a POSA in view of the combined teachings of Willner, Kitts, Broder, and Farahat. A POSA would have had reasons to combine the collective teachings of these references to result in a combination that meets all limitations of claim 13, and would have reasonably expected success in doing so. In the alternative, to the extent the Board finds that the references do not expressly or inherently disclose certain limitations claim 13, a POSA would have had reasons to implement the teachings of these references in a typical, conventional, and obvious way that meets those limitations,

as I discuss in the corresponding sections above and below. The bases for my opinion and the details of my analysis are below.

1. Discussion of Farahat (EX1022)

[0206] Like Willner, Kitts, and Broder, Farahat 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]. An example is illustrated in Farahat’s FIG. 4:



Farahat, FIG. 4

[0207] Farahat explains that an “automated agent may not be able to read text embedded in an image object (i.e., images of text),” whereas a human will see the text and immediately know not to click on the dummy ad. Farahat, [0055]-[0056]. Therefore, if the client selects the dummy ad, it 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] (“[I]f the response consistent of a mouse-click in an inappropriate region, the web viewer may be from a non human entity.”).

2. Discussion of Willner-Kitts-Broder-Farahat Combination

[0208] POSAs would have been motivated by the above-discussed teachings to incorporate a dummy ad like Farahat’s FIG. 4 into one or more of the clickable advertisement locations on Willner’s webpage in the Willner-Kitts-Broder system, 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]. POSAs would have reasonably expected success based on Farahat’s teachings of how to successfully implement such dummy ads in the same context of click-fraud detection in which Willner, Kitts, and Broder operate, and because programming a webpage to display an image of specific text and record any click selecting that image was routine and well within the POSA’s ordinary skill.

3. Mapping of Willner-Kitts-Broder-Farahat Combination to Claim 13 of the ’014 Patent

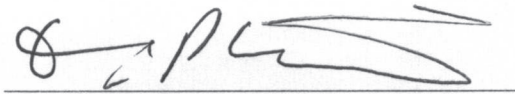
[0209] Claim 13 of the ’014 patent recites, “*The non-transitory machine readable medium of claim 12, wherein the manual device input activity comprises mouse movement over a CAPTCHA test prompt.*” The Willner-Kitts-Broder-Farahat combination discussed above satisfies claim 13. Willner’s techniques monitor the *mouse movement* leading to a click, and in the combination

with Farahat that *mouse movement* can traverse *over* dummy ad 94 to either click on dummy ad 94 (if the client is a bot) or click on the true ad 92 (after passing *over* dummy ad 94, e.g., if the client is human). Because its text tells a human that the dummy ad is testing for bots (“If you click here you are a bot!”—Farahat, FIG. 4), the dummy ad’s text is a *CAPTCHA test prompt*. However, a human user will immediately know to click on the correct advertisement link without having *to decipher a CAPTCHA test* (as recited in [1D]), because the text is a plain instruction telling the human user what (not) to do, with nothing being concealed in any way that would need to be *deciphered*.

I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

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

Dated: July 29, 2026

A handwritten signature in dark ink, appearing to be "J. P. L.", written over a horizontal line.

IX. 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.