

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

NOBOTS LLC,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 1:22-cv-585-ADA

Jury Trial Demanded

GOOGLE'S FIRST AMENDED INVALIDITY AND
SUBJECT-MATTER INELIGIBILITY CONTENTIONS

Deleted: SECOND PRELIMINARY

Nobots LLC - Ex. 2028
IPR2026-00429
Google LLC v. Nobots

TABLE OF CONTENTS

I.	INTRODUCTION	4
A.	Overview of Invalidity Grounds	4
B.	Level of Ordinary Skill in the Art.....	5
C.	Priority Date of the Asserted Patents	5
II.	INVALIDITY CONTENTIONS	7
A.	Anticipation and Obviousness	7
1.	Admitted Prior Art	8
2.	Identification of Prior Art Patents and Patent Publications, Non-Patent Publications, and Systems.....	13
3.	Claim Chart Exhibits.....	52
4.	Exemplary Obviousness Combinations	59
5.	No Evidence of Any Indicia of Non-Obviousness of the Asserted Claims	61
6.	Motivation to Combine Prior Art.....	66
B.	Invalidity Under 35 U.S.C. § 112	95
1.	Lack of Enablement/Written Description Under 35 U.S.C. § 112, ¶ 1.....	95
2.	Invalidity Under 35 U.S.C. § 112, ¶ 2 and/or ¶ 6	116
C.	Double Patenting.....	122
D.	Invalid Patent Term Adjustment.....	130
III.	SUBJECT MATTER ELIGIBILITY CONTENTIONS.....	131
A.	Subject Matter Eligibility Charts	131
B.	Unpatentable Subject Matter Under 35 U.S.C. § 101	132
1.	The '008 patent	133
2.	The '014 patent	145
IV.	ACCOMPANYING DOCUMENT PRODUCTION	151

Deleted: I. INTRODUCTION 4¶

- A. Overview of Invalidity Grounds 4¶
- B. Level of Ordinary Skill in the Art 5¶
- C. Priority Date of the Asserted Patents 6¶
- II. INVALIDITY CONTENTIONS 8¶
- A. Anticipation and Obviousness 8¶
- 1. Admitted Prior Art 9¶
- 2. Identification of Prior Art Patents and Patent Publications, Non-Patent Publications, and Systems 14¶
- 3. Claim Chart Exhibits 53¶
- 4. Exemplary Obviousness Combinations 59¶
- 5. No Evidence of Any Indicia of Non-Obviousness of the Asserted Claims 62¶
- 6. Motivation to Combine Prior Art 66¶
- B. Invalidity Under 35 U.S.C. § 112 95¶
- 1. Lack of Enablement/Written Description Under 35 U.S.C. § 112, ¶ 1 95¶
- 2. Invalidity Under 35 U.S.C. § 112, ¶ 2 and/or ¶ 6 116¶
- C. Double Patenting 122¶
- D. Invalid Patent Term Adjustment 130¶
- III. SUBJECT MATTER ELIGIBILITY CONTENTIONS 130¶
- A. Subject Matter Eligibility Charts 130¶
- B. Unpatentable Subject Matter Under 35 U.S.C. § 101 131¶
- 1. The '008 patent 133¶
- 2. The '014 patent 145¶
- IV. ACCOMPANYING DOCUMENT PRODUCTION 151¶

Pursuant to the operative Scheduling Order (Dkt. 92), on April 15, 2026, Defendant Google LLC (“Google”) served Second Preliminary Invalidity and Subject-Matter Ineligibility Contentions addressing the claims asserted by Plaintiff Nobots LLC from U.S. Patent No. 9,595,008 (the “’008 patent”) and U.S. Patent No. 11,810,014 (the “’014 patent”) (collectively, the “Asserted Patents”) in Plaintiff’s First Amended Infringement Contentions served on February 18, 2026 (“Infringement Contentions”).

Google now provides the following First Amended Invalidity and Subject-Matter Eligibility Contentions (“Invalidity Contentions”). These Invalidity Contentions incorporate two additional contentions regarding why the ’014 patent claims are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1. Pursuant to the Scheduling Order, Google certifies through its undersigned counsel that it undertook reasonable efforts in preparing its original contentions, and that this amendment is based on material identified after service of those contentions, including Plaintiff’s May 6, 2026 letter regarding the scope of its infringement theories.

These Invalidity Contentions address the invalidity and subject-matter ineligibility of the Asserted Claims, identify additional reservations and explanations, and describe the accompanying document production. Google reserves the right to amend or supplement these Invalidity Contentions based on information subsequently identified, including in response to any amendment, supplementation, or clarification of Plaintiff’s Infringement Contentions. Google further reserves the right to supplement these Invalidity Contentions following claim construction and third-party discovery, consistent with Federal Rule of Civil Procedure 26(e), the Court’s Standing Order Governing Proceedings – Patent Cases, and any other applicable rules.

Deleted: current

Deleted: provides these

Deleted: (“Invalidity Contentions”)

Deleted: Plaintiff currently asserts claim 18 of the ’008 patent and claims 1–30 of the ’014 patent (collectively, the “Asserted Claims”).

Deleted: In April 2022, Google filed *inter partes* review (“IPR”) petitions challenging all the claims of the ’008 and U.S. Patent No. 10,423,885 (the “’885 patent”), which Plaintiff had asserted in its original Complaint filed December 13, 2021. In November 2023, the Patent Trial and Appeal Board issued final written decisions, concluding that all 20 claims of the ’885 patent were unpatentable or disclaimed and that 18 of the 20 claims of the ’008 patent were unpatentable. *See* Dkt. 59-2 at 54–55; Dkt. 59-3 at 50–51. Following Google’s appeal as to claim 19 of the ’008 patent, the Federal Circuit held in November 2025 that claim 19 also is unpatentable. As a result of these decisions, Plaintiff has withdrawn from this litigation all 39 claims found unpatentable. ¶ In the First Amended Complaint filed March 5, 2026, Plaintiff newly alleges infringement of claims 1–30 of the ’014 patent and continues to assert claim 18 of the ’008 patent. Google therefore provides the following Invalidity Contentions, which incorporate (1) revised and new Claim Chart Exhibits A-1–A-19 and C for the ’008 patent and new Claim Chart Exhibits E1–E11 and F for the ’014 patent; and (2) additional prior art references relevant to the Asserted Patents.

Deleted: served in 2022

Deleted: the original

Deleted: were served.¹

I. Introduction

A. Overview of Invalidity Grounds

The Asserted Claims of the Asserted Patents are invalid under 35 U.S.C. § 102 and/or § 103 because they are anticipated and/or obvious in view of the prior art and the understanding of a person of ordinary skill in the art at the times of the alleged inventions.² Each of the Asserted Patents discloses and claims concepts that were well known in the prior art. *See* Section II.A (Anticipation and Obviousness), *infra*.

The Asserted Claims also are invalid under 35 U.S.C. § 112 for lack of written description, lack of enablement, indefiniteness, and/or because they do not set forth what the patentee regarded as the invention. *See* Section II.B (Invalidity Under 35 U.S.C. § 112), *infra*.

The Asserted Claims also are invalid because they fail to claim patent-eligible subject matter under 35 U.S.C. § 101. *See* Section III (Subject Matter Eligibility Contentions), *infra*.

Consistent with the Scheduling Order (Dkt. 92), the Court's Standing Order Governing Proceedings – Patent Cases, and any other applicable rules, Google will amend its disclosures herein as appropriate. These disclosures are made based on prior art presently known to Google. Fact discovery in this case has not yet commenced, and the Court has not yet construed the terms of the Asserted Claims, nor has it determined the level of education or experience of one of ordinary skill in the art. Google reserves the right to modify, amend, and/or supplement these Invalidity Contentions in view of, without limitation, information provided by Plaintiff concerning its infringement allegations; discovery concerning the alleged priority, conception, and reduction to practice of any of the Asserted Claims; additional prior art obtained through

² All citations herein to Title 35 of the United States code are to pre-AIA versions of the relevant sections unless otherwise noted.

discovery or further investigation, including without limitation discovery from Plaintiff or third parties; a claim construction order by the Court; positions taken by Plaintiff in this action or any other proceeding, including proceedings before the Patent Trial and Appeal Board; the parties' expert reports; and/or as other circumstances warrant.

B. Level of Ordinary Skill in the Art

A person of ordinary skill in the art, as of the priority date of each Asserted Patent, would have had a bachelor's degree in computer science or a related field with coursework relating to computer science, plus two years' academic and/or industry experience in computer security. More education could substitute for experience, and vice versa.

In its Infringement Contentions, Plaintiff stated that the Asserted Claims are entitled to a priority date of no later than February 17, 2007. Google disputes that Plaintiff has properly shown a conception date of February 17, 2007, that this date is a proper conception date, or that the named inventor conceived of the claimed subject matter as of that date. The level of ordinary skill in the art, however, would not change regardless of whether February 17, 2007, November 19, 2007, or November 19, 2008, is determined to be the relevant date for assessing the level of ordinary skill in the art for the Asserted Patents.

C. Priority Date of the Asserted Patents

Without admitting the validity of any priority date, for the purposes of these Invalidity Contentions, Google uses November 19, 2008, as the priority date for the Asserted Claims of the '008 patent and '014 patent.

The Asserted Claims of the '008 and '014 patents are not entitled to a priority date any earlier than November 19, 2008. While the Asserted Patents claim priority to U.S. Provisional Application No. 61/003,743 (the "'743 application"), filed November 19, 2007, that application did not include certain text that appears in the issued patents, including the text that appears in

the '008 patent at 2:12–25, 2:54–4:8, and 4:15–28 (that is, most of the “Summary of Invention” and “Detailed Description of the Invention” sections that appear in the issued patents).³ The words “value,” “score,” and “confidence level” do not appear in the provisional application, which does not disclose generating any “value,” “score,” or “confidence level” that represents the likelihood that monitored data results from human interaction. The 2007 provisional patent application—like the 2008 non-provisional application discussed below—also did not include any figures. The provisional application therefore lacks support for at least the limitation “generating a value that represents a confidence level . . .” in claim 1 of the '008 patent and its dependent claim 18, and at least the limitation “generate a value indicative of a likelihood . . .” in claim 1 of the '014 patent and its dependent claims and “providing a value indicating a judgment . . .” in claims 16 and 22 of the '014 patent and their dependent claims.

The text that now appears in the '008 patent at 2:12–25, 2:54–4:8, and 4:15–28 was added in non-provisional U.S. Patent Application No. 12/313,502 (the “'502 application”), filed on November 19, 2008.⁴ The new text included a disclosure of “comparing acquired and/or available data relating to the operation of the computing device to suitable models embodying human user derived data (model data),” where this comparison may “yield[] a probability value as to one of the status states, which then may be used by a program administrator of the server to permit or deny access and/or operation to the computing device.” *See* '008 file history, 11/19/2008 Transmittal of New Application at 3; *see also* '008 patent at 2:12–26. In addition, the as-filed non-provisional application added a single patent claim that recited “[a] method for assessing the likely user status of a computing device interacting with a server where computing

³ The '008 and '014 patents share a specification. For simplicity’s sake, the citations in this document are to the '008 patent unless otherwise noted.

⁴ The '502 application also deleted some text that was included in the provisional application.

device is in bi-directional operative communication with the server comprising . . . generating a value that represents the likelihood that the monitored data results from human interaction with or in response to the issued data.” ’502 file history, 11/19/2008 Transmittal of New Application at 8.

In addition, the as-filed ’502 application did not describe a “confidence level” that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application. The language “confidence level” was first added to the application in a proposed amendment to claim 1 of the ’502 application that was filed several years later on August 18, 2015.

Because all the Asserted Claims of the ’008 and ’014 patents recite subject matter that was absent from the non-provisional application and first described in the specification of the ’502 application, a person of ordinary skill would have understood that those claims are not entitled to a priority date any earlier than November 19, 2008.

II. Invalidity Contentions

A. Anticipation and Obviousness

Google contends that all the Asserted Claims are invalid as anticipated and/or obvious under 35 U.S.C. §§ 102 and/or 103. Google relies on and incorporates all prior art references cited on the cover of the Asserted Patents, in the prosecution histories of the Asserted Patents, and in the prosecution histories of other patents and patent applications that are in the same family and/or related by subject matter to the Asserted Patents, including for supporting the obviousness of any asserted claim. Google further relies on and incorporates by reference, as if originally set forth herein, all invalidity positions, and all associated prior art and claim charts, disclosed to Plaintiff by present or former defendants in any lawsuits or other proceedings or by potential or actual licensees to any of the Asserted Claims, including all documents filed in IPR

proceedings IPR2022-00940 and IPR2022-00941. Google hereby discloses and identifies as if originally set forth herein, all prior art references listed and/or asserted in the above as invalidating prior art against each of the Asserted Claims. In addition, Google identifies prior art patents, publications, products, and systems that disclose the elements of the Asserted Claims explicitly, inherently, or as part of an obvious combination, and such references also may be relied on to show the state of the art in the relevant timeframes and/or reasons or motivations to combine prior art references.

In addition, Google reserves the right to assert invalidity under 35 U.S.C. § 102(c) or (d) to the extent that discovery or further investigation yield information forming the basis for such invalidity. Google further reserves the right to assert that any or all of the Asserted Patents are invalid pursuant to § 102(f) and/or § 102(g)(2) on additional grounds if it obtains evidence during discovery that the named inventor of the Asserted Patents did not invent, or did not first invent, the subject matter claimed in the patents. Google further reserves the right to assert that any or all of the Asserted Patents are unenforceable due to prosecution laches and/or inequitable conduct after further discovery.

Further, in those instances in which Google asserts that an Asserted Claim is invalid under 35 U.S.C. § 112, Google has applied the prior art in accordance with its assumption that Plaintiff contends such Asserted Claim (1) has sufficient supporting written description, (2) is enabled, (3) is not indefinite, and (4) sets forth what the inventors regarded as the invention. Google's Invalidity Contentions should not be construed as an admission that any Asserted Claim meets the requirements of § 112.

1. Admitted Prior Art

The Asserted Patents themselves, including in their specifications, also contain statements admitting that certain limitations were already known in the art at the time of the

purported inventions. Such “[a]dmissions in the specification regarding the prior art are binding on the patentee for purposes of a later inquiry into obviousness.” *PharmaStem Therapeutics, Inc. v. ViaCell, Inc.*, 491 F.3d 1342, 1362 (Fed. Cir. 2007);⁵ *see also Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1570 (Fed. Cir. 1988) (“A statement in a patent that something is in the prior art is binding on the applicant and patentee for determinations of anticipation and obviousness.”). The patent applicant also admitted during prosecution that certain limitations were already known in the art at the time of the purported inventions.

The following list of examples of admitted prior art for purposes of one or more of the Asserted Patents is illustrative and not exhaustive. Google further intends to rely on admissions by Plaintiff, the named inventor, and their agents concerning the scope of the claims and prior art relevant to the Asserted Patents found in, *inter alia*, the prosecution history for the Asserted Patents and related patents and/or patent applications; statements made by Plaintiff at any hearings; any deposition testimony of Plaintiff, the named inventor, or their agents; and the papers filed and any evidence submitted by Plaintiff in connection with this litigation or related proceedings before the U.S. Patent and Trademark Office.

- Methods for differentiating between human and bot activity:
 - “In an effort to block these bots, builders of web sites have created a variety of tests to determine if the user is a bot or if the user is a human. Initial efforts required a user to simply enter an alphanumeric string into an input field.” ’008 patent at 1:14–17.
 - “Carnegie Mellon University coined the term ‘CAPTCHA’ (Completely Automated Public Turing test to tell Computers and Humans Apart) for these

⁵ Citations and internal quotation marks omitted unless otherwise noted.

types of tests. A common type of CAPTCHA requires that the user type the letters, digits or characters of a distorted image appearing on the screen. The objective is to create an image that a bot cannot easily parse but that is discernable by a human.” *Id.* 1:22–28.

- “The result of the foregoing is that while CAPTCHAs are becoming increasingly more difficult for bots, they are also becoming more difficult and/or burdensome for human users. In certain instances, the desire to defeat the bots has resulted in images that are so distorted that some human users cannot decipher the images. This is particularly true with users having a visual deficiency or imparity. As a partial solution to this escalation of perception difficulty, some web sites have begun adding a link to a sound file that will speak the characters, but these sound files are also being drastically distorted to protect against being discerned by bots through speech pattern matching algorithms. Other web sites like Facebook.com, have gone so far as to adopt a practice requiring deciphering two distorted word images to increase the complexity for bots.” *Id.* 1:37–51.
- “Current CAPTCHA technology is visual or auditory in nature, requiring the human user to answer a test that should be simple to most humans but difficult for non-humans, e.g., bots. Visual CAPTCHA using distorted images is widely used as the primary test by nearly every top Internet site including Yahoo, Google, YouTube, Microsoft’s Live ID, MySpace, Facebook, Wikipedia, Craigs List. By using solely visual testing criteria, nearly all users will be able to invoke the requested action; not all users have functioning audio equipment or environments such as libraries may not permit such use.” *Id.* 1:54–64.

- “Carnegie Mellon University estimates that 60 million CAPTCHA tests are deciphered every day and with an average time spent of 10 seconds, requiring a total of 150,000 hours of work spent every day trying to protect web sites from bots.” *Id.* 2:1–5.
- “The reader is directed to a very good analysis of the needs and issues related to CAPTCHA at w3.org.” ’743 application at 2.
- “While current CAPTCHA tests are based on discerning visual and/or auditory cues, embodiments of the invention are based on biometric analysis of a user’s actions.” ’743 application at 2.
- Methods for defeating tests used to determine whether a user trying to access computer resources or a website is a human or a bot:
 - “[A]s character recognition engines became more available, such ‘tests’ became easily defeated. What was needed was a more robust form of test—one that couldn’t be easily defeated.” ’008 patent at 1:17–21.
 - “Such efforts have been successful in preventing non-adaptive software from recognizing the imaged characters, but people intent on abusing these sites have designed ways to circumvent the CAPTCHA, such as through specially tuned character recognition programs. A brief survey of the Internet will reveal many resources that describe how to tune and/or use character recognition to decipher CAPTCHA including aiCaptcha, Simon Fraser University and PWNtcha.” *Id.* 1:28–36.

- Conventional computer technology for the collection and use of information regarding a computing device user’s interactions with the computing device or the computing environment:
 - “Such model 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. Generally, such data must be monitored and stored 210, 220 by a program operative on the computing device, which makes the data available to another program, preferably on a server 320, or actively transmits such data to a server.” *Id.* 2:64–3:9.
 - “Passive model data comprises data available from a computing device user’s interactions therewith and within the computing environment where such data is normally stored (logged) or transmitted to a remote location. Such model 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.” *Id.* 3:9–17.
 - “Such monitoring and retaining means for acquiring data from the computing device comprises, without limitation, modification of (an) existing program(s) (e.g., such means are included in available browsers), a covert program (e.g., many malware applications log keystrokes and periodically pass them to remote

servers for malicious purposes; similar technology can be used to exploit necessary aspects of the invention embodiments), or a servlet/Java applet. If user privacy is a concern, the monitoring and retaining means can remain dormant until activated by, for example, an enabled web site 110.” *Id.* 4:6–17.

- “From the foregoing, it can be seen that implementation of the invention embodiments can be accomplished exclusively from the server side; it is not necessary to distribute or install in the conventional sense client side software. Existing available browsers and operating systems provide the means necessary to temporarily install logging code, if such is elected.” *Id.* 4:29–35.
- Encrypting and decrypting data, including for privacy or security purposes.
 - “The monitoring and retaining means may also enable transmission of some or all retained data 410, in encrypted or unencrypted form, as may be desired for privacy and security purposes.” *Id.* 4:18-21.

2. **Identification of Prior Art Patents and Patent Publications, Non-Patent Publications, and Systems**

Subject to its reservation of rights, Google identifies below each item of prior art that anticipates or renders obvious one or more the Asserted Claims in Tables 1, 2, or 3 below. Table 1 provides the identity of each prior art patent by its number, country of origin, and data of issuance. Table 2 provides the identity of each non-patent prior art publication including, where possible, its title, date of publication, author, and publisher. Table 3 provides the identity of each system or product that was the subject of a prior art sale or public disclosure under 35 U.S.C. § 102(b) including, where possible, the name of the item that was offered for sale or publicly used or the information known, the date the offer or use took place or the information became known, and the identity of the person or entity that made the use or that made and received the

offer, or the person or entity that made the information known or to whom it was made known. The identified prior art also qualifies as prior art under 35 U.S.C. § 102(a). Prior art patents and patent publications filed in or designating the United States additionally qualify as prior art under 35 U.S.C. § 102(e). In addition, Tables 1–2 further include references that may be relied upon to show the state of the art at the time and/or inherency regardless of whether the references themselves qualify as prior art.

Discovery is ongoing, and Google expects relevant discovery to be obtained from Plaintiff and third parties. Google’s prior art investigation, therefore, is not yet complete. As a result, Google reserves the right to present additional items of prior art under 35 U.S.C. § 102 or § 103 located through discovery. Google specifically reserves the right to supplement these Invalidity Contentions with information obtained through discovery of these third parties.

Table 1: Prior Art Patents / Patent Publications

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2008/0086524 A1	Aug. 17, 2007	Apr. 10, 2008	Afergan	GOOG- NOBOTS- PA- 00000001
U.S. Patent No. 7089241	Dec. 22, 2003	Aug. 8, 2006	Alspector	GOOG- NOBOTS- PA- 00000019
U.S. Patent App. Pub. No. 2010/0070620 A1	Sept. 16, 2008	Mar. 18, 2010	Awadallah I	GOOG- NOBOTS- PA- 00000052
U.S. Patent App. Pub. No. 2009/0094311 A1	Oct. 4, 2007	Apr. 9, 2009	Awadallah II	GOOG- NOBOTS- PA- 00000041

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent No. 8280993	Oct. 4, 2007	Oct. 2, 2012	Awadallah III	GOOG- NOBOTS- PA- 00000065
U.S. Patent App. Pub. No. 2007/0165911 A1	Dec. 22, 2006	July 19, 2007	Baentsch	GOOG- NOBOTS- PA- 00000076
U.S. Provisional Application No. 61041556 (published as US Patent App. Pub. No. 20110029902 A1)	Apr. 1, 2008	Feb. 3, 2011	Bailey I	GOOG- NOBOTS- PA- 00000092
U.S. Patent App. Pub. No. 2011/0029902 A1	Mar. 31, 2009	Feb. 3, 2011	Bailey II	GOOG- NOBOTS- PA- 00000119
U.S. Patent No. 7917508	Aug. 31, 2007	Mar. 29, 2011	Baluja	GOOG- NOBOTS- PA- 00000160
U.S. Patent App. Pub. No. 2007/0106737 A1	Nov. 10, 2005	May 10, 2007	Barnes	GOOG- NOBOTS- PA- 00000174
U.S. Patent No. 7945952	June 30, 2005	May 17, 2011	Behforooz	GOOG- NOBOTS- PA- 00000181
U.S. Patent App. Pub. No. 2007/0016689 A1	July 14, 2006	Jan. 18, 2007	Birch	GOOG- NOBOTS- PA- 00000197
U.S. Patent App. Pub. No. 2008/0147456 A1	Dec. 19, 2006	June 19, 2008	Broder 456	GOOG- NOBOTS- PA- 00000214
U.S. Patent App. Pub. No. 2005/0015257 A1	July 14, 2003	Jan. 20, 2005	Bronstein	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00000227
U.S. Patent No. 9208461	Apr. 17, 2014	Dec. 8, 2015	Busa	GOOG- NOBOTS- PA- 00000233
U.S. Patent No. 8824659	July 3, 2013	Sept. 2, 2014	Bushey I	GOOG- NOBOTS- PA- 00000279
U.S. Patent No. 9088652	July 1, 2014	July 21, 2015	Bushey II	GOOG- NOBOTS- PA- 00000294
U.S. Patent No. 7606915	Feb. 25, 2003	Oct. 20, 2009	Calinov	GOOG- NOBOTS- PA- 00000308
U.S. Patent App. Pub. No. 2010/0037147 A1	Aug. 5, 2008	Feb. 11, 2010	Champion	GOOG- NOBOTS- PA- 00000328
U.S. Patent No. 7657849	Dec. 23, 2005	Feb. 2, 2010	Chaudhri	GOOG- NOBOTS- PA- 00000340
U.S. Patent App. Pub. No. 2011/0113388 A1	Jan. 18, 2011	May 12, 2011	Eisen I	GOOG- NOBOTS- PA- 00000390
U.S. Provisional Application No. 61047071 (published as US Patent App. Pub. No. 20110113388 A1)	Apr. 22, 2008	May 12, 2011	Eisen II	GOOG- NOBOTS- PA- 00000371
PCT Pub. No. WO2007/090605 A1	Feb. 6, 2006	Aug. 16, 2007	Eldon I	GOOG- NOBOTS- PA- 00000419

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2009/0307028 A1	Feb. 6, 2007	Dec. 10, 2009	Eldon II	GOOG- NOBOTS- PA- 00000402
U.S. Patent No. 8838570	Nov. 6, 2006	Sept. 16, 2014	English	GOOG- NOBOTS- PA- 00000492
U.S. Patent No. 9047458	May 20, 2010	June 2, 2015	Etchegoyen	GOOG- NOBOTS- PA- 00000502
U.S. Patent App. Pub. No. 2005/0198158 A1	Mar. 8, 2004	Sept. 8, 2005	Fabre	GOOG- NOBOTS- PA- 00000519
U.S. Patent App. Pub. No. 2005/0144067 A1	Dec. 19, 2003	June 30, 2005	Farahat	GOOG- NOBOTS- PA- 00000549
U.S. Patent No. 7506170	May 28, 2004	Mar. 17, 2009	Finnegan	GOOG- NOBOTS- PA- 00000566
U.S. Patent App. Pub. No. 2009/0150986 A1	Dec. 5, 2007	June 11, 2009	Foreman	GOOG- NOBOTS- PA- 00000578
U.S. Patent No. 8510795	Sept. 4, 2007	Aug. 13, 2013	Gargi	GOOG- NOBOTS- PA- 00000592
U.S. Patent App. Pub. No. 2007/0255821 A1	May 1, 2006	Nov. 1, 2007	Ge	GOOG- NOBOTS- PA- 00000606
U.S. Patent App. Pub. No. 2007/0192849 A1	Feb. 10, 2006	Aug. 16, 2007	Golle I	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00000622
U.S. Patent No. 7721107	Feb. 10, 2006	May 18, 2010	Golle II	GOOG- NOBOTS- PA- 00000633
U.S. Patent App. Pub. No. 2005/0066201 A1	Sept. 23, 2003	Mar. 24, 2005	Goodman	GOOG- NOBOTS- PA- 00000646
U.S. Patent App. Pub. No. 2008/0288303 A1	Mar. 19, 2007	Nov. 20, 2008	Gray	GOOG- NOBOTS- PA- 00000670
U.S. Patent App. Pub. No. 2007/0038568 A1	Apr. 26, 2006	Feb. 15, 2007	Greene	GOOG- NOBOTS- PA- 00000681
U.S. Patent No. 8056129	Apr. 19, 2007	Nov. 8, 2011	Gusler I	GOOG- NOBOTS- PA- 00000713
U.S. Patent App. Pub. No. 2008/0263636 A1	Apr. 19, 2007	Oct. 23, 2008	Gusler II	GOOG- NOBOTS- PA- 00000703
U.S. Patent No. 8032483	June 29, 2005	Oct. 4, 2011	Haveliwala	GOOG- NOBOTS- PA- 00000728
U.S. Patent No. 8775235	Mar. 8, 2010	July 8, 2014	Hedley I	GOOG- NOBOTS- PA- 00000752
U.S. Patent No. 8775236	May 31, 2013	July 8, 2014	Hedley II	GOOG- NOBOTS- PA- 00000800

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent No. 9240078	Sept. 12, 2013	Jan. 19, 2016	Hedley III	GOOG- NOBOTS- PA- 00000830
U.S. Patent App. Pub. No. 2005/0008148 A1	Apr. 1, 2004	Jan. 13, 2005	Jacobson	GOOG- NOBOTS- PA- 00000878
U.S. Patent App. Pub. No. 2008/0162227 A1	Dec. 5, 2007	July 3, 2008	Jakobsson	GOOG- NOBOTS- PA- 00000897
Japanese Patent Application No. JP2007213409A EP Translation	Feb. 10, 2006	Aug. 23, 2007	Kitagawa English	GOOG- NOBOTS- PA- 00000907
Japanese Patent Application No. JP2007213409A	Feb. 10, 2006	Aug. 23, 2007	Kitagawa Japanese	GOOG- NOBOTS- PA- 00000910
U.S. Patent App. Pub. No. 2008/0114624 A1	Nov. 13, 2006	May 15, 2008	Kitts I	GOOG- NOBOTS- PA- 00000917
U.S. Patent App. Pub. No. 2008/0281606 A1	May 7, 2007	Nov. 13, 2008	Kitts II	GOOG- NOBOTS- PA- 00000934
U.S. Patent App. Pub. No. 2008/0049969 A1	Dec. 18, 2006	Feb. 28, 2008	Koziol	GOOG- NOBOTS- PA- 00000957
U.S. Patent No. 6405922	May 15, 2000	June 18, 2002	Kroll	GOOG- NOBOTS- PA- 00000983
U.S. Patent No. 8413250	June 5, 2008	Apr. 2, 2013	Krynski	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00001001
U.S. Patent App. Pub. No. 2013/0019290 A1	Sept. 10, 2012	Jan. 17, 2013	Lee I	GOOG- NOBOTS- PA- 00001013
U.S. Patent No. 8713657	Sept. 10, 2012	Apr. 29, 2014	Lee II	GOOG- NOBOTS- PA- 00001035
U.S. Patent App. Pub. No. 2008/0040653 A1	Aug. 14, 2006	Feb. 14, 2008	Levine	GOOG- NOBOTS- PA- 00001058
U.S. Patent No. 8793135	Aug. 25, 2008	July 29, 2014	Lewis	GOOG- NOBOTS- PA- 00001074
U.S. Patent No. 6195698	Apr. 13, 1998	Feb. 27, 2001	Lillibridge	GOOG- NOBOTS- PA- 00001086
U.S. Patent App. Pub. No. 2006/0136294 A1	Oct. 26, 2005	June 22, 2006	Linden	GOOG- NOBOTS- PA- 00001104
U.S. Patent App. Pub. No. 2007/0250920 A1	Apr. 23, 2007	Oct. 25, 2007	Lindsay	GOOG- NOBOTS- PA- 00001115
U.S. Provisional Application No. 60891042 (published as US Patent App. Pub. No. 20090055193 A1)	Feb. 22, 2007	Feb. 26, 2009	Maislos I	GOOG- NOBOTS- PA- 00001186
U.S. Patent App. Pub. No. 2009/0055193 A1	Feb. 21, 2008	Feb. 26, 2009	Maislos II	GOOG- NOBOTS- PA- 00001193

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2007/0300077 A1	June 26, 2006	Dec. 27, 2007	Mani	GOOG- NOBOTS- PA- 00001206
U.S. Patent App. Pub. No. 2007/0259716 A1	July 6, 2007	Nov. 8, 2007	Mattice I	GOOG- NOBOTS- PA- 00001219
U.S. Patent No. 8684839	July 6, 2007	Apr. 1, 2014	Mattice II	GOOG- NOBOTS- PA- 00001277
U.S. Patent App. Pub. No. 2008/0091453 A1	July 11, 2007	Apr. 17, 2008	Meehan	GOOG- NOBOTS- PA- 00001335
U.S. Patent App. Pub. No. 2005/0278253 A1	June 15, 2004	Dec. 15, 2005	Meek	GOOG- NOBOTS- PA- 00001363
U.S. Patent App. Pub. No. 2008/0066014 A1	Sept. 13, 2007	Mar. 13, 2008	Misra	GOOG- NOBOTS- PA- 00001377
U.S. Patent No. 8903052	Mar. 15, 2013	Dec. 2, 2014	Moore	GOOG- NOBOTS- PA- 00001397
U.S. Patent No. 7373524	Feb. 24, 2004	Aug. 25, 2005	Motsinger	GOOG- NOBOTS- PA- 00001404
U.S. Patent App. Pub. No. 2007/0239604 A1	Apr. 10, 2006	Oct. 11, 2007	O'Connell I	GOOG- NOBOTS- PA- 00001536
U.S. Patent App. Pub. No. 2007/0240230 A1	Apr. 10, 2006	Oct. 11, 2007	O'Connell II	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00001554
U.S. Patent No. 6460141	Oct. 28, 1998	Oct. 1, 2002	Olden	GOOG- NOBOTS- PA- 00001572
U.S. Patent App. Pub. No. 2008/0319774 A1	June 22, 2007	Dec. 25, 2008	O'Sullivan I	GOOG- NOBOTS- PA- 00001636
U.S. Patent App. Pub. No. 2008/0162200 A1	Dec. 28, 2006	July 3, 2008	O'Sullivan II	GOOG- NOBOTS- PA- 00001625
U.S. Patent No. 7680891	June 19, 2006	Mar. 16, 2010	Pongsajapan	GOOG- NOBOTS- PA- 00001652
U.S. Patent App. Pub. No. 2009/0249477 A1	Mar. 28, 2008	Oct. 1, 2009	Punera	GOOG- NOBOTS- PA- 00001667
U.S. Patent App. Pub. No. 2008/0127302 A1	Aug. 22, 2006	May 29, 2008	Qvarfordt I	GOOG- NOBOTS- PA- 00001689
U.S. Patent No. 8601538	Aug. 22, 2006	Dec. 3, 2013	Qvarfordt II	GOOG- NOBOTS- PA- 00001698
U.S. Provisional Application No. 61029701 (published as US Patent App. Pub. No. 20090241174 A1)	Feb. 19, 2008	Sept. 24, 2009	Rajan I	GOOG- NOBOTS- PA- 00001708
U.S. Patent App. Pub. No. 2009/0241174 A1	Feb. 19, 2009	Sept. 24, 2009	Rajan II	GOOG- NOBOTS- PA- 00001738

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2009/0044264 A1	Aug. 7, 2007	Feb. 12, 2009	Ramanathan	GOOG- NOBOTS- PA- 00001753
U.S. Patent App. Pub. No. 2006/0015390 A1	Nov. 3, 2004	Jan. 19, 2006	Rijsinghani	GOOG- NOBOTS- PA- 00001774
U.S. Patent App. Pub. No. 2007/0018393 A1	June 29, 2006	Jan. 25, 2007	Ritter	GOOG- NOBOTS- PA- 00001786
U.S. Patent No. 7917491	Jan. 30, 2006	Mar. 29, 2011	Sack	GOOG- NOBOTS- PA- 00001809
U.S. Patent App. Pub. No. 2009/0113294 A1	Oct. 30, 2007	Apr. 30, 2009	Sanghavi	GOOG- NOBOTS- PA- 00001818
U.S. Patent No. 8694244	July 9, 2013	Apr. 8, 2014	Schalk I	GOOG- NOBOTS- PA- 00001834
U.S. Patent No. 8700259	Mar. 15, 2013	Apr. 15, 2014	Schalk II	GOOG- NOBOTS- PA- 00001852
U.S. Patent No. 8706405	June 4, 2013	Apr. 22, 2014	Schalk III	GOOG- NOBOTS- PA- 00001870
U.S. Patent No. 8738287	June 3, 2013	May 27, 2014	Schalk IV	GOOG- NOBOTS- PA- 00001887
U.S. Patent No. 8825379	May 24, 2013	Sept. 2, 2014	Schalk V	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00001903
U.S. Patent No. 5933498	Nov. 5, 1997	Aug. 3, 1999	Schneck	GOOG- NOBOTS- PA- 00001918
U.S. Patent No. 8214891	Mar. 26, 2008	July 3, 2012	Seacat	GOOG- NOBOTS- PA- 00001969
U.S. Patent No. 7516220	May 15, 2008	Apr. 7, 2009	Stiert	GOOG- NOBOTS- PA- 00001986
U.S. Patent App. Pub. No. 2008/0225870 A1	Mar. 15, 2007	Sept. 18, 2008	Sundstrom	GOOG- NOBOTS- PA- 00001999
U.S. Patent App. Pub. No. 2007/0255818 A1	Apr. 29, 2006	Nov. 1, 2007	Tanzer	GOOG- NOBOTS- PA- 00002016
U.S. Patent No. 9152381	Nov. 10, 2008	Oct. 6, 2015	Valentino	GOOG- NOBOTS- PA- 00002033
U.S. Patent App. Pub. No. 2009/0197815 A1	June 6, 2007	Aug. 6, 2009	Vincenzi	GOOG- NOBOTS- PA- 00002108
U.S. Patent No. 7785180	July 14, 2006	Aug. 31, 2010	von Ahn VII	GOOG- NOBOTS- PA- 00002125
U.S. Patent No. 7980953	June 24, 2004	July 19, 2011	von Ahn VIII	GOOG- NOBOTS- PA- 00002115

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2007/0192419 A1	Feb. 14, 2006	Aug. 16, 2007	Vuong	GOOG- NOBOTS- PA- 00002151
U.S. Patent App. Pub. No. 2007/0201745 A1	Jan. 30, 2007	Aug. 30, 2007	Wang	GOOG- NOBOTS- PA- 00002159
U.S. Patent No. 7877707	June 13, 2007	Jan. 25, 2011	Westerman	GOOG- NOBOTS- PA- 00002169
U.S. Patent No. 8353764	Nov. 9, 2007	Jan. 15, 2013	Williams	GOOG- NOBOTS- PA- 00002232
U.S. Patent No. 8938395	July 16, 2007	Jan. 20, 2015	Willner I	GOOG- NOBOTS- PA- 00002292
U.S. Patent App. Pub. No. 2009/0024971 A1	July 16, 2007	Jan. 22, 2009	Willner II	GOOG- NOBOTS- PA- 00002276
U.S. Patent App. Pub. No. 2009/0320123 A1	June 20, 2008	Dec. 24, 2009	Yu	GOOG- NOBOTS- PA- 00002312
U.S. Patent No. 8682718	Dec. 14, 2011	Mar. 25, 2014	Zwicky	GOOG- NOBOTS- PA- 00002346
U.S. Patent No. 5375244	May 29, 1992	Dec. 20, 1994	McNair 244	GOOG- NOBOTS- PA- 00015053
U.S. Patent No. 7860870	May 31, 2007	Dec. 28, 2010	Sadagopan 870	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA- 00015124
U.S. Patent No. 7895653	May 31, 2007	Feb. 22, 2011	Calo 653	GOOG- NOBOTS- PA- 00014893
U.S. Patent No. 7908645	Apr. 28, 2006	Mar. 15, 2011	Varghese 645	GOOG- NOBOTS- PA- 00015196
U.S. Patent App. Pub. No. 2004/0215980	May 19, 2004	Oct. 28, 2004	Hamid 980	GOOG- NOBOTS- PA- 00014981
U.S. Patent App. Pub. No. 2005/0097320	Sept. 13, 2004	May 5, 2005	Golan 320	GOOG- NOBOTS- PA- 00014964
U.S. Patent App. Pub. No. 2005/0114705	Mar. 1, 2004	May 26, 2005	Reshef 705	GOOG- NOBOTS- PA- 00015102
U.S. Patent App. Pub. No. 2006/0195328	Feb. 15, 2005	Aug. 31, 2006	Abraham 328	GOOG- NOBOTS- PA- 00014858
U.S. Patent App. Pub. No. 2007/0074169	Aug. 25, 2006	Mar. 29, 2007	Chess 169	GOOG- NOBOTS- PA- 00014902
U.S. Patent App. Pub. No. 2007/0234409	Mar. 30, 2007	Oct 4, 2007	Eisen 409	GOOG- NOBOTS- PA- 00014954
U.S. Patent App. Pub. No. 2007/0271466	May 11, 2007	Nov. 22, 2007	Mak 466	GOOG- NOBOTS- PA- 00015019

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
U.S. Patent App. Pub. No. 2008/0004107	Jul. 3, 2006	Jan. 3, 2008	Nguyen 107	GOOG- NOBOTS- PA- 00015069
U.S. Patent App. Pub. No. 2008/0084975	Jan. 5, 2007	Apr. 10, 2008	Schwartz 975	GOOG- NOBOTS- PA- 00015149
U.S. Patent App. Pub. No. 2008/0113787	Nov. 15, 2006	May 15, 2008	Alderucci 787	GOOG- NOBOTS- PA- 00014867
U.S. Patent App. Pub. No. 2008/0162338	Dec. 30, 2006	Jul. 3, 2008	Samuels 338	GOOG- NOBOTS- PA- 00015134
U.S. Patent App. Pub. No. 2008/0222706	Mar. 6, 2007	Sept. 11, 2008	Renaud 706	GOOG- NOBOTS- PA- 00015089
U.S. Patent App. Pub. No. 2008/0301808	May 31, 2007	Dec. 4, 2008	Calo 808	GOOG- NOBOTS- PA- 00014885
U.S. Patent App. Pub. No. 2009/0037983	Oct. 22, 2007	Feb. 5, 2009	Chiruvolu 983	GOOG- NOBOTS- PA- 00014926
U.S. Patent App. Pub. No. 2010/0211997	Dec. 23, 2009	Aug. 19, 2010	McGeehan 997	GOOG- NOBOTS- PA- 00015038
U.S. Patent App. Pub. No. 2015/0112892	Oct. 18, 2013	Apr. 23, 2015	Kaminsky 892	GOOG- NOBOTS- PA- 00014993
WO2006118968	April 28, 2005	Nov. 9, 2006	Varghese 968	GOOG- NOBOTS-

Patent/Publication	Filing Date	Date of Issuance/ Publication	Herein Referenced As	Production Numbers
				PA-00015247
WO2008096207	Feb. 7, 2007	Aug. 14, 2008	Lior 207	GOOG-NOBOTS-PA-00015001

Table 2: Non-Patent Prior Art Publications

Title/Reference	Date	Herein Referenced As	Production Numbers
CoDeeN: A Content Distribution Network for Planet Lab (Feb. 10, 2007), https://web.archive.org/web/20070210195838/https://codeen.cs.princeton.edu/ .	2007	2007 CoDeeN Website	GOOG-NOBOTS-PA-00011851
A. Al-Qayedi et al., <i>Combined Web/mobile authentication for secure Web access control</i> , 2004 IEEE Wireless Communications and Networking Conference (Mar. 21-25, 2004), pp. 677-681	Mar. 21, 2004	Al-Qayedi	GOOG-NOBOTS-PA-00005504
Alex Andersen & Simen Hagen, <i>Using Alert Levels to Enhance Keystroke Dynamic Authentication</i> (2007), http://www.nik.no/2007/15-Andersen .	2007	Andersen	GOOG-NOBOTS-PA-00011823
Elias Athanasopoulos & Spiros Antonatos, <i>Enhanced CAPTCHAs: using animation to tell humans and computers apart</i> , Proceedings of the 10th International Conference on Communications and Multimedia Security (2006), pp. 97-108.	2006	Athanasopoulos	GOOG-NOBOTS-PA-00008573
Human Interactive Proofs, Second International Workshop (Henry S. Baird & Daniel P. Lopresti eds., 2005).	2005	Baird & Lopresti	GOOG-NOBOTS-PA-00007606
Henry S. Baird & Jon L. Bentley, <i>Implicit CAPTCHAs</i> , Proc. SPIE 5676, Document Recognition & Retrieval XII (Jan 17, 2005), pp. 191-196.	2005	Baird I	GOOG-NOBOTS-PA-00007757

Title/Reference	Date	Herein Referenced As	Production Numbers
Henry S. Baird et al., <i>Scatter Type: A Legible but Hard-to-Segment CAPTCHA</i> , Proceedings of the 8th International Conference on Document Analysis and Recognition (2005), pp. 935-939.	2005	Baird II	GOOG-NOBOTS-PA-00007763
Loren Baker, <i>Click Fraud and How to Stop It</i> , SearchEngineJournal (Dec. 7, 2004), https://www.searchenginejournal.com/click-fraud-and-how-to-stop-it/1123/#close .	2004	Baker	GOOG-NOBOTS-PA-00005509
Karen Bannan, <i>Click Fraud Is Growing on the Web</i> , N.Y. Times (Sept. 23, 2006), https://www.nytimes.com/2006/09/23/technology/23click.html .	2006	Bannan	GOOG-NOBOTS-PA-00008586
Colin Barras, <i>Robot Asimo can understand three voices at once</i> , NewScientist (June 10, 2008), https://www.newscientist.com/article/dn14105-robot-asimo-can-understand-three-voices-at-once/ .	2008	Barras	GOOG-NOBOTS-PA-00012599
BotBarrier FAQ: How effective is BotBarrier? (Mar. 22, 2008), https://web.archive.org/web/20080322231602/http://www.botbarrier.com:80/faq.html .	2008	BotBarrier I	GOOG-NOBOTS-PA-00012605
BotBarrier: Turn any digital image into a clickable CAPTCHA! (June 21, 2008), https://web.archive.org/web/20080621051833/http://www.botbarrier.com:80/ .	2008	BotBarrier II	GOOG-NOBOTS-PA-00012604
Kuan-Ta Chen et al., <i>Identifying MMORPG Bots: A traffic analysis approach</i> (2006).	2006	Chen I	GOOG-NOBOTS-PA-00008589
Kuan-Ta Chen et al., <i>Game Bot Detection Based on Avatar Trajectory</i> , Proceedings of the 7th International Conference on Entertainment	2008	Chen II	GOOG-NOBOTS-PA-00012606

Title/Reference	Date	Herein Referenced As	Production Numbers
Computing (Sept. 25-27, 2008), pp. 95-105.			
Monica Chew & Henry S. Baird, <i>Baffle Text: a Human Interactive Proof</i> , Proc. SPIE 5010, Document Recognition & Retrieval Conf. (Jan. 13, 2003).	2003	Chew I	GOOG-NOBOTS-PA-00005462
Monica Chew & J.D. Tygar, <i>Image recognition CAPTCHAs</i> , 7th International Information Security Conference (Sept. 27-29, 2004), pp. 268-279.	2004	Chew II	GOOG-NOBOTS-PA-00005519
Richard Chow et al., <i>Making CAPTCHAs clickable</i> , Proceedings of the 9th workshop on Mobile computing systems and applications (2008), pp. 91-94.	2008	Chow	GOOG-NOBOTS-PA-00012619
Ko-Kang Chu et al., <i>A Hybrid Training Mechanism for Applying Neural Networks to Web-based Applications</i> , 2004 IEEE International Conference on Systems, Man and Cybernetics (2004), pp. 3543-3547.	2004	Chu	GOOG-NOBOTS-PA-00005538
ClickHawk website (Jan. 2007), https://web.archive.org/web/20070118082529/http://clickhawk.com/ , https://web.archive.org/web/20070116074731/http://clickhawk.com/clickhawk/ , https://web.archive.org/web/20070116074850/http://clickhawk.com/click_fraud.htm , https://web.archive.org/web/20070120182221/http://clickhawk.com/clickhawk/clickhawk_benefits.htm , https://web.archive.org/web/20070121050250/http://www.clickhawk.com/clickhawk/set_up_help.htm , https://web.archive.org/web/20070116074721/http://clickhawk.com/faq.htm , https://web.archive.org/web/20070116074535/http://clickhawk.com/about.htm , https://web.archive.org/web/20070116074535/http://clickhawk.com/about.htm	Jan. 2007	ClickHawk I	GOOG-NOBOTS-PA-00011837

Title/Reference	Date	Herein Referenced As	Production Numbers
74840/http://clickhawk.com/contact.htm			
ClickHawk website (Apr. 25, 2022), at www.clickhawk.com.	2022	ClickHawk II	GOOG-NOBOTS-PA-00013858
Allison L. Coates et al., <i>Pessimist print: a reverse Turing test</i> , 6th International Conference on Document Analysis & Recognition (2001), pp. 1154-1158.	2003	Coates	GOOG-NOBOTS-PA-00005473
Bruno Norberto da Silva & Ana Cristina Bicharra Garcia, <i>KA-CAPTCHA: An Opportunity for Knowledge Acquisition on the Web</i> , Proceedings of the 22nd AAAI Conference on Artificial Intelligence (2007), pp. 1322-1327.	2007	da Silva	GOOG-NOBOTS-PA-00011853
Ritendra Datta et al., <i>IMAGINATION a robust image-based CAPTCHA generation system</i> , Proceedings of the 13th annual ACM International Conference on Multimedia (2005), pp. 331-334.	2005	Datta	GOOG-NOBOTS-PA-00007769
Dossier: Human Differential Intelligence, LLC, RPX Corporation (Aug. 7, 2020).	2020	Dossier	GOOG-NOBOTS-PA-00013834
James Edwards & Cameron Adams, <i>The Javascript Anthology: 101 Essential Tips, Tricks & Hacks</i> (2006).	2006	Edwards	GOOG-NOBOTS-PA-00008602
Jeremy Elson et al., <i>Asirra: a CAPTCHA that exploits interest-aligned manual image categorization</i> , In Proceedings of ACM CCS (2007), pp. 366-374.	2007	Elson	GOOG-NOBOTS-PA-00011859
David Flanagan, <i>JavaScript: The Definitive Guide</i> (5th ed. 2006)	2006	Flanagan	GOOG-NOBOTS-PA-00009228
Hugo Gamboa & Ana Fred, <i>A behavioral biometric system based on human-computer interaction</i> , Proc. SPIE 5404 Biometric Technology for Human Identification (Aug. 25, 2004), pp. 381-392.	2004	Gamboa	GOOG-NOBOTS-PA-00005548

Title/Reference	Date	Herein Referenced As	Production Numbers
Shuman Ghosemanjunder, <i>Google, Click Fraud, and Invalid Clicks</i> , Shumans Blog (Dec. 12, 2006), https://web.archive.org/web/20070629192232/http://shumans.com/articles/000044.php .	2006	Ghosemanjunder	GOOG-NOBOTS-PA-00010251
Philippe Golle & Nicolas Ducheneaut, <i>Preventing Bots from Playing Online Games</i> , 3 Comput. Entertain. (2005).	2005	Golle III	GOOG-NOBOTS-PA-00007773
Philippe Golle, <i>Machine Learning Attacks Against the Asirra CAPTCHA</i> , Proceedings of the 15th ACM Conference on Computer and Communications Security (2008), pp. 535-542.	2008	Golle IV	GOOG-NOBOTS-PA-00012623
Rich Gossweiler et al., <i>What's Up CAPTCHA? A CAPTCHA Based On Image Orientation</i> , Proceedings of the 18th International Conference on World Wide Web (Apr. 20-24, 2009), pp. 841-850.	2009	Gossweiler	GOOG-NOBOTS-PA-00013803
Nicole Immorlica et al., <i>Click Fraud Resistant Methods for Learning Click-Through Rates</i> , Internet and Network Economics (2005).	2005	Immorlica	GOOG-NOBOTS-PA-00007783
Nat Ives, Web Marketers Fearful of Fraud in Pay-Per-Click, N.Y. Times (Mar. 3, 2005), https://www.nytimes.com/2005/03/03/business/media/web-marketers-fearful-of-fraud-in-payperclick.html .	2005	Ives	GOOG-NOBOTS-PA-00007796
Biometrics: Personal Identification in Networked Society (Anil Jain et al., eds. 1999).	1999	Jain I	GOOG-NOBOTS-PA-00002372
Anil K. Jain et al., eds., Handbook of Biometrics (2008)	2008	Jain II	GOOG-NOBOTS-PA-00012632
Peter-Paul Koch, PPK on JavaScript (2007).	2007	Koch	GOOG-NOBOTS-PA-00011868

Title/Reference	Date	Herein Referenced As	Production Numbers
Greg Kochanski et al., <i>A Reverse Turing Test Using Speech</i> , 7th International Conference on Spoken Language Processing (Sept. 16-20, 2002).	2002	Kochanski	GOOG-NOBOTS-PA-00003820
Richard J. Larsen & Morris L. Marx, <i>An Introduction to Mathematical Statistics and Its Applications</i> (4th ed. 2006)	2006	Larsen	GOOG-NOBOTS-PA-00010254
Daniel Lopresti, <i>Leveraging the CAPTCHA Problem</i> , Proceedings of the 2nd International Conference on Human Interactive Proofs (2005), pp. 97-110.	2005	Lopresti	GOOG-NOBOTS-PA-00007799
Markus Jakobsson & Zulfikar Ramzan, <i>Crimeware: Understanding New Attacks and Defenses</i> (Symantec 2008).	2008	M. Jakobsson	GOOG-NOBOTS-PA-00013182
Charles C. Mann, <i>How Click Fraud Could Swallow the Internet</i> , Wired (Jan. 1, 2006, 12:00 PM), https://www.wired.com/2006/01/fraud/ .	2006	Mann	GOOG-NOBOTS-PA-00011184
Matt May, <i>Inaccessibility of CAPTCHA: Alternatives to Visual Turing Tests on the Web</i> , W3C (Nov. 23, 2005), https://web.archive.org/web/20061230090005/https://www.w3.org/TR/2005/NOTE-turingtest-20051123/ .	2005	May I	GOOG-NOBOTS-PA-00007850
Matt May, <i>Escape from CAPTCHA</i> W3C (2004), https://web.archive.org/web/20050206064605/http://www.w3.org/2004/Talks/0319-csun-m3m/Overview-1.html .	2004	May II	GOOG-NOBOTS-PA-00007825
Jamieson McCausland et al., <i>A Proactive Risk-Aware Robotic Sensor Network for Critical Infrastructure Protection</i> , 2013 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) (2013), pp. 132-137.	2013	McCausland	GOOG-NOBOTS-PA-00013821

Title/Reference	Date	Herein Referenced As	Production Numbers
Steve McConnell, <i>Code Complete: a practical handbook of software construction</i> (2d ed. 2004).	2004	McConnell	GOOG-NOBOTS-PA-00005561
Robert McMillan, <i>Researcher Hacks Microsoft Fingerprint Reader</i> , PCWorld (Mar. 6, 2006, 3:00 PM), https://www.pcworld.com/article/124978/article.html .	Aug. 16, 2018	McMillan	GOOG-NOBOTS-PA-00013830
<i>Fingerprint Reader: Replace Passwords with Your Fingerprint</i> , Microsoft (Dec. 30, 2006), https://web.archive.org/web/20061230123302/http://www.microsoft.com/hardware/mouseandkeyboard/productdetails.aspx?pid=036 .	Dec. 30, 2006	Microsoft Fingerprint Reader	GOOG-NOBOTS-PA-00011188
<i>Most people have at least 15 username and password combinations to remember</i> , Microsoft (Jan. 11, 2005), https://web.archive.org/web/20050111041404/http://www.microsoft.com/hardware/mouseandkeyboard/features/docs/fingerprint.html .	Jan. 11, 2005	Microsoft Fingerprint Reader Video	GOOG-NOBOTS-PA-00013827
<i>Tired of passwords? Replace them with your fingerprint</i> , Microsoft (Sept. 26, 2004), https://web.archive.org/web/20040926002804/http://www.microsoft.com/hardware/mouseandkeyboard/features/fingerprint.msp .	Sept. 26, 2004	Microsoft Tired of Passwords	GOOG-NOBOTS-PA-00013829
Michael Moncur, <i>Teach Yourself JavaScript in 24 Hours</i> (3d ed. 2002).	2002	Moncur	GOOG-NOBOTS-PA-00003824
Partha Pal et al., <i>Trust Assessment from Observed Behavior: Toward and Essential Service for Trusted Network Computing</i> , 5th IEEE International Symposium on Network Computing and Applications (2006), pp. 285-292.	2006	Pal	GOOG-NOBOTS-PA-00011218
KyoungSoo Park et al., <i>Securing Web Service by Automatic Robot Detection</i> ,	2006	Park	GOOG-NOBOTS-PA-00011226

Title/Reference	Date	Herein Referenced As	Production Numbers
Proceedings of the USENIX '06 Annual Technical Conference (2006), pp. 255-260.			
Adam L. Penenberg, <i>BlowSearch Tackles Click Fraud</i> , Wired (June 16, 2005, 2:00 AM), https://www.wired.com/2005/06/blowsearch-tackles-click-fraud/ .	2005	Penenberg	GOOG-NOBOTS-PA-00007857
Mark Pilgrim, <i>Greasemonkey Hacks: Tips & Tools for Remixing the Web with Firefox</i> (2006).	2006	Pilgrim	GOOG-NOBOTS-PA-00011250
Thomas Powell & Fritz Schneider, <i>JavaScript: The Complete Reference</i> (2d ed. 2004).	2004	Powell	GOOG-NOBOTS-PA-00006535
Arun Ross & Anil K. Jain, <i>Human recognition using biometrics: an overview</i> , 62 <i>Annales Des Telecommunications</i> (2007), pp. 11-35.	2007	Ross	GOOG-NOBOTS-PA-00012398
Yong Rui et al., <i>Characters or Faces: A User Study on Ease of Use for HIPs</i> , 3517 <i>Lecture Notes in Computer Science</i> (2005), pp. 53-65.	2005	Rui	GOOG-NOBOTS-PA-00007859
Amalia Rusu, <i>Exploiting the Gap in Human and Machine Abilities in Handwriting Recognition for Web Security Applications</i> (2007) (Ph.D. dissertation, State University of New York at Buffalo).	2007	Rusu I	GOOG-NOBOTS-PA-00012424
Amalia Rusu & Venu Govindaraju, <i>Visual CAPTCHA with Handwritten Image Analysis</i> , State University of New York at Buffalo.	2005	Rusu II	GOOG-NOBOTS-PA-00007866
Ayşe Pinar Saygin et al., "Turing Test: 50 Years Later," in <i>Minds and Machines</i> , vol. 10, at 463-516 (2001).	2001	Saygin	GOOG-NOBOTS-PA-00002783
Mohammad Shirali-Shahreza & Sajad Shirali-Shahreza, <i>CAPTCHA for Blind People</i> , IEEE International Symposium	2007	Shirali-Shahreza I	GOOG-NOBOTS-PA-00012565

Title/Reference	Date	Herein Referenced As	Production Numbers
on Signal Processing and Information Technology (2007), pp. 995-998.			
Sajad Shirali-Shahreza & M. Hassan Shirali-Shahreza, <i>Bibliography of Works Done on CAPTCHA</i> , Proceedings of 2008 3rd International Conference on Intelligent System and Knowledge Engineering (2008), pp. 205-210.	2008	Shirali-Shahreza II	GOOG-NOBOTS-PA-00013779
Sajad Shirali-Shahreza & Mohammad Shirali-Shahreza, <i>CAPTCHA for Children</i> , 2008 IEEE International Conference on System of Systems Engineering (2008), pp. 1-6.	2008	Shirali-Shahreza III	GOOG-NOBOTS-PA-00013785
Radu Sion et al., <i>On-the-fly Intrusion Detection for Web Portals</i> , Proceedings of the International Conference on Information Technology, Computers and Communications (2003), pp. 325-330.	2003	Sion	GOOG-NOBOTS-PA-00005478
Hocquet Sylvain et al., <i>Users Authentication by a Study of Human Computer Interactions</i> , Universite Francois-Rabelais, Tours - France (2004).	2004	Sylvain	GOOG-NOBOTS-PA-00007513
Jennifer Tam et al., <i>Breaking Audio CAPTCHAs</i> , Proceedings of the 21st International Conference on Neural Information Processing Systems (2008), pp. 1625-1632.	2008	Tam	GOOG-NOBOTS-PA-00013813
Pang-Ning Tan & Vipin Kumar, <i>Discovery of Web Robot Sessions Based on Their Navigational Patterns</i> , 6 Data Mining and Knowledge Discovery (2002), pp. 9-35.	2002	Tan	GOOG-NOBOTS-PA-00003368
<i>reCAPTCHA: Using Captchas To Digitize Books</i> , TechCrunch (Sept. 16, 2007 5:54 PM), https://techcrunch.com/2007/09/16/recaptcha-using-captchas-to-digitize-books/ .	2007	TechCrunch	GOOG-NOBOTS-PA-00012569

Title/Reference	Date	Herein Referenced As	Production Numbers
Gerald Temple et al., <i>Testability Modeling and Analysis of a Rocket Engine Test Stand</i> , 2005 IEEE Aerospace Conference (2005), pp. 3874-3895.	2005	Temple	GOOG-NOBOTS-PA-00007891
Dave Thau, <i>The Book of Javascript: A Practical Guide to Interactive Web Pages</i> (2d ed. 2007).	2007	Thau	GOOG-NOBOTS-PA-00002839
Clive Thompson, <i>For Certain Tasks, the Cortex Still Beats the CPU</i> , Wired (June 25, 2007, 12:00 PM), https://www.wired.com/2007/06/ff-humancomp/ .	2007	Thompson	GOOG-NOBOTS-PA-00012579
Alexander Tuzhilin, <i>The Lane's Gifts v. Google Report</i> (July 25, 2006), https://web.archive.org/web/20060725201250/http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf .	2006	Tuzhilin Report	GOOG-NOBOTS-PA-00011748
Alexander J. Vincent, <i>JavaScript: Developer's Dictionary</i> (1st ed. 2002).	2002	Vincent	GOOG-NOBOTS-PA-00004269
Luis von Ahn et al., <i>CAPTCHA: Using Hard AI Problems for Security</i> , In <i>Proceedings of Eurocrypt</i> (2003), pp. 294-311.	2003	von Ahn I	GOOG-NOBOTS-PA-00005444
Luis von Ahn & Laura Dabbish, <i>Labeling Images with a Computer Game</i> , <i>Proceedings of the SIGCHI Conference on Human Factors in Computing Systems</i> (2004), pp. 319-326.	2004	von Ahn II	GOOG-NOBOTS-PA-00005485
Luis von Ahn et al., <i>Telling Humans and Computers Apart (Automatically) or How Lazy Cryptographers do AI</i> , 47 <i>Commun. ACM</i> (2004), pp. 56-60.	2004	von Ahn III	GOOG-NOBOTS-PA-00005493
Luis von Ahn, <i>Human Computation</i> (Dec. 7, 2005) (DCS thesis, School of Computer Science, Carnegie Mellon University).	2005	von Ahn IV	GOOG-NOBOTS-PA-00007519

Title/Reference	Date	Herein Referenced As	Production Numbers
Luis von Ahn et al., <i>The CAPTCHA Project</i> , Carnegie Mellon School of Computer Science (Jan. 4, 2007), https://web.archive.org/web/20070104074513/http://www.captcha.net/ .	2007	von Ahn V	GOOG-NOBOTS-PA-00011818
Luis von Ahn et al., <i>reCAPTCHA: Human-Based Character Recognition via Web Security Measures</i> , 321 Science (Sept. 12, 2008), pp. 1465-1468.	2008	von Ahn VI	GOOG-NOBOTS-PA-00012595
Leslie Walker, <i>In Game of Click and Mouse, Advertisers Come Up Empty</i> , Washington Post (Mar. 16, 2006), https://www.washingtonpost.com/wp-dyn/content/article/2006/03/15/AR2006031502339_pf.html .	2006	Walker	GOOG-NOBOTS-PA-00011795
Oli Warner, <i>The Cutest Human-Test: KittenAuth</i> , ThePCSpy (Apr. 6, 2006), https://thepcsy.com/read/the_cutest_humantest_kittenauth/ .	2006	Warner	GOOG-NOBOTS-PA-00011189
<i>Microsoft Fingerprint Reader</i> , Wikipedia, https://en.wikipedia.org/w/index.php?title=Microsoft_Fingerprint_Reader&oldid=1052367656 (Oct. 28, 2021, 7:34 PM).	Aug. 16, 2018	Wikipedia, Microsoft Fingerprint Reader	GOOG-NOBOTS-PA-00013832
Roman V. Yampolskiy & Venu Govindaraju, <i>Embedded Noninteractive Continuous Bot Detection</i> , 5 ACM Comput. Entertain. (Mar. 1, 2008), pp. 1-11.	2008	Yampolskiy	GOOG-NOBOTS-PA-00013792
Jeff Yan, <i>Bot, Cyborg and Automated Turing Test</i> , Univ. of Newcastle upon Tyne, Computing Science, Technical Report Series (2006).	2006	Yan	GOOG-NOBOTS-PA-00011797
S.F. Yeung et al., <i>Detecting Cheaters for Multiplayer Games: Theory, Design and Implementation</i> , Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (Jan. 8-10, 2006), pp. 1178-1182.	2006	Yeung	GOOG-NOBOTS-PA-00011812

Title/Reference	Date	Herein Referenced As	Production Numbers
Nicholas C. Zakas, JavaScript for Web Developers (2005).	2005	Zakas	GOOG-NOBOTS-PA-00007913
www.reCAPTCHA.net (2007), downloaded from https://web.archive.org/web/20070520042149/http://recaptcha.net/ .	2007		GOOG-NOBOTS-PA-00014607
Google Code: reCAPTCHA, at https://web.archive.org/web/20070526055157/http://code.google.com/p/recaptcha/	2007		GOOG-NOBOTS-PA-00014574
Edith Law & Luis von Ahn, Human Computation: A Publication in the Springer Series "Synthesis Lectures on Artificial Intelligence and Machine Learning" (2011).	2011	2011 Law	GOOG-NOBOTS-PA-00014660
ClickHawk.com (Feb. 24, 2007), at https://web.archive.org/web/20070224005240/http://www.clickhawk.com	2022	2007 ClickHawk	GOOG-NOBOTS-PA-00014545
Massimo Piccardi Background subtraction techniques: a review, (2004) IEEE International Conference on Systems, Man and Cybernetics, p. 3099-3104	2004	2004 Piccardi	GOOG-NOBOTS-PA-00014313
A. Al-Qayedi, et. al. Secure Centralised Mobile and Web-based control system Using GPRS with J2ME (2003).	2003	2003 Al-Qayedi	GOOG-NOBOTS-PA-00014219
COMTEX, Jack Henry Selects RSA Cyota Consumer Solutions to Provide Risk-Based Strong Authentication for Online Banking (2006).	2006	2006 COMTEX	GOOG-NOBOTS-PA-00014365
Cyota, RSA Adaptive Authentication: Balancing Risk, Preference, and Security (2006).	2006	2006 Cyota	GOOG-NOBOTS-PA-00014370
Mark Lindeman et. al, A Gentle Introduction to Risk-Limiting Audits (2012).	2012	2012 Lindeman	GOOG-NOBOTS-PA-00014772
Ronald L. Rivest, Bayesian Tabulation Audits Explained and Extended (2018).	2018	2018 Rivest	GOOG-NOBOTS-PA-00014791

Title/Reference	Date	Herein Referenced As	Production Numbers
E. L. Lehmann, Testing Statistical Hypotheses (1991).	1991	1991 Lehmann	GOOG-NOBOTS-PA-00014206
Open Source Initiative OSI, The MIT License: Licensing (2006).	2006	2006 MIT License	GOOG-NOBOTS-PA-00014477
Mir Aman Sheheryar et. al, A Review on Captcha Generation and Evaluation Techniques (2016).	2016	2016 Sheheryar	GOOG-NOBOTS-PA-00014779
Richard J. Larsen et. al, An Introduction to Mathematical Statistics and its Applications (1981).	1981	1981 Larsen	GOOG-NOBOTS-PA-00014200
Srikanth Kandula et. al, Botz-4-Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds (2004).	2004	2004 Kandula	GOOG-NOBOTS-PA-00014299
Kenneth C. Johnson, Election Certification by Statistical Audit of Voter-Verified Paper Ballots (2004).	2004	2004 Johnson	GOOG-NOBOTS-PA-00014256
Clark Pope et. al, Is it Human or Computer? Defending E-Commerce with Captchas (2005).	2005	2005 Pope	GOOG-NOBOTS-PA-00014342
Google, Invalid Clicks (2008).	2008		GOOG-NOBOTS-PA-00014643
Google. Inside AdWords: Meet the Click Quality Team (2007).	2007	2007 Meet the Click Quality Team	GOOG-NOBOTS-PA-00014576
Google, How does Google Detect Invalid Clicks? (2008).	2008		GOOG-NOBOTS-PA-00014641
Google AdWords Help Center: How does Google detect invalid clicks? (Nov. 12, 2006) at https://web.archive.org/web/20061112035942/http://adwords.google.com/support/bin/answer.py?answer=6114	2006	2006 Detecting Invalid Clicks	GOOG-NOBOTS-PA-00014456
Google AdWords Help Center: What kinds of clicks does Google consider invalid? (Apr. 29, 2006), at https://web.archive.org/web/20060429143944/http://adwords.google.com/suppo	2006	2006 What Kinds of Clicks	GOOG-NOBOTS-PA-00014461

Title/Reference	Date	Herein Referenced As	Production Numbers
rt/bin/answer.py?answer=6423&ctx=sib ling			
Google AdWords Help Center: What does Google do when invalid clicks are detected? (Nov. 11, 2006) at https://web.archive.org/web/200611120 41426/http://adwords.google.com/suppo rt/bin/answer.py?answer=6422&topic=3 5 .	2006	2006 Invalid Clicks	GOOG-NOBOTS-PA- 00014459
Google, Does high click volume mean I'm getting invalid clicks? (2006).	2006		GOOG-NOBOTS-PA- 00014455
Google, Invalid Clicks (2006).	2006		GOOG-NOBOTS-PA- 00014458
Google, About the Ad Traffic Quality Resource Center (2007).	2007		GOOG-NOBOTS-PA- 00014575
Bharosa, Strong Multifactor Online Authentication Security for the Enterprise (2007) (collection of related webpages from Wayback Machine archive of www.bharosa.com).	2007	2007 Bharosa.com	GOOG-NOBOTS-PA- 00014508
Pawel Lupkowski et. al, Application of the Technology Acceptance Model to OCR-based CAPTCHA systems (2010).	2010	2010 Lupkowski	GOOG-NOBOTS-PA- 00014645
Google, Ad Traffic Quality Resource Center (2007).	2007		GOOG-NOBOTS-PA- 00014584
MattTopper.com, Oracle Adaptive Access Manager (2007).	2007	MattTopper.co m	GOOG-NOBOTS-PA- 00014604
RSA, eFraudNetwork (2007) (collection of related webpages from Wayback Machine archive of www.rsa.com)	2007	2007 RSA.com	GOOG-NOBOTS-PA- 00014635
Google, Introducing the Ad Traffic Quality Resource Center (2007).	2007		GOOG-NOBOTS-PA- 00014581
Google Code, reCAPTCHA (2007).	2007		GOOG-NOBOTS-PA- 00014574
BioPassword, Internet Authentication Software with Keystroke Dynamics (2007) (collection of related webpages	2007	2007 BioPassword.co m	GOOG-NOBOTS-PA- 00014517

Title/Reference	Date	Herein Referenced As	Production Numbers
from Wayback Machine archive of www.biopassword.com).			
Bharosa, Product Fact Sheet (2007), at https://web.archive.org/web/20070710070813/http://www.bharosa.com/Bharosa_fact_sheet.pdf	2007	2007 Bharosa Fact Sheet	GOOG-NOBOTS-PA- 00014508
Richard Atterer et. al, Knowing the user's every move: user activity tracking for website usability evaluation and implicit interaction (2006).	2006	2006 Atterer	GOOG-NOBOTS-PA- 00014349
Maja Pusara et. al, User re- authentication via mouse movements (2004).	2004	2004 Pusara	GOOG-NOBOTS-PA- 00014319
Finextra, Arcot adds Quova geolocation technology to authentication package (Sept. 27, 2006), at https://www.finextra.com/pressarticle/11524/arcot-adds-quova-geolocation-technology-to-authentication-package	2006	2006 Arcot Adds Quova	GOOG-NOBOTS-PA- 00014420
Finextra, RSA Security introduces adaptive authentication (Mar. 1, 2006), at https://www.finextra.com/pressarticle/8247/rsa-security-introduces-adaptive-authentication	2006	2006 RSA Security Introduces	GOOG-NOBOTS-PA- 00014447
Fabian Monroe et. al, Password hardening based on keystroke dynamics (1999)	1999	1999 Monroe	GOOG-NOBOTS-PA- 00014208
Network Computing, National City Taps Bharosa (Sept. 13, 2006), at https://www.networkcomputing.com/net-work-security/national-city-taps-bharosa	2006	2006 National City Taps Bharosa	GOOG-NOBOTS-PA- 00014473
Jack Henry, Jack Henry Selects RSA Cyota Consumer Solutions to Provide Risk-Based Strong Authentication for Online Banking (Mar. 8, 2006), at https://ir.jackhenry.com/news-releases/news-release-details/jack-henry-selects-rsa-cyota-consumer-solutions-provide-	2006	2006 Jack Henry	GOOG-NOBOTS-PA- 00014471

Title/Reference	Date	Herein Referenced As	Production Numbers
risk#:~:text=The%20RSA%20Adaptive%20Authentication%20technology,location%20and%20prior%20transaction%20behaviors			
BioPassword, The Green Sheet Online Edition (Oct. 8, 2007), at https://greensheet.com/emagazine.php?article_id=349	2007	2007 Green Sheet	GOOG-NOBOTS-PA-00014534
EWeek, Matt Hines, Do Not Enter (Oct. 22, 2006), at https://www.eweek.com/security/do-not-enter/	2006	2006 Hines	GOOG-NOBOTS-PA-00014462
Finextra, E*Trade signs for RSA authentication, anti-phishing technology (Mar. 1, 2006), at https://www.finextra.com/newsarticle/14990/etrade-signs-for-rsa-authentication-anti-phishing-technology	2006	Finextra	GOOG-NOBOTS-PA-00014439
Electronic Frontier Foundation, Biometrics: Who's Watching You? (2003), at https://www EFF.org/wp/biometrics-whos-watching-you	2003	2003 EFF Biometrics	GOOG-NOBOTS-PA-00014223
DarkReading, Bharosa Launches 3.5 (Nov. 21, 2006), at https://www.darkreading.com/cyberattacks-data-breaches/bharosa-launches-3-5	2006	2006 Bharosa Launches 3.5	GOOG-NOBOTS-PA-00014410
ComputerWorld, 2006 Horizon Awards Winner: BioPassword Inc.'s BioPassword -- Computerworld (2006)	2006	2006 Computerworld Website	GOOG-NOBOTS-PA-00014360
TIME, Change Agent: Telltale Fingertips (Dec. 9, 2006), at https://time.com/archive/6679424/change-agent-telltale-fingertips/	2006	2006 Telltale Fingertips	GOOG-NOBOTS-PA-00014484
Google Goowiki, AdSpam: Overview of Ad Click Logging at Google (rev. 1.1) (Oct. 24, 2006)	2006	AdClickLogging 1.1	*Produced with technical document production

Title/Reference	Date	Herein Referenced As	Production Numbers
Google Goowiki, AdSpam: AdSense Spam Classification (rev. 1.24) (Nov. 7, 2007)	2007	AdSenseSpamClassifier 1.24	*Produced with technical document production
Google Goowiki, AdSpam: AdSense Pub Spam Classifier (rev. 1.7) (Oct. 15, 2007)	2007	AdSenseSpamClassifier3 1.7	*Produced with technical document production
Google Goowiki, AdSpam: AdSpam Introduction (rev. 1.8) (Nov. 3, 2006)	2006	AdSpamIntroduction 1.8	*Produced with technical document production
Google Goowiki, AdSpam: Next Generation Online Filters (rev. 1.18) (July 17, 2006)	2006	OnlineFilters 1.18	*Produced with technical document production
Google Goowiki, AdSpam: Anomaly Score for Daily Click Traffic (rev. 1.24) (Aug. 24, 2006)	2006	AnomalyScore 1.24	*Produced with technical document production
Google Goowiki, AdSpam: Archive of AdSpam Cases (rev. 1.1) (Aug. 24, 2007)	2007	AdSpamArchives 1.1	*Produced with technical document production
Google Goowiki, AdSpam: Attack Taxonomy (rev. 1.1) (Jan. 12, 2007)	2007	AttackTaxonomy 1.1	*Produced with technical document production
Google Goowiki, AdSpam: AutomatedSignalAnalysis (rev. 1.4) (Aug. 8, 2006)	2006	AutomatedSignalAnalysis 1.4	*Produced with technical document production
Google Goowiki, AdSpam: BetterAnalysisOfOnlineFilters (rev. 1.9) (Jan. 26, 2006)	2006	BetterAnalysisOfOnlineFilters 1.9	*Produced with technical document production
Google Goowiki, AdSpam: Click Delay Filter (rev. 1.10) (July 20, 2007)	2007	ClickDelayFilter 1.10	*Produced with technical document production
Google Goowiki, AdSpam: FakeClicks (rev. 1.4) (Mar. 10, 2006)	2006	FakeClicks 1.4	*Produced with technical document production
Google Goowiki, AdSpam: FilterReleaseDates (rev. 1.4) (Sept. 29, 2005)	2005	FilterReleaseDates 1.4	*Produced with technical document production
Google Goowiki, AdSpam: General Info (rev. 1.2) (Aug. 23, 2007)	2007	GeneralInfo 1.2	*Produced with technical document production
Google Goowiki, AdSpam: How to Write a Blitzen Filter (rev. 1.9) (Oct. 18, 2006)	2006	HowToWriteAFilter 1.9	*Produced with technical document production

Title/Reference	Date	Herein Referenced As	Production Numbers
Google Goowiki, AdSpam: How We Fight Spam (rev. 1.7) (Jan. 2, 2007)	2007	HowWeFightSpam 1.7	*Produced with technical document production
Google Goowiki, AdSpam: IP Blacklist Rules (rev. 1.15) (Apr. 19, 2007)	2007	IPBlacklists 1.15	*Produced with technical document production
Google Goowiki, AdSpam: IPFrequencyFilter (rev. 1.48) (Oct. 27, 2006)	2006	IPFrequencyFilter 1.48	*Produced with technical document production
Google Goowiki, AdSpam: Javascript Signals (rev. 1.20) (Oct. 30, 2007)	2007	JavascriptSignals 1.20	*Produced with technical document production
Google Goowiki, AdSpam: Logging Javascript Signals in AdMixer Logs (rev. 1.7) (Feb. 20, 2007)	2007	LoggingJavascriptSignals 1.7	*Produced with technical document production
Google Goowiki, AdSpam: NearDuplicateThreshold (rev. 1.26) (June 12, 2007)	2007	NearDuplicateThreshold 1.26	*Produced with technical document production
Google Goowiki, AdSpam: OddFlow (rev. 1.5) (Dec. 13, 2006)	2006	OddFlow 1.5	*Produced with technical document production
Google Goowiki, AdSpam: SignalDocumentation (rev. 1.74) (Nov. 6, 2007)	2007	SignalDocumentation 1.74	*Produced with technical document production
Google Goowiki, AdSpam: TaxonomyOfSignals (rev. 1.1) (Dec. 6, 2005)	2005	TaxonomyOfSignals 1.1	*Produced with technical document production
Google Goowiki, AdSpam: Auto-Termination Classifier Model (rev. 1.4) (Apr. 17, 2006)	2006	AutoTerminateClassifier 1.4	*Produced with technical document production
Google Goowiki, AdSpam: Finding Bad Referrers (rev. 1.22) (Nov. 16, 2007)	2007	BadReferrers 1.22	*Produced with technical document production
Google Goowiki, AdSpam: Precheck Megastats (rev. 1.6) (Dec. 15, 2006)	2006	BlacklistDevelopment 1.6	*Produced with technical document production
Google Goowiki, AdSpam: Clickbot.A Investigation (rev. 1.19) (June 26, 2006)	2006	Clickbot.A 1.19	*Produced with technical document production
Google Goowiki, AdSpam: DupeDetectionSignals (rev. 1.16) (Nov. 14, 2007)	2007	DupeDetectionSignals 1.16	*Produced with technical document production
Google AdSpam, ClicktimeSignal (rev. 1.68) (Oct. 23, 2007)	2007	ClicktimeSignal 1.68	*Produced with technical document production

Title/Reference	Date	Herein Referenced As	Production Numbers
Google Goowiki, AdSpam: MouseoverTracking (rev. 1.6) (Sept. 25, 2006)	2006	MouseoverTracking 1.6	*Produced with technical document production
Google Goowiki, AdSpam: Facts About Headers (rev. 1.11) (Jan. 29, 2007)	2007	FactsAboutHeaders 1.11	*Produced with technical document production
Google Goowiki, AdSpam: Feature Selection in Adspam Classifier Training (rev. 1.10) (Apr. 5, 2006)	2006	FeatureSelection 1.10	*Produced with technical document production
Google Goowiki, AdSpam: FiltersOnVariousProperties (rev. 1.1) (Aug. 1, 2007)	2007	FiltersOnVariousProperties 1.1	*Produced with technical document production
Google Goowiki, AdSpam: Keyboard Dynamics Experiment Results (rev. 1.4) (Dec. 3, 2005)	2005	KeyboardDynamics 1.4	*Produced with technical document production
Google Goowiki, AdSpam: Areas of investigation (rev. 1.10) (Nov. 10, 2005)	2005	OnlineFiltersV2 1.1	*Produced with technical document production
Google Goowiki, AdSpam: Online Spam Filters (rev. 1.29) (Aug. 29, 2007)	2007	OnlineSpamFilters 1.29	*Produced with technical document production
Google Goowiki, AdSpam: SpamCubes -- Automated Filter Analysis and Flagging through Cubed Data (rev. 1.18) (Aug. 23, 2007)	2007	SpamCubes 1.18	*Produced with technical document production
Fineextra, Arcot risk and authentication technology integrated with Yodlee products (Oct. 31, 2006), at https://www.finextra.com/pressarticle/11999/arcot-risk-and-authentication-technology-integrated-with-yodlee-products	2006	2007 FinExtra Arcot Risk	GOOG-NOBOTS-PA-00014414
Arcot, Arcot RiskFort Risk-based Authentication System - Overview (Aug. 26, 2007), at https://web.archive.org/web/20070826215132/http://www.arcot.com/products/riskfort/index.html	2007	2007 Arcot.com Overview	GOOG-NOBOTS-PA-00014506
Arcot, Internet Threat Protection - Overview (Aug. 27, 2007), at https://web.archive.org/web/200708270	2007	2007 Arcot.com Solutions	GOOG-NOBOTS-PA-00014504

Title/Reference	Date	Herein Referenced As	Production Numbers
02720/http://www.arcot.com/solutions/itp.html			
Philip Marriott, Authentication by Typing Rhythm (Sept. 29, 2004), at https://www.giac.org/paper/gsec/4118/authentication-typing-rhythm/106548	2004	2004 Marriott	GOOG-NOBOTS-PA-00014244
Finextra, "Bharosa Develops App-Based Authentication Kit for Mid-Sized Firms) (June 12, 2006), at https://www.finextra.com/pressarticle/9823/bharosa-develops-app-based-authentication-kit-for-mid-sized-firms	2006	2006 Finextra Bharosa Develops Apps	GOOG-NOBOTS-PA-00014427
Finextra, Bharosa to integrate Authenticator and Tracker products with Oracle Access Manager (Oct. 16, 2006), at https://www.finextra.com/pressarticle/11842/bharosa-to-integrate-authenticator-and-tracker-products-with-oracle-access-manager	2006	2006 Bharosa to Integrate Authenticator	GOOG-NOBOTS-PA-00014433
Srikanth Kandula et. al, Botz-4-Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds (2005)	2005	2005 Kandula	GOOG-NOBOTS-PA-00014328
KyoungSoo Park, et. al, Securing Web Service by Automatic Robot Detection (2006)	2006	2006 Park	GOOG-NOBOTS-PA-00014478
Ahmed Awad E. Ahmed et. al, A New Biometric Technology Based on Mouse Dynamics (Sept. 2007)	2007	2007 Ahmed	GOOG-NOBOTS-PA-00014488
Michal Choras et. al, Web Security Enhancement Based on Keystroke Dynamics (2007)	2007	2007 Choras	GOOG-NOBOTS-PA-00014541
Guofei Gu et al., "BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation," presented at the 16th USENIX Security Symposium (2007), at https://www.usenix.org/legacy/event/sec07/tech/full_papers/gu/gu_html/ .	2007	2007 Gu	GOOG-NOBOTS-PA-00014586

Title/Reference	Date	Herein Referenced As	Production Numbers
recaptcha-mediawiki-1.6.zip, downloaded at https://web.archive.org/web/20070526055157/http://code.google.com/p/recaptcha/	2007		GOOG-NOBOTS-PA-00015336
recaptcha-php-1.6.zip, downloaded at https://web.archive.org/web/20070526055157/http://code.google.com/p/recaptcha/	2007		GOOG-NOBOTS-PA-00015337
recaptcha-phpbb-1.6.zip, downloaded at https://web.archive.org/web/20070526055157/http://code.google.com/p/recaptcha/	2007		GOOG-NOBOTS-PA-00015338
recaptcha-phpbb-1.6.zip, downloaded at https://web.archive.org/web/20070526055157/http://code.google.com/p/recaptcha/	2007		GOOG-NOBOTS-PA-00015338
RSA, Experience eFraudNetwork Video, at https://web.archive.org/web/20071018161317/http://www.rsa.com/experience/consumer/efraudnetwork_3_20_1.html	2007	2007 RSA Video	GOOG-NOBOTS-PA-00015335

Table 3: Prior Art Products and Systems

Name	Use/Knowledge/Offer Date
AdSpam (also called “Legacy AdSpam” in the Claim Chart Exhibits)	Google AdSpam, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as February 17, 2005. Versions of AdSpam date back to as early as 2002. Google’s investigation into AdSpam is ongoing and Google expressly reserves the right to supplement its contentions with respect to AdSpam.
Alchemist	Alchemist, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Alchemist system in third party discovery and will supplement when such information is received.

Name	Use/Knowledge/Offer Date
Arcot RiskFort	Arcot RiskFort, which provided automated, web-based fraud assessment and detection, was publicly known, used, and/or disclosed in the United States at least as early as August 26, 2007. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Arcot RiskFort system in third party discovery and will supplement when such information is received.
Authenticlick	Authenticlick, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Authenticlick system in third party discovery and will supplement when such information is received.
Bharosa Tracker	Bharosa Tracker, which provided automated, web-based fraud assessment and detection, was publicly known, used, and/or disclosed in the United States at least as early as June 27, 2007. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Bharosa Tracker system in third party discovery and will supplement when such information is received.
BioPassword	BioPassword, which provided automated, web-based authentication and fraud assessment, was publicly known, used, and/or disclosed in the United States at least as early as June 30, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the BioPassword system in third party discovery and will supplement when such information is received.
Avenue A/Razorfish Search, part of aQuantive	Avenue A/Razorfish Search, part of aQuantive, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Avenue A/Razorfish Search system in third party discovery and will supplement when such information is received.
Click Defender	Click Defender, a click fraud detection and protection system available at TrafficSentry.com, was publicly known, used, and/or disclosed in the United States at least as early as June 16, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Click Defender system in third party discovery and will supplement when such information is received.
Click Defense	Click Defense (www.clickdefense.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge,

Name	Use/Knowledge/Offer Date
	use, offers to sell, sales, and/or disclosures of the Click Defense system in third party discovery and will supplement when such information is received.
ClickAssurance	ClickAssurance, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the ClickAssurance system in third party discovery and will supplement when such information is received.
ClickDetective	ClickDetective (www.clickdetective.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 30, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the ClickDetective system in third party discovery and will supplement when such information is received.
ClickHawk	ClickHawk, a click fraud detection and protection system with an optional CAPTCHA feature, was publicly known, used, and/or disclosed in the United States at least as early as 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Clickhawk system in third party discovery and will supplement when such information is received.
Clicklab	Clicklab, a score-based click fraud detection system, was publicly known, used, and/or disclosed in the United States at least as early as December 7, 2004. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Clicklab system in third party discovery and will supplement when such information is received.
Clickrisk	Clickrisk (www.clickrisk.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 30, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Clickrisk system in third party discovery and will supplement when such information is received.
CoDeeN	CoDeeN (https://codeen.cs.princeton.edu/), a proxy server created at Princeton University in 2003 and deployed for general use on PlanetLab, employed a system for automatically identifying human-generated web traffic and separating it from robot-generated traffic that was publicly known, used, and/or disclosed in the United States beginning January 6, 2006, as reported in KyoungSoo Park & Vivek S. Pai, "Securing Web Service by Automatic Robot Detection," in Annual Tech '06: 2006 USENIX Annual Technical Conference at 255–60 (2006), at https://www.usenix.org/legacy/events/usenix06/tech/park.html . Google expects to obtain further information regarding public knowledge, use, offers

Name	Use/Knowledge/Offer Date
	to sell, sales, and/or disclosures of the CoDeeN system in third party discovery and will supplement when such information is received.
Did-It.com	Did-It.com, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Did-It.com system in third party discovery and will supplement when such information is received.
HitsLink	HitsLink by Net Applications (www.hitslink.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 30, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the HitsLink system in third party discovery and will supplement when such information is received.
Impaqt	Impaqt, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Impaqt system in third party discovery and will supplement when such information is received.
PPCtrax.com	PPCtrax.com (www.ppcetrax.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 30, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the PPCtrax.com system in third party discovery and will supplement when such information is received.
RSA Adaptive Authentication	RSA Adaptive Authentication, which provided automated, web-based authentication and fraud assessment, was publicly known, used, and/or disclosed in the United States at least as early as November 8, 2007. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the RSA Adaptive Authentication system in third party discovery and will supplement when such information is received.
VeriClix	VeriClix, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the VeriClix system in third party discovery and will supplement when such information is received.
Visitlab	Visitlab (www.visitlab.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed

Name	Use/Knowledge/Offer Date
	in the United States at least as early as January 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Visitlab system in third party discovery and will supplement when such information is received.
Web Traffic Intelligence, Inc.	Web Traffic Intelligence, Inc., which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as May 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Web Traffic Intelligence system in third party discovery and will supplement when such information is received.
WhosClickingWho	WhosClickingWho (www.whosclickingwho.com), which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as January 1, 2006. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the WhosClickingWho system in third party discovery and will supplement when such information is received.
Yahoo!	Yahoo!, which provided a click fraud detection and protection system to customers, was publicly known, used, and/or disclosed in the United States at least as early as March 3, 2005. Google expects to obtain further information regarding public knowledge, use, offers to sell, sales, and/or disclosures of the Yahoo! system in third party discovery and will supplement when such information is received.

3. Claim Chart Exhibits

Google has prepared Claim Chart Exhibits (Exhibits A-1–A-19 and E-1–E-11) of prior art references that render the Asserted Claims anticipated and/or obvious. All of the Asserted Claims of the Asserted Patents are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified herein as specified in the Claim Chart Exhibits, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art reference, and/or obvious under 35 U.S.C. § 103 in view of the state of the prior art alone, the admitted prior art described above, and/or in combination with the references and disclosures detailed in the prior art references described in Exhibit A-1–A-19 ('008 patent) and Exhibit E-11

('014 patent) and Tables 1–3 above as well as the prior art references identified herein as specified in the Claim Chart Exhibits. As such, Google’s inclusion of exemplary prior art references and combinations listed below (Exhibits A-1–A-19 and E-1–E-11) does not preclude Google from identifying other invalidating combinations as appropriate.

Claim Charts for the '008 Patent

Exhibit	Primary Reference and/or System Prior Art for the '008 Patent
A-1	Willner I
A-2	Ge
A-3	O’Sullivan I
A-4	O’Connell I
A-5	Krynski
A-6	Farahat
A-7	Awadallah I
A-8	Kitts I
A-9	Meek
A-10	Tanzer
A-11	Eldon I
A-12	Obviousness Combinations
A-13	Sadagopan 870
A-14	Renaud 706
A-15	Arcot RiskFort
A-16	RSA Adaptive Authentication
A-17	Bharosa Tracker
A-18	BioPassword
A-19	Legacy AdSpam

Claim Charts for the '014 Patent

Exhibit	Primary Reference and/or System Prior Art for the '014 Patent
E-1	Willner I
E-2	O’Sullivan I
E-3	O’Connell II
E-4	Kitts I
E-5	Kitts II
E-6	Eldon I
E-7	Broder 456
E-8	Nguyen 107
E-9	Legacy AdSpam
E-10	Ge
E-11	Mak 466

Google's Claim Chart Exhibits cite to particular teachings and disclosures of the prior art as applied to features of the Asserted Claims. However, persons of ordinary skill in the art generally may view an item of prior art in the context of other publications, literature, products, understanding, and prior art. As such, the cited portions of prior art identified herein are exemplary only. Google will rely on the entirety of the prior art references listed herein, including uncited portions of those prior art references, and on other publications and expert testimony for any purpose, including as aids in understanding and interpreting the cited portions, as providing context thereto, and as additional evidence that the prior art discloses a claim limitation. Google also will rely on the entirety of prior art references listed herein, including uncited portions of the prior art references, as well as other publications not used as prior art, and testimony and documents, to establish bases for and motivations to make combinations of certain cited references that render the Asserted Claims obvious. Specifically, Google will rely upon the identified prior art in its entirety; other prior art identified in future supplements pursuant to the Local Rules and Federal Rules; corroborating references, documentation, products, and testimony, including materials obtained through further investigation and third-party discovery, that demonstrate the invalidating functionality identified in these contentions; references that show the state of the art in the relevant time period (irrespective of whether such references themselves qualify as prior art to the Asserted Claims); and/or expert testimony to provide context to or aid in understanding the cited portions of the identified prior art.

The Claim Chart Exhibits may cite and incorporate by reference prior art references, other relevant material, and/or sections of other charts. These citations are intended to incorporate the referenced information in its entirety. The identification of any patent or patent

publication shall be deemed to include any counterpart patent or application filed, published, or issued anywhere in the world.

The references discussed in the Claim Chart Exhibits may disclose the elements of the Asserted Claims explicitly or inherently, or they may be relied upon to show the state of the art in the relevant time frame. In addition, statements in the Claim Chart Exhibits that it would be obvious to modify the teachings of a reference are not meant to exclude arguments that it would also be obvious to combine the reference with other prior art.

Some of the disclosures cited in certain of the Claim Chart Exhibits are based on Google's understanding of how Plaintiff is interpreting the Asserted Claims for the purpose of its Infringement Contentions (to the extent Plaintiff's contentions can be understood). Google does not intend to and does not adopt Plaintiff's claim interpretations or concede that Plaintiff's claim interpretations are correct. Nothing stated herein or in any Claim Chart Exhibit should be treated as an admission or suggestion that Google agrees with Plaintiff regarding either the scope of any of the Asserted Claims, or any express or implied claim constructions advanced by Plaintiff in its Infringement Contentions or anywhere else, or that any of Google's accused products meet any limitation of the Asserted Claims. Nothing stated herein or in any Claim Chart Exhibit should be construed as an admission or waiver of any particular construction of any claim term. Nothing stated herein or in any Claim Chart Exhibit should be construed as a waiver of any argument available under 35 U.S.C. § 112. Google reserves all rights to challenge any of the Asserted Claims under 35 U.S.C. § 112, including by arguing that they are not supported by the written description, not enabled, indefinite, and/or do not set forth what the inventors regarded as the invention, notwithstanding the disclosure in any Claim Chart Exhibit corresponding to that claim. *See* Section II.A, *infra*. Nothing stated herein or in any Claim Chart Exhibit should be

construed as an admission that the Asserted Claims are directed to patent-eligible subject matter. Google reserves all rights to challenge any of the Asserted Claims under 35 U.S.C. § 101. *See* Section III, *infra*. Nothing stated herein or in any Claim Chart Exhibit should be construed as an admission or waiver with respect to the effective filing date of any of the Asserted Claims.

The alleged “inventions” recited in the Asserted Claims of the Asserted Patents would have been anticipated and/or obvious because the prior art, common knowledge, and the nature of the problems, viewed through the eyes of a person of ordinary skill in the art, suggested the claimed elements. A person of ordinary skill in the relevant fields would have possessed knowledge and skills rendering him or her capable of combining the prior art references with knowledge in the field and common sense. Moreover, the Asserted Claims represent well-known combinations of familiar and pre-existing elements, yielding only predictable results. For example, many of the prior art references describe methods for differentiating between authorized and unauthorized activity—including distinguishing between human and bot activity—to protect access to resources and websites, including methods that could be used instead of, or in addition to, typical CAPTCHA systems. For example, prior art references such as O’Connell I describe “detect[ing] fraud by . . . automated programs during Internet commerce,” by “comparing the user’s interaction” including “keyboard interactions, movement device [e.g., mouse] interactions, and navigation/selection tendencies” as well as “[i]dentification information” including “IP address . . . and cookies.” O’Connell I at [0005], [0020], [0027]-[0029]. As another example, Willner I had disclosed detecting fraud by “automated scripts (clickbots)” by “tracking the movement of a [mouse] cursor on a web page” “to determine if the cursor movement is human-like.” Willner I at 1:9–2:10, 8:20–34. Similarly, Kitts I had disclosed detecting “click fraud” perpetrated by “various automated methods” by analyzing “attributes”

including “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 I at [0003]-[0005], [0021], [0046], [0049]. Indeed, the prior art provided far more detail than the Asserted Patents regarding how to use biometrics and other collected data to distinguish human users from bots. It would have been obvious to a person of ordinary skill in the art to protect websites using well-known techniques for distinguishing human users from bots. Additional reasons that a person of ordinary skill in the art would have been motivated to combine the identified prior art are provided herein and in the Claim Chart Exhibits attached hereto, and in Section II.A.6 (Motivation to Combine Prior Art) below.

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed, Google also will rely on any other combination of any prior art references disclosed herein. Google further will rely upon combinations disclosed within the prosecution history of the references cited herein.

The obviousness combinations set forth in these contentions reflect Google’s present understanding of the potential scope of the claims that Plaintiff appears to be advocating and in no way demonstrate (and should in no way be viewed as) Google’s acquiescence to Plaintiff’s interpretation of the Asserted Claims. Google will amend or supplement these contentions regarding anticipation and/or obviousness of the Asserted Claims as appropriate under the applicable Rules, including in response to further information from Plaintiff or information discovered during discovery. Plaintiff has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that Plaintiff alleges is not disclosed in a particular prior art reference, Google reserves the right

to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time and in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the Asserted Claims obvious.

In an effort to focus the issues, Google has generally cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general technical knowledge. As noted above, Google will rely upon the prior art references identified herein in their entirety, including uncited portions.

Additionally, any reference or combination of references that renders obvious an asserted independent claim also renders obvious any Asserted Claim dependent on that independent claim because every element of such dependent claim was known by a person of ordinary skill at the time of the alleged invention, and it would have been obvious to combine those known elements with the independent claims at least as a matter of common sense and routine innovation.

Furthermore, as noted above, the cited references under 35 U.S.C. § 102(a), (b), (c), and/or (g) include the publications themselves as well as the use of the products and systems described therein. Although Google's investigation continues, information available to date indicates that such products and systems were (1) known or used in the country before the alleged invention of the claimed subject matter of the Asserted Claims, (2) were in public use and/or sale in this country more than one year before the actual or effective filing date of the

Asserted Patents, and/or (3) were invented by another who did not abandon, suppress, or conceal, before the alleged invention of the claimed subject matter of the Asserted Claim. Upon information and belief, these prior art products and systems and their associated references render obvious each of the Asserted Claims.

4. Exemplary Obviousness Combinations

The following charts provide exemplary combinations of prior art that renders the Asserted Claims obvious. However, all the Asserted Claims of the Asserted Patents are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references identified herein as specified in the Claim Chart Exhibits, which identify specific examples of where each limitation of the Asserted Claims is found in the prior art reference, and/or obvious under 35 U.S.C. § 103 in view of the state of the prior art alone, the admitted prior art described in the Invalidity Contentions, and/or in combination with the references and disclosures detailed in Tables 1–3 of the Invalidity Contentions as well as the prior art references identified herein as specified in the Claim Chart Exhibits. As such, Google’s inclusion of exemplary prior art references and combinations listed below does not preclude Google from identifying other invalidating combinations as appropriate.

Claim Chart Exhibits A-1 through A-19: Prior Art References or Combinations for the ’008 Patent

Exhibit	Prior Art Reference or Combinations
A-1	Willner I alone or in combination with one or more of the references in Exhibits A-2–A-19.
A-2	Ge alone or in combination with one or more of the references in Exhibits A-1 and A-3–A-19.
A-3	O’Sullivan I alone or in combination with one or more of the references in Exhibits A-1, A-2, and A-4–A-19.
A-4	O’Connell I alone or in combination with one or more of the references in Exhibits A-1–A-3 and A-5–A-19.
A-5	Krynski alone or in combination with one or more of the references in Exhibits A-1–A-4 and A-6–A-19.

Exhibit	Prior Art Reference or Combinations
A-6	Farahat alone or in combination with one or more of the references in Exhibits A-1–A-5 and A-7–A-19.
A-7	Awadallah I alone or in combination with one or more of the references in Exhibits A-1–A-6 and A-8–A-19.
A-8	Kitts I alone or in combination with one or more of the references in Exhibits A-1–A-7 and A-9–A-19.
A-9	Meek alone or in combination with one or more of the references in Exhibits A-1–A-8 and A-10–A-19.
A-10	Tanzer alone or in combination with one or more of the references in Exhibits A-1–A-9 and A-11–A-19.
A-11	Eldon I alone or in combination with one or more of the references in Exhibits A-1–A-10 and A12–A-19.
A-12	Obviousness combinations for the '008 patent, alone, in combination with one or more of the other references charted in A-12, or in combination with one or more of the other references in Exhibits A-1–A-11 and A-13–A-19.
A-13	Sadagopan 870 alone or in combination with one or more of the references in Exhibits A-1–A-12 and A14–A-19.
A-14	Renaud 706 alone or in combination with one or more of the references in Exhibits A-1–A-13 and A15–A-19.
A-15	Arcot RiskFort alone or in combination with one or more of the references in Exhibits A-1–A-14 and A16–A-19.
A-16	RSA Adaptive Authentication alone or in combination with one or more of the references in Exhibits A-1–A-15 and A17–A-19.
A-17	Bharosa Tracker alone or in combination with one or more of the references in Exhibits A-1–A-16 and A18–A-19.
A-18	BioPassword alone or in combination with one or more of the references in Exhibits A-1–A-17 and A-19.
A-19	Legacy AdSpam alone or in combination with one or more of the references in Exhibits A-1–A-18.

**Claim Chart Exhibits E-1 through E-11:
Prior Art References or Combinations for the '014 Patent**

Exhibit	Prior Art Reference or Combinations
E-1	Willner I alone or in combination with one or more of the references in Exhibits E-2–E-11.
E-2	O'Sullivan I alone or in combination with one or more of the references in Exhibits E-1 and E-3–E-11.
E-3	O'Connell II alone or in combination with one or more of the references in Exhibits E-1–E-2 and E-4–E-11.
E-4	Kitts I alone or in combination with one or more of the references in Exhibits E-1–E-3 and E-5–E-11.
E-5	Kitts II alone or in combination with one or more of the references in Exhibits E-1–E-4 and E-6–E-11.

Exhibit	Prior Art Reference or Combinations
E-6	Eldon I alone or in combination with one or more of the references in Exhibits E-1–E-5 and E-7–E-11.
E-7	Broder 456 alone or in combination with one or more of the references in Exhibits E-1–E-6 and E8–E-11.
E-8	Nguyen 107 alone or in combination with one or more of the references in Exhibits E-1–E-7 and E-9–E-11.
E-9	Legacy AdSpam alone or in combination with one or more of the references in Exhibits E-1–E-8 and E-10–E-11.
E-10	Ge alone or in combination with one or more of the references in Exhibits E-1–E-9 and E-11.
E-11	Mak 466 alone or in combination with one or more of the references in Exhibits E-1–E-10.

5. No Evidence of Any Indicia of Non-Obviousness of the Asserted Claims

The Asserted Claims of the Asserted Patents would have been obvious in view of the prior art combinations set forth in the Claim Chart Exhibits. All of the limitations of the Asserted Claims are taught by these references. To the extent any limitation is not explicitly or inherently disclosed by any item of prior art listed in these Exhibits, the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art on its own as read by one of skill in the art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

Furthermore, there is no evidence of any indicia of non-obviousness, including any long-felt but unsolved need; copying; failure of others; commercial success due to the patented invention; no industry praise; no unexpected results; no industry skepticism and no licensing. Each is addressed in turn below:

No long felt but unsolved need. There was no long-felt but unsolved need that the Asserted Claims solve. The concepts described in the Asserted Patents were all well known

before the alleged invention dates of the Asserted Patents as evidenced by the patents themselves, their file histories and references cited therein, and the prior art identified herein, including those identified in the above-referenced Claim Chart Exhibits. In addition, there was no long-felt but unsolved need because there is nothing particularly compelling about the claimed methods, systems, and apparatus.

No copying. Plaintiff has provided no credible evidence that the alleged inventions of the Asserted Patents were copied, or more specifically, that any functionality that practices the Asserted Patents was copied. Copying “requires evidence of efforts to replicate a specific product.” *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1246 (Fed. Cir. 2010). Here, Plaintiff has not, and cannot, show that Google copied any product that embodies the Asserted Patents. Further, evidence of copying is “not sufficient to demonstrate nonobviousness of the claimed invention” where, as here, there is a “substantial question of validity raised by the prior art references” cited by Google. *Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1366 (Fed. Cir. 2001). As explained in detail in these contentions, the Asserted Patents are rendered obvious by the prior art. Thus, Plaintiff cannot show any nexus between any alleged copying and the merits of the claimed inventions of the Asserted Patents.

No failure of others. Although “[n]onobviousness is suggested by the failure of others to find a solution to the problem which the patents in question purport to solve,” *Symbol Techs., Inc. v. Opticon, Inc.*, 935 F.2d 1569, 1578–79 (Fed. Cir. 1991), this is not such a case. As explained in detail in these contentions, a variety of methods for differentiating between human and bot activity to protect access to resources and websites were well known in the art. Such methods included evaluating data such as CAPTCHAs, mouse movements, keystroke combinations and cadence, time differentials between a display element and a response, 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), and so on. A person of ordinary skill in the art would have been motivated to use such well-known techniques to assess a confidence level that an operator of a client computing device interacting with a server is a human rather than a bot, or to test for the presence of such data to limit or condition access to a server. Furthermore, a person of ordinary skill in the art would have found combining such teachings to be straightforward and predictable.

No commercial success. Plaintiff has not provided any evidence that any alleged success of its products or any other products is due to the alleged inventions claimed in the Asserted Patents. A patentee bears the burden of demonstrating that the relevant commercial success is attributable to the claimed invention “as opposed to other economic and commercial factors unrelated to the technical quality of the patented subject matter.” *Cable Elec. Prods., Inc. v. Genmark, Inc.*, 770 F.2d 1015, 1027 (Fed. Cir. 1985), *overruled on another ground by Midwest Indus., Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356. Here, Plaintiff has not shown and cannot show that the Accused Products’ success is due to the alleged invention of the Asserted Patents. The commercial success of the accused product is unrelated to the purported inventions of the Asserted Patents. Furthermore, if any commercial success is due to any of the concepts disclosed in the Asserted Patents, those concepts are also present in the prior art and thus are irrelevant to the question of obviousness. *See Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1369–70 (Fed. Cir. 2011) (“If commercial success is due to an element in the prior art, no nexus exists.”); *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) (“Where the offered secondary consideration actually results from something other than what is both claimed and novel in the

claim, there is no nexus to the merits of the claimed invention.”); *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1312 (Fed. Cir. 2006) (“[I]f the feature that creates the commercial success was known in the prior art, the success is not pertinent.”).

No industry praise. Plaintiff has presented no evidence of industry praise for the alleged inventions of the Asserted Patents or any functionality that allegedly practices the Asserted Patents. To the extent any praise is related to any functionality that allegedly practices the Asserted Patents, that praise is not due to the allegedly novel features of the Asserted Patents, but instead only to features present in the prior art, which is not a sufficient nexus to be relevant to the question of industry praise for purposes of obviousness. *See Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008).

No unexpected results. There is no evidence of any unexpected results when the elements of the Asserted Claims were combined. Instead, as discussed above, the concepts claimed in the Asserted Patents were already combined or would have been obvious to combine in the same manner as the Asserted Claims. These prior art systems and products, as described in in these contentions, disclosed the same combinations of elements, and the same results of such combinations, that are recited in the Asserted Claims of the Asserted Patents. Thus, there were no unexpected results that arose from combining the well-known elements in the Asserted Claims of the Asserted Patents.

No industry skepticism. Plaintiff has presented no evidence that others were skeptical before the alleged invention date of the Asserted Patents, nor can it. In fact, there was no industry skepticism concerning the claimed concepts that predates the Asserted Patents. Instead, many companies and individuals were already using the concepts claimed in the Asserted Patents. Thus, there was no industry skepticism that using or combining these well-known prior art

concepts would be viable; others in the field were already combining them in the same manner as arranged in the Asserted Claims. For example, as noted above, others before Plaintiff, had implemented methods for differentiating between human and bot activity to protect in order to prevent fraudulent activity, spam, and abuse. Well-known methods of bot detection included presenting issued data from a server to the client computing device and monitoring and comparing at least some of the data generated at the client computing device in response to the issued data and assigning a confidence level that the user was a human rather than a bot. Prior art methods also included conditioning access to websites or resources based on the presence or absence of data likely to be associated with human activity as opposed to bots, such as CAPTCHAs, mouse movements, keystroke combinations and cadence, and time differentials between a display element and a response. Prior art methods also included evaluating data such as 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), and so on.

Simultaneous Invention. Individuals working independently of the Asserted Patents' named inventor simultaneously or near-simultaneously invented the alleged invention of the Asserted Claims of the Asserted Patents. Such evidence supports a finding that the Asserted Claims would have been obvious to a person of ordinary skill in the art at the time of the invention. *See Geo. M. Martin Co. v. Alliance Mach. Sys. Int'l, LLC*, 618 F.3d 1294, 1305 (Fed. Cir. 2010) ("Independently made, simultaneous invention, made 'within a comparatively short space of time,' are persuasive evidence that the claimed apparatus 'was the product only of ordinary mechanical or engineering skill.'") (citing *Concrete Appliances Co. v. Gomery*, 269

U.S. 177, 184 (1925)); *see also Ecolchem, Inc. v. So. Cal. Edison Co.*, 227 F.3d 1361, 1379 (Fed. Cir. 2000).

6. Motivation to Combine Prior Art

A motivation, teaching, or suggestion to combine the prior art identified exists for each obviousness combination identified above. In *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007), the Supreme Court held that a claimed invention can be obvious even if there is no teaching, suggestion, or motivation for combining the references to produce the claimed invention. *KSR* holds that patents based on new combinations of elements or components already known in a technical field may be found obvious. Specifically, the Court in *KSR* rejected a rigid application of the “teaching, suggestion, or motivation to combine” test. *Id.* at 418–19. “In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. What matters is the objective reach of the claim.” *Id.* at 419. “Under the correct analysis, any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *Id.* at 420. The Court noted that “[c]ommon sense teaches, however, that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *Id.* The Court further stated that “[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *Id.* at 416. “When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.” *Id.* at 421.

One of skill in the art would have had reason to or been motivated to combine the references identified herein because, for example, the combinations fall into one or more of the following categories:

- A combination of elements known in the prior art according to known methods to yield a predictable result;
- A combination that is a simple substitution of one or more known elements for another to obtain a predictable result;
- A combination that involves using a known technique to improve a similar device or method in the same way;
- A combination that involves applying a known technique to a known device or method ready for improvement to yield a predictable result;
- A combination that results from a finite number of identified, predictable solutions with a reasonable expectation of success, such that the solution was one which was “obvious to try”;
- A combination that results from known work in one field of endeavor prompting variations of it for use either in the same field or a different field based on design incentives or other market forces in which the variations were predictable to one of ordinary skill in the art; and
- A teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine the teachings of various prior art references to arrive at the claimed invention.

Further, the Federal Circuit has held that a motivation to combine references takes into account the scope of the patent claims and content of the prior art and “may include recourse to logic, judgment, and common sense, in lieu of expert testimony.” *Wyers*, 616 F.3d at 1239. In addition, the Federal Circuit has held that an implicit motivation to combine references exists when the alleged improvement in the claimed invention is technology-independent:

[A]n implicit motivation to combine exists not only when a suggestion may be gleaned from the prior art as a whole, but when the “improvement” is technology-independent and the combination of references results in a product or process that is more desirable, for example because it is stronger, cheaper, cleaner, faster,

lighter, smaller, more durable, or more efficient. Because the desire to enhance commercial opportunities by improving a product or process is universal—and even common-sensical—we have held that there exists in these situations a motivation to combine prior art references even absent any hint of suggestion in the references themselves. In such situations, the proper question is whether the ordinary artisan possesses knowledge and skills rendering him *capable* of combining the prior art references.

DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co., 464 F.3d 1356, 1368 (Fed. Cir. 2006). Trivial improvements that would have been a matter of common sense to one of ordinary skill in the art are obvious. *W. Union Co. v. MoneyGram Payment Sys., Inc.*, 626 F.3d 1361, 1372 (Fed. Cir. 2010).

A person of ordinary skill in the art at the time of the claimed inventions had reason to combine or modify one or more of the references listed and charted in Google’s Claim Chart Exhibits in light of the knowledge of a person of ordinary skill at the time and information in the prior art references cited herein.

Additional evidence establishing that there would have been a motivation to combine the prior art references identified above and herein includes the interrelated teachings of multiple prior art references; the effects of demands known to the design community or present in the marketplace; the existence of a known problem for which there was an obvious solution encompassed by the Asserted Claims; the existence of a known need or problem in the field of the endeavor at the time of the invention(s); and the background knowledge that would have been possessed by a person having ordinary skill in the art.

Further, the prior art references explicitly or implicitly reference other prior art references, share common authors or inventors, were published in the same journals, presented at the same conferences, and/or were developed at common companies, schools, or organizations, all of which would motivate one of skill in the art to combine them. These references are also within the field of the Asserted Patents and are directed to similar subject matter within that

field. Additionally, any products, devices, or processes described in the references existed and/or were invented before or during the period in which the claimed inventions were developed, providing further motivation to combine them.

Thus, the motivation to combine the teachings of the prior art references disclosed herein is found in the references themselves and: (1) the nature of the problem being solved, (2) the express, implied and inherent teachings of the prior art, (3) the knowledge of persons of ordinary skill in the art, (4) the fact that the prior art is generally directed toward bot detection for the purpose of enhancing web security and minimizing user friction, and (5) the predictable results obtained in combining the different elements of the prior art—e.g., using known techniques for differentiating between human and bot activity to protect access to resources and websites.

The following discussion of prior-art bot detection and related technology provides further support for Google’s contentions. The motivations to combine discussed herein, including in the Claim Chart Exhibits, are exemplary and subject to further investigation and discovery, including third-party and expert discovery. Further rationale and support for motivations to combine various types of references can be found in at least the specifications of the Asserted Patents, their prosecution history, and prior art identified above.

(a) Unauthorized Use of Computerized Resources Was a Known Problem, as Were Methods of Addressing It

By way of background, the prior art describes the explosion in popularity of the Internet and the corresponding rise of fraudulent and abuse activity online.⁶ Common types of Internet fraud described in the prior art include unauthorized, illegitimate, or just undesirable access to and/or interaction with computerized resources. For example, resources hosted on a network

⁶ Renaud at [0001]-[0004].

such as the Internet may be intended for only a specific user or set of users; or a particular user may have the ability to perform transactions that others cannot (*e.g.*, economic transactions).⁷ In either case, it is important to verify that the purported user of the internet resource is who she claims to be. A related issue involves access to computerized resources by bots. Some computerized resources are meant to be accessed exclusively by human users. Allowing bots to access such resources is undesirable because it may consume limited network resources that could otherwise be devoted to legitimate activity, facilitate fraudulent or abusive conduct (including automated scraping, account creation, or transaction manipulation), and degrade system performance and reliability.⁸ Allowing bots to access such resources may also skew popularity or usage metrics, which has a deleterious effect on certain business practices such as search engine placement or pay-per-click (“PPC”) advertising.⁹ It was well understood in the art, therefore, that it was advantageous to assess and verify whether a user is a human or a bot.

The prior art also describes well-known methods for authenticating human users and distinguishing humans from bots. Methods for authenticating humans and detecting bots employed similar techniques based on the same sets of information, including information regarding a user’s machine or network connection—such as IP address, user agent, cookies, etc.—or the user’s interaction with her machine—such as mouse movements or keystrokes.¹⁰ A relevant artisan, therefore, would have understood, for example, that methods for authenticating

⁷ Broder at [0002], [0007]-[0009]; Eldon at 1-4; Goodman at [0001]-[0005]; Gusler at 1:13-2:27; O’Connell I at [0003];

⁸ Afergan at [0013]; Awadallah II at [0002]-[0005]; Sadagopan 870 at 1:59-67.

⁹ Broder at [0002]-[Ge at [0004]-[0010]; Krynski at 1:11-24; O’Sullivan I at [0002]-[0004]; Sadagopan at 1:23-2:6.

¹⁰ *See generally* Ge; *see also* Awadallah II at [0006]-[0009]; O’Connell I at [0002]-[0005]; O’Sullivan I at [0001]-[0011].

a human user could be adapted to distinguish humans from bots. Accordingly, a relevant artisan would have been motivated to combine prior art teachings related to human authentication and bot detection, and would have had a reasonable expectation of success in doing so.

**(b) Methods for Protecting Computerized Resources and Websites
By Distinguishing Between Human-Generated and Bot-
Generated Web Traffic Were Well Known, As Expressly
Admitted by Plaintiff**

An extensive body of prior art described a variety of methods for differentiating between human and bot activity to protect access to computerized resources and websites, including methods that could be used instead of, or in addition to, typical CAPTCHA systems. For example, prior art references such as O’Connell I describe “detect[ing] fraud by . . . automated programs during Internet commerce,” by “comparing the user’s interaction” including “keyboard interactions, movement device [e.g., mouse] interactions, and navigation/selection tendencies” as well as “[i]dentification information” including “IP address . . . and cookies.”¹¹ As another example, Willner I had disclosed detecting fraud by “automated scripts (clickbots)” by “tracking the movement of a [mouse] cursor on a web page” “to determine if the cursor movement is human-like.”¹² Similarly, Kitts I had disclosed detecting “click fraud” perpetrated by “various automated methods” by analyzing “attributes” including “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.”¹³

Indeed, as discussed in Section II.A.1 (Admitted Prior Art) above, the Asserted Patents acknowledge that CAPTCHAs (Completely Automated Public Turing test to tell Computers and

¹¹ O’Connell I at [0005], [0020], [0027]-[0029].

¹² Willner I at 1:27–2:10, 8:20–60.

¹³ Kitts I at [0003]-[0005], [0021], [0046], [0049].

Humans Apart) were widely used in the prior art to prevent abuse, with visual CAPTCHAs in use “as the primary test by nearly every top Internet site, including Yahoo, Google, You Tube, Microsoft’s Live ID, MySpace, Facebook, Wikipedia, Craigs List,” and so on. ’008 patent at 1:57–60.

Even before the earliest claimed priority date for the Asserted Patents, it was known that CAPTCHAs might not be the most desirable solution in some circumstances, as human users do not want to solve quizzes every time they access a web page, and CAPTCHAs therefore discourage legitimate website visitors from interacting with the site.¹⁴ In addition, CAPTCHAs could be defeated by tricking or even hiring real people to solve CAPTCHAs.¹⁵ A person of ordinary skill in the art therefore would have been motivated to supplement or replace CAPTCHAs by collecting information about the user passively (e.g., by collecting available information from the client device or the computing environment in which the device operates) or actively (e.g., by having the client answer queries or by using JavaScript event listeners). The skilled person would have been familiar with such methods. Indeed, methods for distinguishing human users from bots, both passive and active, were already in wide use well before the priority date. Ad networks, in particular, were using hundreds or even thousands of passive and active signals to determine whether HTTP requests might be generated by a bot instead of a human.¹⁶

(c) Passive Techniques for Differentiating Between Humans and Bots Were Well Known in the Prior Art

A variety of techniques for the detection of bots through passive means—that is, without sending any new information to the client computing device or requiring explicit human

¹⁴ Park.

¹⁵ 11/23/2005 W3C Working Group Note.

¹⁶ M. Jakobsson at 340; *see generally* Ge, Kitts I, Motsinger, and Tan.

interaction like a CAPTCHA—were widely used before the earliest claimed priority date in 2007.¹⁷

For example, a standard way of detecting bots was to examine the HTTP request messages sent to a web server. Access by well-known bots could be detected by comparing their IP address and user agent fields of their HTTP request messages against those of known bots, whether benign (e.g., search engines and link checkers) or malicious (e.g., clickbots).¹⁸

Another method of detecting bots was to look for sessions that have a large number of HTTP requests with unassigned referrer fields. The referrer field is provided by the HTTP protocol to allow a web browser to specify the address of the web page that contains the link the client followed to reach the current requested page. For example, whenever a user requests the page <http://www.xyz.com/A.html> by clicking on a hyperlink found at <http://www.xyz.com>, the user's browser will generate an HTTP request message with its referrer field assigned to <http://www.xyz.com>. Because most bots do not assign any value to their referrer fields, these values appears as “-” in the web server logs.¹⁹

Yet another method for distinguishing humans from bots took advantage of the fact that many bots, such as web crawlers, scrapers, and click-fraud generators, do not download presentation-related information (e.g., cascading style sheet (CSS) files, embedded images) or JavaScript files because they do not need to display the page or execute the code.²⁰ Similarly, because web crawlers tend to use a breadth-first search strategy to retrieve as many files as possible in a short time, tracking the total number of pages requested and the order in which the

¹⁷ See generally M. Jakobsson at 344–45.

¹⁸ Tan at 195.

¹⁹ Tan at 200.

²⁰ Tan at 213; Park.

pages are requested may help identify bots. In addition, temporal attributes of the requests—such as the timestamps of the requests, the total time of the session, the average time between two HTML requests, and the standard deviation of time between requests—also can be used to distinguish bots from humans.²¹

Additionally, computer cookies were used to distinguish humans from bots. A cookie is a file that a server may leave in a client’s memory for later examination or analysis.²² Cookies can be used to identify a particular user and associate multiple user requests to a webserver into a single session.²³ Thus a server may examine a user’s cookie and compare it to a database of known bots, or may analyze the number and frequency of transactions associated with that cookie to determine whether the user is behaving like a bot.²⁴ Use of cookies in this manner—to authenticate users and distinguish them from bots—were prevalent and well known.²⁵ It was also known that a user’s treatment of cookies could indicate whether the user was a bot or human. It was known that a user who disallows setting cookies, routinely deletes them, or modifies them could likely be a malicious or a bot.²⁶

(d) Techniques for Monitoring Mouse Movements and Keystrokes to Distinguish Humans from Bots Were Well Known in the Prior Art

Other methods of detecting bots were “active,” in the sense that they involved acquiring data that the client computing device ordinarily would not store. One such method involved

²¹ Tan at 213–14. For example, not surprisingly, human traffic tends to peak during the day. *Id.*

²² Lillibridge 9:16-17.

²³ *See* Ge at [0008], [0061]; Afergan at [0011].

²⁴ Ge at [0055]-[0061], [0082]-[0084].

²⁵ *See, e.g.,* Ge at [0055]-[0061], [0082]-[0084]; Greene at [0094]-[0105]; Jakobsson at [0008]-[0011]; Kitts I at [0047].

²⁶ *See, e.g.,* Motsinger at 42:34-44:39; Krynski 7:63-8:4.

detecting mouse and keyboard activity by embedding custom JavaScript in the pages served to the client. This method took advantage of the fact that humans may use a mouse or keyboard to access servers, whereas bots do not need to generate mouse or keyboard activity.²⁷ This was especially true in the early 2000s before smart phones were prevalent. Thus, when a server received evidence of mouse movement or keyboard typing from the client computing device, it could assume that a human was using the client computing device.

For example, using JavaScript, a hyperlink in a web page could be used to detect many kinds of events involving interactions with the mouse. The `onMouseMove` event handler (also known as `mousemove`) was called whenever the mouse was moved while it was over a link or other object. Similarly, the `onMouseOver` event handler could detect when your mouse moved over a link and the `onMouseOut` event handler could detect when your mouse moved off of it. The `onClick` event handler knew when you clicked down on a link. The `onMouseDown` event handler was triggered when a mouse button was pressed down while the mouse was over the link (and the `button` property could track which mouse button—right or left—was clicked); and the `onMouseUp` event handler was triggered when the mouse button was lifted up again. The `onClick` event handler was triggered whenever an `onMouseDown` event was followed by an `onMouseUp` event.²⁸ All of these mouse event handlers were available in JavaScript 1.2+, and Jscript 3.0+ and were supported by browsers such as Internet Explorer and Netscape Navigator.²⁹

²⁷ See generally Jain I at 11, 213–224 (describing how keystroke dynamics can be used to authenticate/verify access to computer systems and networks); see also Willner I, Ge, O’Connell I, O’Sullivan I, Awadallah I, and Tanzer.

²⁸ See, e.g., Thau at 53.

²⁹ See, e.g., Vincent at 965, 975–77.

Keyboard event handlers also were well known. For example, the `onKeyDown` (or `keydown`) and `onKeyUp` (or `keyup`) event handlers created an event object that stored which key had been pressed (or unpressed) and whether or not any special keys (`ALT`, `CTRL`, or `SHIFT`) were pressed at the same time.³⁰ The `keydown` event fired when the user initially depressed a key, and the `keyup` event fired when the user released the key. The `keypress` event handler could be used to fire repeatedly while the user had a key depressed. Like the mouse event handlers discussed above, all of these keyboard event handlers were available in JavaScript 1.2+, and Jscript 3.0+ and were supported by browsers such as Internet Explorer and Netscape Navigator.³¹

Such event handlers helped to make web pages more dynamic, although keyloggers and other event handlers also could be used by malicious attackers to steal passwords, banking credentials, and other sensitive data. Indeed, the Asserted Patents acknowledge that prior art programs, including both internet browsers and malware applications, were capable of logging and transmitting a user's mouse movements and keystroke combinations. '008 patent at 4:3–35 (“Existing available browsers and operating systems provide the means necessary to temporarily install logging code, if such is elected.”).

The 2007 article by Ahmed and others in *IEEE Transactions on Dependable and Secure Computing* (“2007 Ahmed”) further confirms that monitoring mouse movement as a behavioral

³⁰ See, e.g., Thau at 250, Zakas at 284, 2007 Ahmed.

³¹ See, e.g., Vincent at 974. Prior art web browsers also supported a variety of event handlers for detecting the actions of website visitors in addition to mouse movements and keystrokes. Other examples of events that could be tracked at least as early as 2000 included whether the value of a form field was modified during its last access, whether a page element had been double-clicked, whether a page element had received or lost focus, whether text had been selected by the user, whether the Submit button had been activated, whether the browser was navigating away from the current page. See, e.g., Edwards at 229–44, 393–401; Flanagan at 5–9, 248–50, 388–436; Koch at 283–348; Moncur at 131–145; Powell at 297–344; Thau at 53–55, 57, 250–59; Vincent at 907–61; Zakas at 261–301.

signal for distinguishing human users was well known well before the priority date. Specifically, Ahmed describes collecting “raw mouse data” over extended user sessions and extracting behavioral features such as movement speed, direction, distance, and timing to build a “mouse dynamics signature” for a user. These features are derived from continuous tracking of mouse actions—including “mouse movement,” “point-and-click,” and “drag-and-drop” events—and are analyzed to model user behavior and distinguish between different users. Ahmed further explains that such data is captured through a “data interception unit” that “intercept[s] and convert[s] all mouse movements and actions into meaningful information” for downstream analysis. Ahmed also discloses generating a “confidence ratio” based on the analyzed mouse dynamics data to quantify the likelihood that observed behavior corresponds to a particular user. This disclosure demonstrates that, as of 2007, it was routine to (i) collect detailed mouse movement data from a client device, (ii) analyze that data using statistical or machine-learning techniques, and (iii) compare it against behavioral models to identify or verify a human user.³²

The 2007 article by Michal Choras and Piotr Mrockowski presented at the Third International Conference on Web Information Systems and Technologies - Internet Technology (“2007 Choras”) likewise demonstrates that, prior to the alleged invention, it was well understood to collect and analyze user interaction data at a client device and compare it to stored behavioral models to determine whether the user is legitimate. Choras describes a web-based authentication system in which a client-side component (implemented as a web applet) collects “keyboard statistics” during a login session and transmits those data to a server for analysis. The collected data include detailed timing information such as key press and release events, inter-keystroke delays, and digraph/trigraph durations—i.e., “active data relating to interactions of the

³² 2007 Ahmed.

client computer” with a web interface. On the server side, Choras performs statistical analysis by generating feature vectors and comparing them against “model counterparts stored in database,” which are derived from prior user sessions and adapt over time to reflect evolving human behavior. This comparison yields a determination of whether the current user’s behavior matches the expected human profile, thereby controlling access to the system (i.e., allowing or denying login).³³

The 2004 article by Maja Pusara and Carla Brodley, published in *IVizSEC/DSEC'04* (“2004 Pusara”) likewise discloses a system that collects user interaction data at a client device, transmits that data to a server, and analyzes it against previously learned behavioral models to determine whether the current user is legitimate. Specifically, Pusara describes capturing “mouse movement” data and “mouse events” (including clicks and cursor trajectories) from the client computer during a user session, i.e., active data reflecting interactions with an application interface. The system extracts features such as distance, speed, angle, and statistical summaries over time windows, and uses these features to construct a behavioral profile for each user based on prior observations. During operation, newly collected interaction data are compared against this learned “model of normal behavior,” and if the current behavior “deviates sufficiently” from the stored model, the system flags the activity as anomalous and may require re-authentication or deny access. Pusara further explains that this analysis may produce a “confidence value” for each observation and apply thresholds or smoothing over multiple observations to determine whether the user should be treated as legitimate or anomalous.³⁴

³³ 2007 Choras.

³⁴ 2004 Pusara.

The 2006 article by KyoungSoo Park and Kang-Won Lee presented at the 2006 USENIX Annual Technical Conference (“2006 Park”) and the article by Srikanth Kandula and others presented at the 2nd Symposium on Networked Systems Design & Implementation (“2005 Kandula”) further demonstrate that it was well known to (i) collect client-side interaction data, (ii) analyze that data to distinguish humans from automated processes, and (iii) condition access or require additional verification (e.g., CAPTCHA) based on that analysis. Park discloses embedding JavaScript in web pages to “detect . . . mouse movement or keyboard typing from the client,” thereby causing the client computer to generate and transmit active interaction data (e.g., event-triggered requests containing identifying parameters) back to the server.³⁵ The server then evaluates this data—e.g., whether a correct event-driven request with a matching key is received—and classifies the session as human or robot, optionally combining this with additional behavioral analysis (including request patterns and machine-learning-based classification) in a staged process that first performs “fast analysis” and then a “careful decision algorithm” using learned models of human browsing behavior.³⁶ 2005 Kandula similarly teaches a multi-stage authentication framework in which the server generates and evaluates responses to CAPTCHA challenges, using the client’s success or repeated failure to meet thresholds (e.g., number of unsolved tests) as a basis for determining whether the client is human or a bot and for controlling access.³⁷ In particular, Kandula describes an initial stage in which clients are presented with graphical tests and their responses are evaluated, followed by subsequent stages in which

³⁵ 2006 Park at 255-56.

³⁶ *Id.* at 256-59.

³⁷ 2005 Kandula at 287-91.

continued failures (or successes) are aggregated and used to generate a decision about whether to admit or block the client.³⁸

An example of a prior art website that employed JavaScript event handlers for detecting mouse movement and keystrokes for the purpose of differentiating human and bot traffic was the publicly available CoDeeN peer-to-peer web cache proxy server system

(<https://codeen.cs.princeton.edu/>), which implemented this capability as early as January 2006.³⁹

(e) Other Active Detection Techniques for Distinguish Humans from Bots Were Well Known in the Prior Art

Other prior-art techniques for identifying bots included deliberately planting information on a web page and observing the user's response to information. For example, many goal-oriented robots—such as web crawlers, scrapers, and click-fraud generators—may not download presentation-related information (e.g., cascading style sheet (CSS) files, embedded images) or JavaScript files because they do not need to display the page or execute the code. A server trying to detect bots could embed an empty CSS File for each HTML page and observe if the CSS file gets requested. Since CSS files are only used when rendering pages, this technique can catch many special-purpose robots that ignore presentation-related information. Alternatively, the server might use silent audio files or 1-pixel transparent images for the same purpose. Another related technique is to place a hidden link in the HTML file that is not visible to users and see if the link is fetched. If the link is placed on a transparent image that is invisible to human users, humans should not fetch it, but bots might.⁴⁰

³⁸ *Id.*

³⁹ See Park; CoDeeN: Wayback Machine; <https://en.wikipedia.org/wiki/CoDeeN>.

⁴⁰ See Park. Interestingly, the authors of this study also noted that “[a] serious hacker could implement a bot that could generate mouse or keystroke events if he or she knows that a human

(f) **Methods for Assessing a Confidence Level that a User Was a Human Rather than a Bot Were Well Known in the Prior Art**

The prior art also provided methods for assessing a confidence level that an operator of a client computing device interacting with a server, such as an ad server, was a human being rather than an autonomic computer application. For example, Kitts I described calculating a “quality score” corresponding to “the *probability* that a selection of an advertisement impression is initiated from a user or by software attempting to induce click fraud.” Kitts I at [0031]-[0032], [0049], [0067]-[0068]. A relevant artisan would have understood, including based on the prior art discussed above, that determining whether the user is a bot or not, as opposed to a human acting with fraudulent or malicious intent, would have been advantageous and relatively easy to do. O’Sullivan I similarly described a method of fraud detection in which “[i]nstances where the mouse click occurred very quickly and without crossing a pixel cluster would be judged to be click fraud with a *high confidence level*.” O’Sullivan I at [0029], [0032], [0047]. Willner I likewise described a method for detecting click fraud that includes tracking the user’s mouse movements on a web page prior to clicking on an advertisement, analyzing the user’s mouse movements, “determining a *confidence level*” that is “high” for human-like movement and “low” for machine-like movement, and “denying the click in response to the confidence level being at a level indicating the possible click fraud attempt.”⁴¹

In another example, ad networks developed methods of “smart pricing” in which they assigned confidence levels representing the likelihood that a click was human. The usual cost-per-click (“CPC”) for such traffic could then be discounted by a smart pricing multiplier, also

activity detection mechanism has been implemented by a site. Although we are not aware of any such intelligent bots today, we may need to address such issues in the future.” *Id.*

⁴¹ Willner I at claim 1; *see id.* at Abstract, 9:32–10:18, 10:41–60, & FIGs. 4-5, and 8.

called a click cost multiplier (“CCM”).⁴² Alternatively, ad buyers could specify a desired confidence level for their ads to be shown, or specify reduced bids for lower confidence levels.⁴³

Indeed, people have been assigning probabilities to all kinds of determinations for centuries. Well before the earliest priority date of the Asserted Patents, a person of ordinary skill in the art would have been familiar with well-known concepts and techniques from applied statistics including hypothesis testing, classification, and confidence levels. In particular, a person of ordinary skill would have been familiar with hypothesis testing with a single (null) hypothesis, and hypothesis with two competing hypotheses (null and alternative). Similarly, a person of ordinary skill would have been familiar with binary classification (assigning an observation into one of two categories). The skilled person also would have been familiar with the use of confidence levels to measure the probability that decisions yield correct answers. All of these concepts are explained in basic textbooks for statistics, such as Richard J. Larsen and Morris L. Marx’s *An Introduction to Mathematical Statistics and Its Applications* (4th ed. 2006).⁴⁴

A person of ordinary skill in the art would have known that one standard way to solve classification and hypothesis-testing tasks is to collect sample data and compare it against a model. Such a person would have known that one technique is to compute a value from the sample data, and from this value determine a confidence level for correctly classifying the sample. Similarly, such a person would have known how from this value to determine a confidence level for correctly rejecting the null hypothesis. The field of computing science

⁴² Jakobsson at 346.

⁴³ Kitts at [0060]-[0061].

⁴⁴ See generally Larsen.

naturally lends itself to many such determinations, including in the context of human-bot differentiation, and a person of ordinary skill in the art would have understood generating a probability value to be a straightforward, conventional, and obvious way of representing the confidence level in a computer-implemented system.⁴⁵

In particular, a person of ordinary skill in the art would have understood that collected interaction data—such as keystrokes, mouse activity, and other user-input activity—could be compared against sample or model data derived from prior human interactions with the same website or even the same webpage. For example, Renaud 706 discloses analyzing current user interaction data against “previously stored data associated with the user account” to generate a composite security status score—that is, a quantified assessment of whether the activity is consistent with expected human behavior.⁴⁶ It further explains that the system constructs a risk measure by combining multiple behavioral and contextual inputs into a unified score reflecting the likelihood of legitimate versus fraudulent activity.⁴⁷ Renaud 706 also teaches that the applicable thresholds or access criteria may be set by the institution or system administrator.⁴⁸ Eldon I likewise teaches tracking website-interaction signals including “use of the mouse pointer,” cursor movement, “typing speed,” and “number of corrections made while entering

⁴⁵ See Afergan at [0040], [0155] (corroborating a person of ordinary skill’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,” and “[b]y combining one or more attributes using a weighted algorithm, a Valid User Score (VUS) is generated to represent the service provider’s confidence that this user agent is associated with a normal human user.”).

⁴⁶ Renaud 706 at Abstract.

⁴⁷ *Id.* at [0031].

⁴⁸ See *id.* at claim 4 (disclosing receiving a “system administrator-specified value” and processing the access data “based on at least one configurable threshold,” and that the weighted risk functions and thresholds “are configurable by the system administrator”).

text,” and then determining a fraud risk by “combining information regarding the present interaction with said at least one website with previously recorded behaviour profiles of said entity” or with profiles of prior users who visited that website or other monitored websites.⁴⁹

Kitts II reinforces the same point. It teaches determining whether a request is likely robotic by using the “nature of the request” together with “historic behavior related to the requesting user” to assign a score, and further explains that historic user behavior is stored and used to train the scoring module for future evaluations.⁵⁰ Kitts II also discloses comparing current request behavior against known traffic patterns and threshold values associated with robotic traffic, including measured user behaviors such as click location relative to expected coordinates on the page.⁵¹ O’Connell II similarly shows that it was known to compare newly collected browser-interaction data—including keystroke timing, mouseover behavior, and cursor movement tendencies—to prior-session interaction data for the same user and to compute a resulting “pattern matching score” from that comparison.⁵² It explains that the score reflects a comparison between current-session interaction data and a stored “user-browser interaction profile” built from prior sessions.⁵³

⁴⁹ Eldon I at 23:25-24:11, 29:10-32:5, 38:16-40:10, and claim 23.

⁵⁰ Kitts II at [0007].

⁵¹ *Id.* at [0027]-[0029], [0041]-[0042], [0048]-[0049], [0052]-[0053], [0056]-[0062], [0088]-[0089]; *see also* Samuels 338 at [0033]-[0056], Fig. 4 (comparing attributes of a current session against a user’s own historical session data to calculate an improbability score: it “compares the session statistics of the current login with session statistics for previous sessions of the current user ID” and then computes individual Network, Browser, Time-of-Day, and Frequency scores that are combined into a composite score).

⁵² O’Connell II at [0009], [0026]-[0028], [0034]-[0035], [0044]-[0049], and Fig. 6.

⁵³ *Id.*

Mak 466 provides still further support. It expressly teaches comparing current manually collected interaction data to prior-session model data and deriving a score from that comparison. In particular, it states that received user input, including manual manipulation of a mouse or other input device in pursuit of a displayed objective, “is then compared to a user profile representing prior manual manipulation,” and it discloses recording and comparing cursor movement patterns, hover patterns, clicking patterns, and path characteristics against “previously-stored parameters” in the user profile.⁵⁴ Mak 466 is especially probative because it discloses that sessions for “those same screens” are compared to prior sessions for those screens, and it further teaches generating probabilities or scores, including heat-graph based scores, to assess whether the current session matches the stored profile.⁵⁵

In analogous circumstances, Krynski teaches building model data from previous human interactions with a server. Krynski recognizes that illegitimate use of network resources is undesirable.⁵⁶ To combat illegitimate bot use of web resources, Krynski teaches a system for automatically classifying user sessions based on observed user activity.⁵⁷ To evaluate a given session, Krynski teaches comparing the monitored session data with session models.⁵⁸ Krynski explicitly teaches that session models “may be derived based on analysis of historical data associated with interactions with the one or more servers.”⁵⁹ “The number of probability models 412 and the specific types of legitimate or illegitimate use that are modeled may be depend on

⁵⁴ Mak 466 at Abstract, [0029], [0040]–[0086], Fig. 3.

⁵⁵ *Id.* at [0018], [0046]–[0049], [0052].

⁵⁶ Krynski at 1:11–24.

⁵⁷ *Id.* at 2:63–3:20.

⁵⁸ *Id.* at 4:24–42, 8:5–28.

⁵⁹ *Id.* at 8:14–16.

the nature of the servers. For example, illegitimate users of a news and information website server may be of a different type (and thus have a different probability model 412) than illegitimate users of a storefront website server.”⁶⁰ Krynski further explains that, for these models, “parameter values and their distributions used to calculate the probabilities can be determined based on sample user activity data related to the network resources (e.g., the search engine). In a particular embodiment, unsupervised parameter learning can be used.”⁶¹

Taken together, these disclosures show that it was conventional to compare newly collected interaction data—including user-input behavior such as keystrokes and mouse behavior—to prior-session behavioral data from the same user, website, or page, and to compute a score based on that model data. At a minimum, they confirm that a person of ordinary skill in the art would have understood such comparisons and scoring to be well-known techniques for distinguishing expected human behavior from suspicious or automated activity.

(g) It Was Well Known to Repeat Data Collection and Analysis

It was well known in the prior art to repeat data collection and analysis steps to authenticate human users and/or determine whether they are bots. When calculating the probability of an event based on evidence—for instance, the probability that a user is Jane Smith, or the probability that the user is a bot—repeating that calculation when new evidence is available is an elementary application of Bayesian statistics.⁶² Such techniques were well known long before the priority date of the Asserted Claims. It was also well known to employ these

⁶⁰ *Id.* at 8:23-28.

⁶¹ *Id.* at 10:51-55.

⁶² Eldon I at 7-10, 31, 35-40; Larsen at 410-420; *see also* Larsen at 344-426.

techniques when authenticating human users and detecting bots.⁶³ Such repeated analysis is advantageous when the underlying determination is probabilistic and uncertain.

It was also common practice to request and collect additional information from a user on which to perform this analysis. For example, in the context of human authentication and bot detection, it was well recognized that an initial determination that a user was authentic may not cover an entire session—*e.g.*, if a user were subject to man-in-the-middle attack where her session was hijacked by another human or a bot.⁶⁴ It was therefore advantageous to collect data multiple times during a user’s session to determine whether she was still authentic. In another example, an initial analysis may be indeterminate, so additional information would be necessary in order to make a more confident prediction before acting on that analysis.⁶⁵

And it was well known to compare the results of these analyses. For example, scores from multiple users could be compared to assess how a given user compares to other users.⁶⁶ Or scores from a single user could be compared over time to assess whether it departs from norms for a given user and to determine trends.⁶⁷

Additionally, it was well known in the art and obvious to perform a first analysis of a user’s activity and, if the user’s activity seems suspicious, to administer additional tests, including a CAPTCHA, to determine whether the user is a human or bot. For example, Farahat

⁶³ Eldon I at 31-40; Arcot RiskFort; Bharosa Tracker; BioPassword; RSA Adaptive Authentication;

⁶⁴ Ramanathan at [0032]; Rijsinghani at [0034]-[0035], [0064]; Renaud at [0031].

⁶⁵ Broder at [0059]; Greene at [0060]-[0065]; O’Connell I at [0056]-[0057]; O’Sullivan II at [0032].

⁶⁶ Motsinger at 47:61-48:21, 49:12-38; Sadagopan at 7:22-44; Rijsinghani at [0013], [0035], [0069].

⁶⁷ Eldon I at 35-40; Motsinger at 47:61-48:21, 49:12-38; Renaud at [0031].

discloses monitoring user behavior and “comparing the observed behavior to the predicted behavior to identify unexpected behavior” indicative of non-conforming or potentially automated activity, and further teaches “redirect[ing] the user to a web page having a CAPTCHA requiring user input to determine if the user is a human or an automated agent with more certainty” when the user’s behavior is identified as “suspicious.”⁶⁸ Likewise, Broder 456 expressly discloses that, after detecting potentially suspicious activity (such as a click on an advertisement), a system may “display[] an intermediate web page . . . [and] analyze[] the web viewer’s response...to make a determination as to whether the web viewer is a human or non-human entity,” and that this intermediate page may include a CAPTCHA test.⁶⁹ Together, these references confirm that it was conventional to (1) perform an initial behavioral analysis to identify suspicious activity and (2) conditionally administer a CAPTCHA or similar challenge as a follow-on verification step. As another example, 2004 Pusara discloses a system in which, “[i]f the current behavior of a user deviates significantly from the model of normal behavior, the system flags this behavior as anomalous” and can “ask[] the user to authenticate again.”⁷⁰

(h) It Was Well Known to Encrypt Data Sent from the Client Device to the Server

Techniques for incorporating encryption between a client device and a server were well-known, widely implemented, and understood to enhance the security and integrity of data

⁶⁸ Farahat at [0058]; *see also* Ramanathan at [0005] (disclosing monitoring communications to identify “characteristics associated with a bot” and, based on that detection, invoking a human interaction proof (of which a CAPTCHA is one type) to authenticate the user’s identity).

⁶⁹ Broder at [0039]-[0041] (“[I]f it seems that a web site is being attacked by a malicious robot program, that web site may elect to use a CAPTCHA intermediate page in order to filter out all of the accesses by the malicious robot program.”).

⁷⁰ 2004 Pusara at 2.

transmitted over networks well before the priority date of the Asserted Patents.⁷¹ For example, Varghese 058 discloses systems in which sensitive user data is encrypted prior to transmission from a client device and subsequently decrypted at a remote server. Varghese explains that user authentication data may be “encrypted . . . before transmission from the user’s computer . . . to the remote server,” and that the server performs “decryption of the identifier” upon receipt. Varghese further situates this approach within the well-known use of secure communication protocols (e.g., SSL/HTTPS) to ensure confidentiality, authentication, and data integrity during transmission over public networks.

These disclosures reflect the state of the art well before the earliest effective filing date of the Asserted Patents. It was widely understood that data transmitted from a client to a server—particularly sensitive user information—should be encrypted prior to transmission and decrypted upon receipt to prevent interception, tampering, or unauthorized access. Such client-side encryption and server-side decryption were standard, conventional practices in networked systems, implemented using well-known cryptographic protocols and techniques, and would have been routinely applied by a person of ordinary skill in the art to any system involving transmission of user data between a client device and a server.

(i) Motivation to Combine Prior Art Bot Detection Techniques to Practice the Claimed Methods

To the extent that there are any differences between the prior art and the claimed methods of the Asserted Claims, a person of ordinary skill in the art would have been motivated to

⁷¹ See, e.g., Afergan at [0011] (describing storing identifiers used to track user activity as “an encrypted cookie”); Varghese 058 at 12 (describing “encryption and decryption of information or data, such as user authentication information, and/or data that is representative of other information, for transactions on the Internet or other networks”); Billingsley 154 at [0028] (describing encrypting client-related data into an “encrypted and encoded token” prior to transmission, which is later decoded and decrypted by the server to validate the user interaction).

combine prior art methods to practice such methods. For example, the claimed methods recited in the '008 and '014 patents would have been obvious because they simply combine well-known methods for differentiating between humans and bots with well-known methods for generating probability values. *See I/P Engine, Inc. v. AOL Inc.*, 576 F. App'x 982, 989 (Fed. Cir. 2014) (finding obvious as a matter of law patent claims directed to a computerized search system that combined two well-known methods for filtering internet search results); *see also In re Translogic Tech., Inc.*, 504 F.3d 1249, 1259 (Fed. Cir. 2007) (“[O]bvious variants of prior art references are themselves part of the public domain.”). Similarly, the claimed methods recited in the '014 patent would have been obvious because they simply combine well-known methods for controlling access to websites or other computing resources, including presenting CAPTCHAs or testing for the presence of biometric data such as keystrokes and mouse movements or CAPTCHAs.

In particular, as discussed in detail above, extensive prior art disclosed the use of passive and active data to differentiate between humans and bots, including testing for the presence or absence of data associated with humans such as browser cookies, destination IP histories, originating IP address, originating IP address traffic data, originating IP address physical location, third party data regarding abusers, pointing device (e.g., mouse) movements and/or cadence, keystroke combinations and/or cadence, time differentials between stimulus and user response, and so on. In addition, as discussed above, the prior art disclosed methods for assessing a confidence level that an operator of a client computing device interacting with a server (such as an ad server) was a human being rather than an autonomic computer application. Thus, even if no single prior art reference disclosed assessing a confidence level that a user interacting with a server was a human rather than a bot, logic and common sense lead inexorably to the conclusion

that it would have been useful to implement such a method on a website. *See I/P Engine, Inc.*, 576 F. App'x at 989 (overturning verdict of nonobviousness and finding obvious as a matter of law patent claims directed to a computerized search system that combined two well-known methods for filtering internet search results).

Similarly, as discussed in detail above, extensive prior art disclosed testing for the presence of mouse movements, keystrokes, and other signals to distinguish human users of computerized resources (such as ad servers) from machines. Indeed, the prior art provided far more detail than the Asserted Patents regarding how such data could be used to distinguish human users from bots. Prior art methods of controlling access to computerized resources and websites, including CAPTCHAs and other authentication and verification methods, also were widely used, routine, and conventional. Thus, even if no single prior art reference disclosed testing for the presence of mouse movements, keystrokes, or other so-called biometric data to control access to a server, logic and common sense lead inexorably to the conclusion that it would have been useful to implement such a method on a website. *See I/P Engine, Inc.*, 576 F. App'x at 989. The same is true for the methods described in the dependent claims of the Asserted Patents.

Additionally, to the extent any reference or prior art system does not disclose repeating data collection and/or analyses steps, a relevant artisan would have been motivated to modify any such piece of art to include those features. As discussed in detail above, collecting additional data and/or performing multiple analysis steps was well known in the art. Repeating analysis in this fashion was simply the consequence of applying fundamental statistical analysis to human authentication and bot detection systems. Accordingly repeated collection and analysis was widely used, routine, and conventional. A relevant artisan would have found performing

additional data collection and/or analysis advantageous because such repetition allowed one to authenticate a user or detect bots over a period of time, make more accurate determinations, and achieve other beneficial results. Furthermore, to the extent any reference or prior art system does not disclose comparing the results of an analysis to other results, a relevant artisan would have found it obvious to implement such a feature in any such system. Comparing the results of analysis is a fundamental and basic concept. And a relevant artisan would have been motivated to implement such a comparison to, *e.g.*, advantageously compare users to one another and/or compare a user's results to her prior results, possibly to uncover trends in her performance. Therefore, modifying any prior art to perform repeated data collection, repeated analyses, and/or comparing the results of those analyses would have been obvious to try, and would have been no more than applying a known technique to yield a predictable improvement.

From a technical perspective, a person of ordinary skill in the art, by the time of the priority date of the patents, would have had a clear and well-understood reason to combine known techniques for (i) collecting client-side interaction data, (ii) analyzing those data in conjunction with stored models of human behavior, (iii) generating a quantitative value representing the likelihood of human versus automated activity, and (iv) conditionally performing additional verification steps based on that value. Combining these techniques was already routinely used together to address anti-cheat in video games, click fraud detection, as well as distinguishing human users from automated agents in networked systems as described in the asserted patents.

As clearly described by the prior art discussed above, by the priority date of the patents it was well known that servers could cause a client device to collect active interaction data (*e.g.*, mouse movements, keystrokes) and transmit those data along with passive data (*e.g.*, IP address,

cookies) back to the server. It was also well known to analyze such data in conjunction with model data derived from prior human interactions, including prior sessions associated with the same page or website, to determine whether current behavior is consistent with expected human patterns. Systems performing this analysis commonly generated a numerical value or score (such as a probability, confidence level, or risk score) representing the likelihood that the activity was human-generated. These operations correspond directly to the core limitations of claim 1 of the '008 patent and the core limitations of independent claims 1, 16 and 22 of the '014 patent, including monitoring or receiving interaction data, comparing that data to model data based on prior human interaction, and generating a value indicative of whether the user is human or an automated process.

A person of ordinary skill would have been motivated to combine these techniques because they form a natural and widely used analytical procedure. Collecting active and passive data provides behavioral and contextual signals, comparing those signals to prior-session model data provides a basis for classification, and generating a value representing a likelihood or confidence enables automated decision-making. Combining these elements yields the predictable result of automated classification using known methods applied in their conventional manner.

The '014 claims further recite threshold-based decision-making and staged verification, including determining whether an analysis value meets a predetermined criterion and, if not, requesting additional data (such as a CAPTCHA) and performing further analysis. These steps also reflect well-known and widely deployed techniques. By the priority date of the patents, it was conventional to use an initial, low-cost behavioral analysis as a first-pass filter and, upon detecting uncertainty or suspicious activity, to escalate to additional verification mechanisms. The use of thresholds to trigger such escalation, and the use of CAPTCHA or similar challenges

as a secondary verification step, were standard practices that would have been straightforward to incorporate into any system performing behavioral classification.

Similarly, the recitation in claim 18 of the '008 patent and the multi-level analyses in the '014 claims of repeating data collection and analysis and comparing successive values reflects routine and well-understood statistical practice. Because determinations of whether a user is human or a bot are inherently probabilistic, a person of ordinary skill would have recognized that accuracy can be improved by collecting additional observations over time and refining or confirming prior results. Comparing successive analysis values allows detection of changes in behavior, reduction of noise, and increased confidence in classification. This is a straightforward application of established classification and hypothesis-testing techniques and would have yielded predictable improvements in reliability and robustness.

In sum, the asserted claims of both the '008 and '014 patents recite a combination of well-known techniques: collecting active and passive user data, comparing those data to prior-session behavioral models, generating a confidence or likelihood value, and using that value to drive threshold-based decisions, including repeated analysis and conditional escalation. These elements were commonly used together in the prior art to address the same problem and would have been combined by a person of ordinary skill with a reasonable expectation of success and predictable results

Therefore, a person of ordinary skill in the art would have been motivated to combine the references listed and charted in Google's Claim Chart Exhibits according to known methods to achieve desired benefits and predictable results.

B. Invalidity Under 35 U.S.C. § 112

As detailed below, certain of the Asserted Claims lack written description or enablement, are indefinite, and/or fail to claim what the inventors regard as the invention under provisions of 35 U.S.C. § 112.

1. Lack of Enablement/Written Description Under 35 U.S.C. § 112, ¶ 1

Paragraph 1 of 35 U.S.C. § 112 requires that the specification contain a written description of the invention. “[T]he hallmark of written description is disclosure.” *Boston Scientific Corp. v. Johnson & Johnson*, 647 F.3d 1353, 1361–62 (Fed. Cir. 2011). The test for whether a specification adequately describes an invention is “whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date. . . . [T]he test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. . . . [It] is a question of fact.” *Ariad Pharms., Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc); *Boston Scientific*, 647 F.3d at 1362. “Adequate written description means that the applicant, in the specification, must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the [claimed] invention.” *Agilent Techs., Inc. v. Affymetrix, Inc.*, 567 F.3d 1366, 1379 (Fed. Cir. 2009). It is well settled that “one cannot disclose a forest in the original application, and then later pick a tree out of the forest and say here is my invention.” *Purdue Pharma L.P. v. Faulding Inc.*, 230 F.3d 1320, 1326 (Fed. Cir. 2000). Rather, the specification must provide some guides or “blaze marks” that disclose the claimed invention “specifically, as something appellants actually invented.” *Ariad*, 598 F.3d at 1348.

The enablement requirement of § 112 requires that the patent specification enable “those skilled in the art how to make and use the full scope of the claimed invention without ‘undue

experimentation.”” *Genentech, Inc. v. Novo Nordisk A/S*, 108 F.3d 1361, 1365 (Fed. Cir. 1997) (quoting *In re Wright*, 999 F.2d 1557, 1561 (Fed. Cir. 1993)). “[T]he scope of the claims must be less than or equal to the scope of the enablement.” *Nat’l Recovery Techs., Inc. v. Magnetic Separation Sys., Inc.*, 166 F.3d 1190, 1196 (Fed. Cir. 1999).

(a) Enablement/Written Description Contentions for the ’008 Patent:

The ’008 patent’s Asserted Claims recite methods for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application. However, there are no working examples of any such methods. A description that amounts “to no more than a ‘wish’ or ‘plan’ for obtaining the claimed [invention]” fails the written description requirement. *Ariad*, 598 F.3d at 1350. Moreover, none of the claims of the ’008 patent is adequately described or enabled by the specification. The claims of the ’008 patent thus fail to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention and fail to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the ’008 patent⁷² is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of the claim elements “the server presenting data issued by the server to the client computing device” and “the issued data.” The specification does not sufficiently describe what the server presenting data issued by the server to the client computing device entails or how it is accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had

⁷² References to specific claims include all claims depending from such claims.

possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '008 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of “monitoring at least some data generated by the user at the client computing device in response to the issued data.” The specification does not sufficiently describe what monitoring at least some data generated by the user at the client computing device in response to the issued data entails or how it is accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- To the extent that the term “at least some data generated by the user at the client computing device in response to the issued data” in claim 1 of the '008 patent and any claims dependent therefrom is interpreted broadly enough to cover other types of data not explicitly described in the patent, that claim (and any claims depending therefrom) are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of such “data generated by the user.” The only disclosure of “data” in the '008 patent are “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,” and “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).” ’008 patent at 2:65–3:17.

- Claim 1 of the ’008 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of “comparing the monitored data to model data relating to human interaction with or in response to the issued data.” The specification does not sufficiently describe what comparing the monitored data to model data relating to human interaction with or in response to the issued data entails or how it is accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 1 of the ’008 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of “generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.” The specification does not sufficiently describe what generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data entails or how it is accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of

the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 18 of the '008 patent is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the specification as filed does not contain an adequate written description and/or enabling disclosure of “repeating a)-c) and comparing the first instance of d) to the second instance of d).” The specification does not sufficiently describe what repeating a)-d) entails or how it is accomplished. The specification does not sufficiently describe what reaching a predetermined value for d) entails or how it is accomplished. And, the specification does not sufficiently describe what repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d) entails or how it is accomplished. Nor does the specification contain an adequate written description and/or enabling disclosure of “repeating b)-d) and comparing the first instance of the value of e) to the second instance of the value of e),” which is Plaintiff’s preferred construction. Dkt. 91, ¶61. The specification does not sufficiently describe repeating steps b)-d) or describe how it is accomplished. Nor does the specification describe comparing a first value of e) to a second instance of the value of e) or describe how it is accomplished. Accordingly, the specification fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

(b) Enablement/Written Description Contentions for the '014 Patent:

The Asserted Claims of the '014 patent purport to recite detailed, multi-step methods for assessing whether a client computer is operated by a human or an automated program, including (i) collecting “active data” and “passive data,” (ii) performing one or more levels of analysis

using “model data based on human interactions from a prior session with the same website,” (iii) generating one or more “analysis value[s]” subject to “predetermined criteria,” and (iv) conditionally requiring and evaluating CAPTCHA tests or requesting further data. Despite this breadth and technical specificity, the specification provides no working examples implementing these claimed, multi-stage analysis frameworks. A description that amounts “to no more than a ‘wish’ or ‘plan’ for obtaining the claimed [invention]” fails the written description requirement. *Ariad*, 598 F.3d at 1350. Moreover, many claims and claim elements are not adequately described or enabled by the specification. The claims of the ’014 patent thus fail to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention and fail to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the ’014 patent, as well as independent claims 16 and 22, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of generating a “value indicative of a likelihood” or “a value indicating a judgment” of whether a human or autonomic computer application is operating a client computer interacting with a server or attempting to access a protected page of a website. The written description does not sufficiently describe what it means to generate such a value, what form that value takes, or how such a value is computed or derived. Nor does the written description describe any concrete implementation of the claimed instructions on a “non-transitory machine readable medium,” beyond generic and purely functional descriptions. Accordingly, the written description fails to reasonably convey to one of

ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22 to the extent they rely on access-controlled interactions with a website or server, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of a “protected page of the website.” The written description does not describe what makes a page “protected,” how such protection is implemented, or how access to such a page is controlled or enforced in practice. Nor does the written description describe any system architecture or access-control mechanism governing transitions between protected and unprotected resources or otherwise restricting interactions with a server. To the extent the claims are interpreted broadly to encompass any form of access-controlled content or restricted interaction, the written description provides no enabling disclosure sufficient to support such implementations across their full scope. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 1 of the '014 patent, as well as independent claims 16 and 22, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of providing data collection data that causes a client computer to collect, and the server to receive, “active data” and “passive data” relating to interactions with a website or server. The written description provides only high-level and functional descriptions of

“monitoring” or collecting user interaction data, but does not describe what “data collection data” is, what form it takes, how it is generated or deployed, or how it causes the client computer to collect the claimed “active data.” Nor does the written description sufficiently describe what constitutes “active data” versus “passive data,” how such data is distinguished in practice, or how either category of data is actually received from the client computer. The written description also does not describe with any specificity how such data is captured, structured, transmitted, aggregated, or processed at the server, including any mechanisms, protocols, or system architecture by which such data moves from the client computer to the server. To the extent the claims are interpreted broadly to encompass any mechanism (e.g., scripts, embedded code, or other client-side instrumentation) for collecting such interaction data, or any types of “active” and “passive” data or any manner of receiving such data, the written description fails to describe or enable the full scope of the claimed functionality. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed interaction between a “client computer” and a “server.” The written description does not describe which claimed operations are performed at the client versus the server, how responsibilities are divided between those components, or how data is exchanged, synchronized, or processed across the system. Nor does the written description disclose

any architecture, protocols, or communication mechanisms sufficient to implement the claimed distributed functionality, including interactions with a website or server as recited in the claims. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of performing an analysis of received “active data” and “passive data” in conjunction with “model data based on human interactions from a prior session with the same website.” The written description does not sufficiently describe what the claimed “first analysis” or multi-level analyses entail, how the received data is analyzed, or how such analysis is performed “in conjunction with model data.” Nor does the written description adequately describe what constitutes the claimed “model data,” how such model data is generated, trained, or stored, or how it is tied to “human interactions from a prior session with the same website,” including how such prior-session data is identified, selected, or applied. The written description also fails to describe how the received data is combined or used “in conjunction with” model data, including any mechanism for correlating, weighting, or integrating these different data sources in the claimed analysis. The written description further fails to describe any algorithms, rules, or techniques for performing the claimed comparison or analysis, including any implementation of statistical modeling, pattern recognition, or machine learning sufficient to achieve the claimed functionality. To the

extent the claims are interpreted broadly to encompass any such analytical techniques, the written description provides no guidance enabling a person of ordinary skill to implement them across their full scope. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of generating an analysis value at a subsequent stage of processing—such as a “first analysis value” or a “value indicating a judgment”—based on a preceding analysis, determining whether that analysis value fails to meet predetermined criteria, and using such a value to control access or otherwise govern interactions with a website or server based on predetermined criteria. The written description does not sufficiently describe what such analysis values are, what form they take, how they are computed from the claimed analyses, or how they quantitatively or qualitatively represent the outcome of those analyses. Nor does the written description describe how any “predetermined criteria” are defined, selected, or applied, including any thresholds, rules, or decision logic used to determine whether access should be granted or further action should be taken. The written description also does not sufficiently describe how such a determination is made, including how an analysis value is compared to the predetermined criteria, what conditions constitute “fail[ure] to meet” the criteria, or how such determinations are implemented in practice across one or more levels of analysis. The written description

further fails to describe how the claimed outputs and subsequent actions are generated “based on” the preceding analyses or determinations, including any causal linkage or dependency between stages of the claimed process. The written description further fails to describe how such analysis values are used to control access to a “protected page” or otherwise regulate interactions with a server, including any system architecture or control flow implementing such decisions. To the extent the claims are interpreted broadly to encompass any scoring, classification, or decision-making technique, or any type of comparison or decision rule, the written description provides no guidance enabling a person of ordinary skill to implement such techniques across their full scope.

Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22 to the extent they require requesting additional data based on prior analysis results, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of providing a CAPTCHA test or other request for further data to the client computer based on a prior determination, and receiving a response from the client computer. The written description does not sufficiently describe how a CAPTCHA test or other challenge is selected, generated, or presented to the client computer, or how such a request is dynamically triggered “based on” a prior analysis or determination. Nor does the written description describe how responses to such CAPTCHA tests or other data requests are received, processed, or associated with earlier stages of analysis. The written description,

moreover, teaches that “an object of the invention embodiments is to minimize user exposure to CAPTCHA tests,” ’008 patent at 5:31–33, which is in tension with the claimed requirement of conditionally providing CAPTCHA tests or other requests for additional data as part of a multi-stage analysis framework. To the extent the claims are interpreted broadly to encompass any type of CAPTCHA, challenge-response mechanism, or adaptive data request, the written description provides no enabling disclosure of how such mechanisms are integrated into the claimed system or workflow. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the ’014 patent, as well as independent claims 16 and 22 to the extent they require further analysis of additional data or responses, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of “perform a second analysis comprising assessing accuracy of the response of the client computer to the CAPTCHA test” and “generate a second analysis value based on the second analysis.” The written description does not sufficiently describe what constitutes “accuracy” of a CAPTCHA response, how such accuracy is evaluated, or how the second analysis is performed. Nor does the written description describe how a “second analysis value” is generated, what form it takes, or how it is derived from the assessed response. The written description further fails to describe any algorithms, scoring methods, or evaluation criteria for performing this second-stage analysis. To the extent the claims are interpreted broadly to encompass any technique for evaluating responses and generating a

corresponding value, the written description provides no guidance enabling a person of ordinary skill to implement such techniques across their full scope. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claim 1 of the '014 patent, as well as independent claims 16 and 22 to the extent they require granting access or permitting interaction based on a subsequent analysis value meeting predetermined criteria, is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of “wherein the client computer is granted access to the protected page based on the second analysis value meeting a second analysis predetermined criteria.” The written description does not sufficiently describe how the second analysis value is compared to the “second analysis predetermined criteria,” how such criteria are defined or selected, or how the resulting determination governs access to the protected page. Nor does the written description describe the control logic, system architecture, or decision-making framework required to implement this second-stage access determination. To the extent the claims are interpreted broadly to encompass any multi-stage decision process using successive analysis values and criteria, the written description fails to describe or enable the full scope of such iterative and conditional access-control mechanisms. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1–15, 21, and 27 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the limitation “CAPTCHA test.” The written description describes CAPTCHA technology as requiring a user to “type the letters, digits or characters of a distorted image appearing on the screen.” ’008 patent, 1:22–2:8. The written description does not describe the broader field of prior-art CAPTCHA tests or provide representative examples sufficient to support the full scope of the broadly recited “CAPTCHA test” limitations in claims 1–15, 21, and 27. To the contrary, the patent states that “an object of the invention embodiments is to minimize user exposure to CAPTCHA tests.” ’008 patent, 5:31–33. The written description thus does not reasonably convey that the named inventor possessed, or enabled a person of ordinary skill to make and use, the full scope of the claimed “CAPTCHA test” limitations. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 16 and 22 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of “provid[ing] instructions that allow client computer interactions with a website of the server to be remotely monitored.” The written description does not describe how such instructions are generated, transmitted, or executed on the client computer, or how remote monitoring is implemented in practice. Nor does the written description describe any mechanisms for observing, capturing, or transmitting client-side interaction data in a remote or distributed environment.

Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the subject matter of the invention, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 2, 20, 21, 25, 26, and 27 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed multi-stage escalation process in which, after an initial analysis fails to satisfy predetermined criteria, the system requests further data, performs an additional level of analysis, and in some claims repeats that process through still further levels of analysis or CAPTCHA-based challenges. The written description does not describe any concrete architecture, algorithm, or decision logic for escalating from a first analysis to a second or third analysis, for determining when and how further data is requested, for incorporating CAPTCHA responses into successive rounds of analysis, or for generating second- or third-level analysis values that govern access to the protected page. Nor does the written description explain how repeated CAPTCHA-based challenges would be sequenced, evaluated, or integrated into a multi-level decision framework. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claims 1[d], 1[i], 3, 17, and 22[f] are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed access-control scheme in which access to a protected page is granted or denied based on whether an analysis value

meets or fails to meet predetermined criteria, including in some instances without presenting a CAPTCHA test at all. The written description does not describe any concrete mechanism, algorithm, or decision logic for generating such analysis values, applying the claimed predetermined criteria, and then using the result of that comparison to decide whether the client computer is granted access, denied access, or required to complete a CAPTCHA challenge. Nor does the written description explain how those criteria are defined, how they interact with the claimed analysis values, or how the system implements the claimed branching decisions governing access to the protected page. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 4, 19, and 23 of the '014 patent are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of decrypting received data, including “decrypt[ing] the received active data and the received passive data” and “decrypt[ing] the received monitored data.” The written description does not describe any encryption or decryption scheme, key management, protocol, algorithm, or other mechanism by which such data would be encrypted or decrypted, nor does it explain how any such functionality would be implemented or integrated into the claimed system. To the extent these claims are interpreted to encompass any form of encryption or decryption of the claimed data, the specification provides no disclosure that would enable a person of ordinary skill in the art to practice that functionality across the full scope of the claims. Accordingly, the written description fails to reasonably convey to one of ordinary skill

that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 5, 12, 13, 14, 15, and 24 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed requirement that model or recorded data be based on human interaction from a prior session with the “same given page.” The written description does not describe any mechanism for collecting, storing, or organizing human-interaction data at the level of a particular webpage, as opposed to a website more generally, nor does it explain how the system would identify a later-visited page as the “same given page” and retrieve corresponding prior-session human interaction data for use in the claimed analysis. Nor does the written description disclose how page-specific model data would be generated, maintained, or applied, including where the claims require prior human interaction of another client computer with the same given page, page-specific keyboard or manual device input activity, or mouse movement over a CAPTCHA test prompt. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 6 is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the limitation “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.” The written description does not describe any mechanism for

restricting collection of active data so that it is enabled only during the client computer's visit to a particular web page, as opposed to before, after, or more generally during operation of the client device or browser. Nor does the written description explain what it means for a web page to be "enabled with data collection data," how such data is associated with a particular page, or how the system would activate and deactivate client-side collection functionality based on entry to and exit from that page. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 7 and 8 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of receiving configuration input from an "operator or administrator of the website," including the claimed receipt of the first or second analysis predetermined criteria and the claimed receipt of CAPTCHA tests to be provided to a client computer after the second analysis value fails to meet the second analysis predetermined criteria. The written description does not describe any interface, protocol, data structure, control logic, or other mechanism by which an operator or administrator supplies such criteria or CAPTCHA tests to the claimed system, nor does it explain how such administrator-provided inputs are stored, interpreted, selected, or applied in the claimed analysis and access-control framework. Nor does the written description disclose how administrator-supplied thresholds or CAPTCHA tests would interact with the claimed first, second, or later-stage analyses. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed

subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 9, 15, 18, 29, and 30 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed analysis of manual input behavior—such as mouse movement, keyboard activity, keystrokes, or other manual device input activity—in conjunction with prior human-interaction data from the same website or page. The written description does not describe any mechanism for capturing and classifying mouse and keyboard activity at the level required by the claims, for storing corresponding prior-session human interaction data as model data, or for comparing current manual input behavior against that prior human-interaction data in the claimed analysis. Nor does the written description explain how such mouse or keyboard activity is processed, what features of that activity are analyzed, or how the results of any such comparison are incorporated into the claimed decision-making framework. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- Claim 10 is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the limitation “wherein the data collection data comprises JavaScript code that causes a browser of the client computer to collect the active data.” The written description does not describe any JavaScript code, browser-executed script, client-side scripting architecture, or other implementation details by which a browser

would be caused to collect the claimed active data. Nor does the written description explain what code would be delivered to the browser, how that code would operate within the browser environment, what active data it would collect, or how the collected data would be transmitted back to the system. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 11, 18, and 28 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed use of browser cookies and internet protocol (IP) addresses as received passive or monitored data in the claimed analysis. The written description does not describe any mechanism for obtaining browser cookies or IP addresses from the client computer as claimed, for associating such data with the client computer, or for incorporating those data into the claimed analysis together with model data based on prior human interactions. Nor does the written description explain what role browser cookies or IP addresses play in the analysis, how those data are processed, or how they are used to generate any claimed analysis value or judgment. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.
- [Claim 13 is invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed requirement that the “manual device input activity”](#)

analyzed in conjunction with model data “comprises mouse movement over a CAPTCHA test prompt.” The written description discloses mouse movement generally as an example of active data, and separately discusses conventional CAPTCHA tests, but it does not disclose mouse movement over a CAPTCHA test prompt or describe using such movement as the manual device input activity analyzed in conjunction with model data based on human interaction with the same given page, as required by claims 12 and 13. Nor does the written description provide representative examples or implementation details sufficient to show possession of, or enable, that claimed subject matter. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1[d], 1[e], 1[i], 7, 8, 16[d], 17, 20[c], 22[d], 22[e], 22[f], 25, 26, and 27 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of the claimed “predetermined criteria,” including first-, second-, and later-stage criteria used to govern access decisions, trigger additional requests for data, or control the provision of CAPTCHA tests. The written description does not describe how any such criteria are defined, selected, stored, configured, or supplied by the system, let alone by an operator or administrator of the website, and does not disclose any thresholds, rules, parameters, or decision logic for applying such criteria at the various claimed stages of analysis. Nor does the written description explain how these purportedly predetermined criteria interact with the claimed analysis values or later-stage requests and determinations. Accordingly, the written description fails to reasonably

convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

- Claims 1[c], 5, 9, 12, 14, 15, 16[c2], 18, 22[e], and 24 are invalid for failure to satisfy the requirements of 35 U.S.C. § 112, ¶ 1, because the written description as filed does not contain an adequate written description and/or enabling disclosure of using prior “human interactions” as model or recorded data without describing how the system determines in the first instance that such prior interactions are in fact human. The written description does not describe any mechanism, criteria, validation process, or training methodology by which prior-session data is identified as human-generated rather than bot-generated, fraudulent, or otherwise non-human before being stored and later used as model data or recorded data in the claimed analyses. Nor does the written description explain how the integrity or reliability of that supposed human-interaction baseline is established or maintained over time. Accordingly, the written description fails to reasonably convey to one of ordinary skill that the inventor had possession of the claimed subject matter, and it fails to enable a person of ordinary skill to make and use the invention as claimed.

* * *

Therefore, all of the Asserted Claims are invalid for lacking sufficient written description and/or an enabling disclosure.

2. Invalidity Under 35 U.S.C. § 112, ¶ 2 and/or ¶ 6

Claims are indefinite under 35 U.S.C. § 112, ¶ 2 when they “fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). To the extent an asserted apparatus claim includes both apparatus and method limitations, that claim is invalid for indefiniteness under

§ 112, ¶ 2 because it fails to identify or notify the public of what constitutes direct infringement. *See IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377 (Fed. Cir. 2005).

Paragraph 2 of 35 U.S.C. § 112 also requires that the claimed subject matter be what “the inventor or a joint inventor regards as the invention.” “Where it would be apparent to one of skill in the art, based on the specification, that the invention set forth in a claim is not what the patentee regarded as his invention, we must hold that claim invalid under § 112, paragraph 2.” *Allen Eng’g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1349 (Fed. Cir. 2002).

Google also identifies each claim element governed by 35 U.S.C. § 112, ¶ 6. The presence of the word “means” in a claim element creates a rebuttable presumption that § 112, ¶ 6 applies. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348 (Fed. Cir. 2015). In addition, “[g]eneric terms such as ‘mechanism,’ ‘element,’ ‘device,’ and other nonce words that reflect nothing more than verbal constructs may be used in a claim in a manner that is tantamount to using the word ‘means’ because they ‘typically do not connote sufficiently definite structure’ and therefore may invoke § 112, para. 6.” *Id.* at 1350 (holding that “module” was simply a generic description for software or hardware that performs a specific function, and applying § 112, ¶ 6); *see Rain Computing, Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1006 (Fed. Cir. 2021) (“‘Module’ is a well-known nonce word that can operate as a substitute for ‘means.’”) (quoting *Williamson*, 792 F.3d at 1350). The essential inquiry under § 112, ¶ 6 is whether the words of the claim are understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure. *Id.* at 1348. A means-plus-function element is “construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.” 35 U.S.C. § 112, ¶ 6. However, claims governed by § 112, ¶ 6 are indefinite if “the claim term fails to recite sufficiently definite structure or else

recites function without reciting sufficient structure for performing that function.” *Williamson*, 792 F.3d at 1348.

Means-plus-function claims directed to software require the specification to disclose an algorithm corresponding to the claimed function. *See EON Corp. IP Holdings LLC v. AT&T Mobility LLC*, 785 F.3d 616, 621 (Fed. Cir. 2015); *Aristocrat Techs. Austl. Pty Ltd. v. Int’l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008); *WMS Gaming, Inc. v. Int’l Game Tech.*, 184 F.3d 1339, 1348–49 (Fed. Cir. 1999). The specification must disclose some algorithm in “understandable terms” that “provide[] sufficient structure”; it cannot merely restate the function recited in the claim. *Finisar Corp. v. DirecTV Grp.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008); *see also Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1383 (Fed. Cir. 2009) (“The ACM is essentially a black box that performs a recited function. But how it does so is left undisclosed.”); *ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 518 (Fed. Cir. 2012) (holding that “black box” labeled “Purchase Orders” was insufficient structure to perform the “generate the purchase orders” function); *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1317 (Fed. Cir. 2012) (“[T]he disclosure must identify the method for performing the function, whether or not a skilled artisan might otherwise be able to glean such a method from other sources or from his own understanding.”).

Google hereby incorporates by reference the enablement and written description contentions above regarding the same claim limitations. In addition to Google’s reservation of rights stated above, Google notes that the Court’s Docket Control Order contemplates that all indefiniteness issues be brought to the Court’s attention through the *Markman* briefing process. Google specifically reserves the right to present any (or none) of the indefiniteness arguments

outlined below and will present its detailed arguments as to any indefiniteness at that time, through the *Markman* meet and confer and briefing processes.

(a) Section 112, ¶ 2 and/or ¶ 6 Contentions for the '008 Patent

Google reserves the right to argue that the limitation(s) of the '008 patent listed below, when read in light of the specification and prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention, either because the specification does not use phrases that appear in these limitation(s) and/or fails to delineate the scope of each limitation, including with relation to other limitation(s), and therefore one of ordinary skill would not understand the metes and bounds of the claims in which these limitation(s) appear, as required by 35 U.S.C. § 112, ¶ 2.

- “a single user of a client computing device” (claim 1 and any claims dependent therefrom)
- “presenting data issued by the server” (claim 1 and any claims dependent therefrom)
- “data generated by the user at the client computing device in response to the issued data” (claim 1 and any claims dependent therefrom)
- “model data relating to human interaction” (claim 1 and any claims dependent therefrom)
- “with or in response to the issued data” (claim 1 and any claims dependent therefrom)
- “a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.” (claim 1 and any claims dependent therefrom)
- “repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d)” (claim 18).

(b) Section 112, ¶ 2 and/or ¶ 6 Contentions for the '014 Patent

Google reserves the right to argue that independent claims 1, 16, and 22 of the '014 patent and any claims dependent therefrom recite both a system/device and method for using that system/device, which “does not apprise a person of ordinary skill in the art of [their] scope” and renders them invalid under § 112, ¶ 2. *IPXL Holdings*, 430 F.3d at 1384. Furthermore, Google reserves the right to argue that the limitation(s) of the '014 patent listed below, when read in light of the specification and prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention, either because the specification does not use phrases that appear in these limitation(s) and/or fails to delineate the scope of each limitation, including with relation to other limitation(s), and therefore one of ordinary skill would not understand the metes and bounds of the claims in which these limitation(s) appear, as required by 35 U.S.C. § 112, ¶ 2.

- “active data” (claims 1, 16, and 22, and any claims dependent therefrom)
- “passive data” (claims 1, 16, and 22, and any claims dependent therefrom)
- “in conjunction with model data based on human interactions” (claims 1 and 16, and any claims dependent therefrom)
- “in conjunction with previously recorded data relating to human interactions” (claim 22, and any claims dependent therefrom)
- “value indicative of a likelihood that a human or autonomic computer application is operating a client computer” (claim 1, and any claims dependent therefrom)
- “value indicating a judgment of whether a human or an autonomic computer application operating a client computer” (claims 16 and 22, and any claims dependent therefrom)
- “receive monitored data originating with the client computer” (claim 22, and any claims dependent therefrom).

These identifications are preliminary and are provided to preserve Google's rights in light of the early stage of the case. Plaintiff first asserted the '014 patent on March 5, 2026, and the parties have not yet begun the claim construction exchange or briefing process. Under the Court's Standing Order Governing Proceedings – Patent Cases, the parties will exchange proposed claim terms and constructions and subsequently narrow the set of disputed terms prior to Markman briefing. Accordingly, Google's identification of the above terms is tentative and subject to refinement, supplementation, or withdrawal based on further analysis, the parties' claim construction exchanges, and the intrinsic and extrinsic record. Google reserves the right to assert indefiniteness as to these or other terms following the claim construction process and consistent with the Scheduling Order.

(c) Failure to Claim What the Inventor Regards As the Invention

Additionally, the Asserted Claims are invalid under § 112, ¶ 2 for failure to claim what “the inventor or a joint inventor regards as the invention.” For example, all the Asserted Claims are specifically directed to assessing whether the operator of the client computing device is a human being rather than an autonomic computer application, not whether the user is merely invalid, fraudulent, suspicious, abusive, or otherwise undesirable. The written description repeatedly describes the relevant status determination as human-versus-bot, and the prosecution history confirms that applicant relied on that distinction in amending and defending the claims. *See* NOBOTS_00000013 ('008 file history) at NOBOTS_00000096–98 (8/18/2025 Response to 8/16/2011 Non-Final Office Action) (arguing amended claims require a confidence level that monitored data reflects “human interaction” rather than “that of an autonomic user,” and distinguishing U.S. Patent Application Publication No. 2008/0225870 (Sundstrom) on the ground that it is “silent as to any distinction between human and autonomic users”). To the

extent the Asserted Claims purport to cover any invalid, abusive, or fraudulent user behavior, they do not appear to claim what the named inventor regarded as his invention.

The written description explains that “an object of the invention embodiments is to minimize user exposure to CAPTCHA tests.” ’008 patent, at 5:31-33. Moreover, the written description expressly frames the alleged invention as a probability-based alternative to CAPTCHA, stating that the embodiments “provide a probability result as opposed to a binary result,” “avoid the ‘there is only one right answer’ phenomena inherent in prior art CAPTCHA tests,” and shift the burden “to the server side of the equation.” *Id.* at 2:25-33. Yet several of the Asserted Claims sweep more broadly, or differently, than that described invention. For example, ’014 patent claims 1[f], 2, 16[e], 20–21, and 25–27 recite CAPTCHA-based or other follow-on testing triggered by failure of a prior analysis.

In addition, ’014 patent claims 16 and 22 broadly recite “providing a value indicating a judgment” and multi-level follow-on requests for “further data,” untethered to the more specific human-confidence-score and limited follow-on verification framework described in the specification. And ’014 patent claims 1[c], 5, 9, 12, 14–15, 16[c2], 18, 22[e], and 24 require model data from a prior session with the “same website” or “same given page,” whereas the specification’s general description of model data is framed more broadly as data indicative of human interaction with a “computing environment.” To the extent the Asserted Claims purport to cover those broader concepts, they do not appear to claim what the named inventor regarded as his invention.

C. Double Patenting

The ’008 patent is invalid under 35 U.S.C. § 101, which provides that, “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain *a patent*,” that is, a single patent.

35 U.S.C. § 101 (emphasis added). The '008 patent is also invalid under the judicially created doctrine of obviousness-type double patenting (ODP). ODP “is intended to prevent a patentee from obtaining a time-wise extension of patent for the same invention or an obvious modification thereof” and prevents an inventor from claiming a second patent for claims that are not patentably distinct from the claims of a first patent. *In re Collect, LLC*, 81 F.4th 1216, 1226 (Fed. Cir. 2023) (quoting *In re Lonardo*, 119 F.3d 960, 965 (Fed. Cir. 1997)). The Asserted Claims of the '008 patent recite the same invention as, or an obvious modification of, the claims recited in the following reference patents:

- U.S. Patent No. 10,423,885
- U.S. Patent No. 11,775,853
- U.S. Patent No. 11,810,014
- U.S. Patent No. 11,836,647

All the reference patents listed above are in the same patent family as the '008 patent and all have been terminated or will expire prior to the '008 patent.

Google provides the following non-limiting examples of how the Asserted Claims of the '008 patent are rendered obvious by the claims of U.S. Patent No. 11,836,647 (the “'647 patent”), alone or in combination with the prior art references listed in Tables 1–3 above:

'008 Claim	'647 Claim
1[pre] A method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:	1[pre] 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, the method comprising: 16[pre] 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, the method comprising:

'008 Claim	'647 Claim
	22[pre] 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, the method comprising:
1[a] a) a single user of a client computing device requesting data from a server;	1[pre] 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, the method comprising: [6] The method 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. 16[pre] 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, the method comprising: 22[pre] 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, the method comprising:
1[b] b) the server presenting data issued by the server to the client computing device;	1[a] providing 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; 16[a] providing data collection data requesting active and passive data of the client computer; 22[a] providing instructions that allow client computer interactions with a website of the server to be remotely monitored;
1[c] c) monitoring at least some data generated by the user at the client computing device in response to the issued data;	1[b] receiving at least some of the collected active data from the client computer and at least some passive data from the client computer;

'008 Claim	'647 Claim
	16[b] receiving 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; 22[b] receiving 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;
1[d] d) comparing the monitored data to model data relating to human interaction with or in response to the issued data; and	1[c] performing 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; 16[c] analyzing 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; 22[c-d] analyzing the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including: performing 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;
1[e] e) generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.	1[d] generating 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;

'008 Claim	'647 Claim
	16[c] analyzing 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; 22[c-d] analyzing the received monitored data for indication of a human or an autonomic computer application operating the client computer, the analyzing including: performing 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;
Claim 18	
18. The method of claim 1 further comprising repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d).	1[e-i] determining that the first analysis value fails to meet the first analysis predetermined criteria; providing a CAPTCHA test to the client computer based on the determination that the first analysis value fails to meet the first analysis predetermined criteria; receiving a response of the client computer to the CAPTCHA test; performing a second analysis comprising assessing accuracy of the response of the client computer to the CAPTCHA test; and generating 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. [2] The method of claim 1, further comprising: determining that the second analysis value fails to meet the second analysis predetermined criteria;

'008 Claim	'647 Claim
	providing 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; receiving a response of the client computer to the additional CAPTCHA test; performing a third analysis comprising assessing the accuracy of the client computer's response to the additional CAPTCHA test; and generating 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. 16[d-e] determining that the first analysis value fails to meet a first analysis predetermined criteria; and providing 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. [20] The method of claim 16, further comprising: receiving further data from the client computer in response to the request for further data; performing a second level of analyzing on the received further data; and providing a second analysis value based on the second level of analyzing. 22[e-g] determining that the first-level analysis does not meet a first-level analysis predetermined criteria; performing a second level of analyzing to obtain a second-level analysis, the second-level analysis based on the determination that the first-level analysis does not meet the first-level analysis

'008 Claim	'647 Claim
	predetermined criteria, the second level of analyzing comprising analyzing the received data in conjunction with previously recorded data relating to human interactions from a prior session with the same website; and providing a second-level analysis value when the second-level analysis meets a second-level analysis predetermined criteria. [25] The method of claim 22, the analyzing further comprising: determining that the second-level analysis does not meet the second-level analysis predetermined criteria; and providing 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. [26] The method of claim 25, the analyzing further comprising: receiving further data from the client computer in response to the request for further data; performing a third-level of analyzing on the received further data; and providing a third-level analysis value after completion of the third-level of analyzing.

Google provides the following non-limiting examples of how the Asserted Claims of the '008 patent are rendered obvious by the claims of U.S. Patent No. 10,423,885 (the "'885 patent"), alone or in combination with the prior art references listed in Tables 1–3 above:

'008 Claim	'885 Claim
1[pre] A method for assessing a confidence level that an operator of a	[1pre-a] A method comprising:

'008 Claim	'885 Claim
client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:	testing for a presence of biometric data associated with an operator of a computing device attempting to access a server;
1[a] a) a single user of a client computing device requesting data from a server;	[1pre-a] A method comprising: testing for a presence of biometric data associated with an operator of a computing device attempting to access a server;
1[b] b) the server presenting data issued by the server to the client computing device;	[1pre-a] A method comprising: testing for a presence of biometric data associated with an operator of a computing device attempting to access a server; [20] A method as claim 13 recites, wherein at least some of the issued data is in response to a request issued by the computing device.
1[c] c) monitoring at least some data generated by the user at the client computing device in response to the issued data;	[13] A method as claim 1 recites, further comprising: acquiring interest data from the computing device prior to delivery of issued data from the server to the computing device; comparing the interest data to model data relating to human interaction with the computing device; and generating a probability value associated with an operator of the computing device.
1[d] d) comparing the monitored data to model data relating to human interaction with or in response to the issued data; and	[13] A method as claim 1 recites, further comprising: acquiring interest data from the computing device prior to delivery of issued data from the server to the computing device; comparing the interest data to model data relating to human interaction with the computing device; and

'008 Claim	'885 Claim
	generating a probability value associated with an operator of the computing device. [14] A method as claim 13 recites, wherein the model data comprises at least one of passive model data or active model data.
1[c] e) generating a value that represents a confidence level that the monitored data is a result of human interaction on the client computing device rather than that of an autonomic user with or in response to the issued data.	[13] A method as claim 1 recites, further comprising: acquiring interest data from the computing device prior to delivery of issued data from the server to the computing device; comparing the interest data to model data relating to human interaction with the computing device; and generating a probability value associated with an operator of the computing device. [15] A method as claim 13 recites, wherein the probability value represents an assessment of likelihood that the operator of the computing device interacting with the server is a human being rather than an autonomic computer application.
Claim 18	
18. The method of claim 1 further comprising repeating a)-c) and comparing the first instance of the value of d) to the second instance of the value of d).	[17] A method as claim 13 recites, further comprising providing a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to the computing device attempting to access the server if the probability value does not indicate a greater likelihood that the operator of the computing device is a human.

D. Invalid Patent Term Adjustment

35 U.S.C. § 282(c) states in relevant part that the “[i]nvalidity of the extension of a patent term or any portion thereof under section 154(b) . . . because of the material failure (1) by the applicant for the extension, or (2) by the Director, to comply with the requirements of such

section shall be a defense in any action involving the infringement of a patent during the period of the extension of its term and shall be pleaded.” Section 282(c) thus provides an affirmative defense against patent infringement during the portion of the patent term that is invalid.

Here, the ’008 patent was accorded PTA under 35 U.S.C. § 154(b), extending its term. Specifically, the ’008 patent received 780 days of patent term adjustment (“PTA”) under section 154(b). NOBOTS_00000013 at NOBOTS_00000185. Google contends that at least a portion of the patent term adjustment accorded to the ’008 patent is invalid.

III. Subject Matter Eligibility Contentions

A. Subject Matter Eligibility Charts

Exhibits C and F attached to these Invalidity and Subject Matter Eligibility Contentions contain charts as set forth in the Court’s Standing Order Governing Proceedings – Patent Cases pertaining to the ’008 patent and the ’014 patent, respectively. The Subject Matter Eligibility Contentions set forth below and in each exhibit, pursuant to this Court’s Standing Order Governing Proceedings – Patent Cases, are subject to revision and amendment pursuant to Federal Rule of Civil Procedure 26(e) and the Orders in this matter to the extent appropriate in light of, without limitation, further investigation and discovery, the Court’s construction of the claims at issue, positions taken by Plaintiff in this action or any other proceeding, the review and analysis of expert witnesses, and/or as other circumstances warrant.

Section 1 of Exhibits C and F contain Google’s chart identifying each exception to eligibility to which each Asserted Claim of the patent at issue is directed and the factual and legal basis therefor. The charts also identify whether one or more of the Asserted Claims are representative of any other Asserted Claim. Section 2 of Exhibits C and F contains Google’s chart describing the industry, at the relevant time. Section 3 of Exhibits C and F describe how each element of each Asserted Claim, both individually and in combination with the other

elements of that claim, was well understood, routine, and conventional, and the factual and legal basis therefor.

B. Unpatentable Subject Matter Under 35 U.S.C. § 101

Section 101 of the Patent Act defines the type of subject matter that is patent-eligible. 35 U.S.C. § 101. The Supreme Court has long interpreted § 101 to hold that “[l]aws of nature, natural phenomena, and abstract ideas are not patentable.” *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014). These basic principles are excluded from patent eligibility because they are the very “building blocks of human ingenuity,” *id.*, and should be “free to all men and reserved exclusively to none.” *Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.*, 566 U.S. 66, 71 (2012).

The Supreme Court’s *Alice* test sets forth a two-part standard for assessing subject-matter eligibility. In the first step, the court must determine whether the claims are “directed to” patent-ineligible subject matter, such as an abstract idea. *Alice*, 573 U.S. at 217. In deciding whether a claim is “directed to” an abstract idea, the court must look at the “focus of the claimed advance over the prior art to determine if the claim’s character as a whole is directed to excluded subject matter.” *Affinity Labs of Texas, LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016) (internal quotation marks omitted). Limiting the claims directed to an abstract idea to a particular “technological environment” or “field of use” does “not render the claims any less abstract.” *Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, 873 F.3d 1364, 1373, 1382 (Fed. Cir. 2017) (citing *Affinity Labs*, 838 F.3d at 1259) (holding that claims applying abstract idea to particular field of use, namely mass transit, were not patent eligible); *Alice*, 573 U.S. at 222 (“the prohibition against patenting abstract ideas cannot be circumvented by attempting to limit the use of the idea to a particular technological environment”); *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 768 (Fed. Cir. 2019), *cert. denied*, 140 S. Ct. 983, 206 L. Ed.

2d 135 (2020) (limiting abstract idea of “communication over a network for interacting with a device” to electric vehicle charging stations did not make claims patent eligible).

Under *Alice* step two, the court must determine whether the patent claims include an “inventive concept” that is “sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [abstract idea] itself.” *Alice*, 573 U.S. at 217–18. The inventive concept must be truly inventive; it is not sufficient to include “well-understood, routine, conventional” features. *Mayo*, 566 U.S. at 79–80. For example, merely reciting conventional computer elements “cannot transform a patent-ineligible abstract idea into a patent-eligible invention.” *Alice*, 573 U.S. at 223; *see also Content Extraction and Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014) (“use of a generic scanner and computer to perform well-understood, routine, and conventional activities commonly used in industry” did not make claim patent eligible). Moreover, “generic functional language” to achieve purported solutions to technical problems, without “any requirements for *how* the desired result is achieved” will not suffice for an inventive concept. *Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1339 (Fed. Cir. 2017).

1. The ’008 patent

(a) *Alice* Step One

As set forth in detail in Exhibit C, the Asserted Claims of the ’008 patent are directed to methods for telling humans and computers apart. Although the ’008 patent does not specifically refer to it, tests for telling humans and computers apart have been known since at least 1950 when famed mathematician Alan Turing developed the well-known “Turing test” for telling humans and computers apart. The original Turing test consists of an interrogation game where a

human questions one human and one computer. If the questioner cannot tell the difference, then the computer passes the Turing test.⁷³

CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are often called “reverse Turing tests,” because a computer administers a test to determine whether a user is human or not.⁷⁴ The ’008 patent acknowledges that CAPTCHAs have long been implemented by websites to prevent abuse by “[p]eople who want to take advantage of websites . . . by creating automated programs employing various algorithms and routines (hereinafter ‘bots’) that create fictitious accounts or access content for a multitude of reasons.” ’008 patent at 1:10–13; *see id.* 1:57–60.

The ’008 patent has two independent method claims (claims 1 and 19) that mirror the steps of well-known Turing tests such as CAPTCHAs. Claim 1 recites “[a] method for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than an autonomic computer application, the method comprising:” (1) a user “of a client computing device requesting data from a server”; (2) “the server presenting data to the client computing device”; (3) monitoring data generated by the user in response to the data presented by the server; (4) and analyzing the user’s response to determine a statistical probability or “value that represents a confidence level” that the use is human and not a bot. Claim 19 is similar to claim 1, except that the data used to determine whether the user is a human or a bot is acquired “prior to the delivery” of data from the server. Dependent claims 2–18 and 20 add only insignificant limitations on the types of data that should be considered in the Turing

⁷³ See generally https://en.wikipedia.org/wiki/Turing_test.

⁷⁴ *Id.*; see also generally Saygin, Athanasopoulos, Baird & Lopresti, Baird I, Baird II, BotBarrier I, Chew II, Chow, da Silva, Datta, Elson, Golle, Gossweiler, Lopresti, May I, May II, Rusu II, Shirali-Shahreza I, Shirali-Shahreza II, TechCrunch, von Ahn I, von Ahn II, von Ahn III, von Ahn IV, von Ahn V, and von Ahn VI.

test (claims 2–5, 10, 13–14, 20), the way in which user data is collected using generic computer functionality (claims 6–9, 11–12), the number of times the test should be conducted (claims 16–18), or the server’s response to the results of the test (claim 15).

While the ’008 patent generally describes monitoring different types of “active data” or “passive data,” the only specific disclosures of how to differentiate humans from bots are: (1) “if no [mouse movement and/or keystroke] activity is recorded there is a very high probability that the user is actually a bot”; and (2) “if the dataset is sufficiently robust, it is impossible to have duplicative input data unless the input data was derived from a machine.” Even here, the patent makes clear that it relies on the knowledge of “the skilled practitioner” to refine the claimed methods to “reduc[e] computational overhead and storage issues.” ’008 patent at 5:5–9. Any other specifics or guidance for presenting data to the client computing device, monitoring user data, acquiring user data, and analyzing user responses to determine a “confidence level” that the user is human and not a bot are absent from the patent.

Moreover, the claims of the ’008 patent merely contemplate the use of generic computer network components, such as “a client computing device,” “a computing device,” “a server,” and a “pointing device,” to carry out these steps. There are no special definitions for these terms in the specification.

Setting aside these generic computer components, as the Court will do under *Alice*, the claims of the ’008 patent are no different from gathering data, comparing the gathered data to other data, and scoring the gathered data based on this comparison — all things that have been done for centuries, such as in standardized tests.⁷⁵ Indeed, the procedures set forth in the present claims are a generalized formulation for computer programs to solve mathematical problems.

⁷⁵ See, e.g., https://en.wikipedia.org/wiki/Standardized_test.

From this generic formulation, programs may be developed as specific applications. Note, the mathematical procedures can be carried out in existing computers long in use, without new machinery or equipment. Indeed, the calculation of the claimed confidence level can be performed without a computer. As such, the claims are ineligibly abstract. *See CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372 (Fed. Cir. 2011) (a patent that claims a process that “can be performed in the human mind or by a human using a pen and paper” is ineligibly abstract).

The application or context of the '008 patent's test does not render its claims any less abstract. First, as discussed above, the idea of using a test to “tell computers and humans apart” is also a fundamental concept that dates back to the dawn of computers in the 1950s. Simply limiting a claim to a specific application, or appending to the claim additional steps consisting of conventional or routine activity, such as collecting “data generated by the user at the client computing device,” is insufficient. *Bilski v. Kappos*, 561 U.S. 593, 612 (2010) (“[L]imiting an abstract idea to one field of use or adding token postsolution components [does] not make the concept patentable.”). Similarly, applying the test to granting access to a website is “merely limiting the field of use of the abstract idea to a particular existing technological environment,” which “does not render the claims any less abstract.” *Affinity Labs of Texas*, 838 F.3d at 1259; *see also Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016). Indeed, courts routinely find claims reciting processes for managing and controlling “access” based on a test or query to be ineligibly abstract. *See Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 712, 715–16 (Fed. Cir. 2014) (invalidating claims directed to granting a consumer access to media content upon responding to a “query” for watching an advertisement); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093 (Fed. Cir. 2016) (invalidating method that “relates to a

system and method of detecting fraud and/or misuse in a computer environment based on analyzing data such as in log files, or other similar records, including user identifier data”); *Smartflash LLC v. Apple Inc.*, 680 F. App’x 977, 982–83 (Fed. Cir. 2017) (invalidating claims “directed to the abstract idea of conditioning and controlling access to data based on payment”).

Even if the claims did recite novel subject matter (they do not), that would be irrelevant to the § 101 analysis, for “a claim for a new abstract idea is still an abstract idea.” *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016). Although the ’008 patent purports to address a problem that occurs in the online world, namely the targeting of websites by malicious programs, the Federal Circuit has made clear that “not all claims purporting to address Internet-centric challenges are eligible for patent.” *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014). For example, in *Internet Patents Corp. v. Active Network, Inc.*, the Federal Circuit invalidated patent claims directed to a method that addresses the problem of retaining information in online forms when navigating between webpages. 790 F.3d 1343, 1347–48 (Fed. Cir. 2015). In *Intellectual Ventures I LLC v. Symantec Corp.*, the Federal Circuit invalidated a claimed method of filtering emails that “address[ed] the problems of spam e-mail and the use of e-mail to deliver computer viruses.” 838 F.3d 1307, 1313 (Fed. Cir. 2016).

Moreover, the fundamental problem allegedly solved by the ’008 patent claims—telling humans and computers apart—is rooted in the pre-Internet and even pre-modern computer era that harkens back to the middle of the last century and the rudimentary computing machines addressed by the “Turing test.” Thus, unlike in *DDR*, the ’008 patent addresses no such “Internet-centric challenge.” The claims here are also unlike those found to be patent-eligible at *Alice* step one in *Enfish, LLC v. Microsoft Corp.* In *Enfish*, the Federal Circuit rejected the § 101

challenge because the claims focused on a specific improvement for a particular hierarchical database structure, i.e., how computers could carry out one of their basic functions of storage and retrieval of data. 822 F.3d 1327, 1335–36 (Fed. Cir. 2016). But here, unlike in *Enfish*, the claims are not directed to improving any technological device or process. Instead, they can be carried out just the same using pen and paper or with generic computing components performing their routine functions.

The claims in the '008 patent align more with the patent-ineligible claims in *FairWarning IP v. Iatric Systems, Inc.*, where the Federal Circuit invalidated claims directed to “a system and method of detecting fraud and/or misuse in a computer environment based on analyzing data such as in log files, or other similar records, including user identifier data,” observing that the use of generic computer components to “select[] information, by content or source, for collection, analysis, and [announcement] does nothing significant to differentiate a process from ordinary mental processes, whose implicit exclusion from § 101 undergirds the information-based category of abstract ideas.” 839 F.3d at 1093, 1097 (quoting *Elec. Power*, 830 F.3d at 1355). The fact that claims 1 and 19 of the '008 patent require “generating a value that represents a confidence level” that the user is human and not a bot—a mathematically calculated statistical prediction—does not render the claims any less abstract. The Federal Circuit has held that “implementing and processing calculations with a regular computer” cannot change the character of a claim from an abstract idea to a practical application. *In re Bd. of Trustees of Leland Stanford Junior Univ.*, 991 F.3d 1245, 1250–51 (Fed. Cir. 2021) (“The different use of a mathematical calculation, even one that yields different or better results, does not render patent eligible subject matter.”).

(b) Alice Step Two

Where the claims at issue are directed to a patent-ineligible concept, such as an abstract idea, the court must “examine the elements of the claim to determine whether it contains an ‘inventive concept’ sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Alice*, 573 U.S. at 221 (internal quotation marks omitted).

Here, the elements of claims 1 and 19 of the ’008 patent, taken individually or together, do not contain a sufficiently transformative inventive concept so as to be patent eligible. Even when viewed as a whole, these claims do not, for example, purport to improve the functioning of the computer itself, or effect an improvement in any other technology or technical field.

The focus of the claims is on abstract ideas that use computers as tools, and not on improvements in how computers carry out their functions of storing and retrieving data. Because the claims do not contain any inventive concept that removes them from a class of subject matter ineligible for patenting, merely selecting information for collection, analysis, and display does nothing significant to differentiate the claimed methods from ordinary mental processes, as the claims do not require any new source or type of information, or a new technique for analyzing such information. The claims here do not propose a solution or overcome a problem “specifically arising in the realm of computer [technology].” *DDR Holdings*, 773 F.3d at 1257.

In addition, the limitations in claim 1 and 19 that require calculating a probability or “confidence level” that the user is human does not establish an inventive concept that transforms the abstract idea into patent-eligible subject matter. There is no inventive concept in the use of algorithms and mathematical calculations. See *In re Bd. of Trustees of Leland Stanford Junior Univ.*, 991 F.3d at 1251. Indeed, the ’008 patent does not describe the algorithm or mathematical calculation that should be used to determine this “confidence level,” leaving that calculation to

the knowledge of a person of ordinary skill in the art—further confirming that this calculation was conventional and well understood in the prior art.

At most, the claims require that these processes be executed on a generic computer. But, “after *Alice*, there can remain no doubt: recitation of generic computer limitations does not make an otherwise ineligible claim patent-eligible.” *DDR Holdings*, 773 F.3d at 1256. “Thus, while the patent may in fact require that the claimed data relate to transactions or activities that are executed in the computer environment, limiting the claims to the computer field does not alone transform them into a patent-eligible application.” *FairWarning IP*, 839 F.3d at 1097.

Further, the claims do not require non-conventional computer, network, or display components, or nonconventional arrangements of known components. *See Elec. Power Grp.*, 830 F.3d 1350. A claim requiring no more than mere instructions to implement an abstract idea on a computer or requiring no more than a generic computer to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the industry does not qualify as “significantly more” in the determination of whether the claim amounts to significantly more than an abstract idea itself. *See Alice*, 573 U.S. 208.

Plaintiff may point to the fact that the claims require a computer to gather signals from another computer and then analyze those signals and argue that, because of the inherently computer-based nature of this analysis and the speed with which the computer can execute it, the claims are directed to the solution of technical problems unique to the computer environment and therefore should be patent eligible. However, the Federal Circuit has repeatedly rejected this argument. In *Vehicle Intelligence and Safety LLC v. Mercedes-Benz USA, LLC*, for example, the Federal Circuit rejected the patent owner’s argument that its claims provided an inventive concept because the patent touted a “faster, more accurate and reliable impairment testing of

vehicle operators” over prior-art testing. 635 F. App’x 914, 920 (Fed. Cir. 2015). The Court found that “[s]uch bald assertions made at such a high level of generality and not tied to any claim language” did not save the claims from patent-ineligibility. *Id.*

In short, there is nothing claimed in the ’008 patent—either by considering the claim limitations individually or as an ordered combination—that makes its claims patent eligible.

(c) Dependent Claims

The dependent claims of the ’008 patent do not add anything to the independent claims beyond generic computer components and functions. As set forth in detail in Exhibit C, the claims simply add well-understood, routine, and conventional functionality to the same abstract idea of conducting secure transactions. These claims therefore contain nothing that would turn the underlying abstract idea of presenting and settling an invoice into a patent-eligible inventive concept.

(d) Claim 18 of the ’008 Patent

As discussed above, claim 18 of the ’008 patent is the sole remaining claim from the original Complaint. In view of the PTAB’s decision finding claim 1 of the ’008 patent invalid, Google amends these contentions to further explain why claim 18 is invalid under 35 U.S.C. § 101.

(i) At *Alice* step one, claim 18 is directed to an abstract idea.

Claim 18’s only asserted advances over claim 1 are the requirements to repeat conventional activities and compare the resulting values. These purported advances amount to nothing more than mental exercises that can be performed by the human mind. The Supreme Court has recognized that such “fundamental” and “long prevalent” practices are indicative of abstract ideas, *Id.* at 219, and the Federal Circuit has stated that “mental processes that can be

performed in the human mind or using a pencil and paper [are] a telltale sign of abstraction,” *PersonalWeb Techs.*, 8 F.4th at 1316 (citations and internal quotation marks omitted). Claim 18 is thus directed to the combination of two abstract ideas, satisfying step one of *Alice*.

Beginning with claim 18’s requirement of “repeating a)-d),” the Federal Circuit made clear in *Content Extraction & Transmission LLC v. Wells Fargo Bank, National Association*, 776 F.3d 1343, 1348-49 (Fed. Cir. 2014) that merely “repeating some steps” is an abstract idea. This Court applied that principle in *Health Discovery Corp. v. Intel Corp.*, 577 F. Supp. 3d 570 (W.D. Tex. 2021). In *Health Discovery*, representative claim 1 recited a “computer-implemented method” for “performing feature ranking, selection, and reduction” using a support vector machine (“SVM”) to facilitate a recursive feature elimination (“RFE”) process. *Id.* at 574, 577. The claim required producing weight values, generating ranking criteria, eliminating the smallest ranking criterion, and then “repeating” those steps. *Id.* at 574. Although the plaintiff argued that the claimed method improved computer functionality and was therefore patent-eligible under *Alice*, the Court rejected that argument and held that claim 1 was directed to the abstract mathematical concept of SVM-RFE. *Id.* at 585. In doing so, the Court emphasized that the “the iterative nature of RFP” did not raise either SVM or RFE above the level of an abstract idea. *Id.*

That reasoning applies here. Iteration is a fundamental technique that has long been used to carry out and refine tasks. For example, humans routinely repeat steps to confirm results or make comparisons, such as by rechecking calculations or by conducting multiple trials to confirm a result. Claim 18’s reliance on repeating conventional steps, in the context of otherwise known activities, does not alter its abstract character.

Claim 18’s requirement of “comparing the first instance of the value of d) to the second instance of the value of d),” is also abstract. In *In re BRCA1- & BRCA2-Based Hereditary*

Cancer Test Pat. Litig., 774 F.3d 755, 763-64 (Fed. Cir. 2014), the court considered two method claims that required “comparing” an individual’s gene sequence to a reference sequence, identifying differences, and repeating the process for subsequent sequences. The court concluded that those claims were directed to “unpatentable abstract ideas,” explaining that they recited “nothing more than the abstract mental steps necessary to compare” two sequences and warning that “allowing a patent on the comparison step could impede a great swath of research . . . and it is antithetical to the patent laws to allow these basic building blocks of scientific research to be monopolized.” *Id.* at 764.

Here, claim 18 presents the same defect. Its “comparing” limitation requires nothing more than the same type of analytical comparison deemed by the Federal Circuit to be abstract in *In re BRCA1*. See also *Elec. Power Grp., LLC v. Alston S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (stating that claims that focus “collecting information, analyzing it, and displaying certain results of the collection and analysis” “fall into a familiar class of claims ‘directed to’ a patent-ineligible concept”); *In re Killian*, 45 F.4th 1373, 1380 (Fed. Cir. 2022) (concluding that claims “directed to collection of information, comprehending the meaning of that collected information, and indication of the results, all on a generic computer network operating in its normal, expected manner” were abstract); *Intell. Ventures I LLC v. Cap. One Fin. Corp.*, 850 F.3d 1332, 1341 (Fed. Cir. 2017) (concluding that claims related to a system which allowed users to dynamically view and update documents in different formats were abstract because they were broadly directed to the “concept of collecting, displaying, and manipulating data of particular documents”).

Claim 18 is nothing more than two abstract ideas. Layering one abstract idea on top of another does not alter the § 101 analysis where, as here, the claim remains “clearly focused on

the combination of those abstract-idea processes,” rather than on “any particular assertedly inventive technology for performing those functions.” *Id.*; see *Ubiquitous Connectivity, LP v. City of San Antonio*, No. SA-18-CV-00718-XR, 2019 WL 4696421 at *8 (W.D. Tex. Sep. 26, 2019) (“The fact that [a claim] combine[s] two abstract concepts . . . does not render [it] non-abstract.”). Accordingly, claim 18 is directed to patent-ineligible subject matter under step one of *Alice*.

(ii) At *Alice* step two, claim 18 lacks an inventive concept.

Claim 18 lacks any inventive concept. At step two of the *Alice* inquiry, courts ask whether the claim contains an “inventive concept”—that is, an element or ordered combination of elements “sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Alice*, U.S. at 217–18 (internal quotation marks and alterations omitted). Merely “[s]tating an abstract idea while adding the words ‘apply it with a computer’” is not enough to transform a patent-ineligible abstract idea into a patent-eligible invention. *Id.* at 223; see *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1368 (Fed. Cir. 2015) (“[R]eciting no more than generic computer elements performing generic computer tasks does not make an abstract idea patent-eligible.”).

Claim 18 has no inventive concept. Claim 18 does not claim any new computer architecture, improved security protocol, or particular machine-learning model. Instead, it largely incorporates the same steps recited in claim 1. Both the Supreme Court and the Federal Circuit have made clear that evidence showing claim elements were already known and routinely practiced in the field is highly probative of whether there is an inventive concept. For example, in *Mayo Collaborative Servs. v. Prometheus Lab’ys, Inc.*, 566 U.S. 66, 73 (2012), the Supreme Court held that there was no inventive concept where the claim limitations involved “well-understood, routine, conventional activity previously engaged in by researchers in the field.”

Similarly, in *In re BRCAI*, the Federal Circuit held that there was no inventive concept where the non-ineligible claim elements consisted only of “comparison techniques” that were “well-understood, routine, and conventional activity engaged in by scientists at the time of [the] patent applications.” 774 F.3d at 764.

Here, multiple references demonstrate that the steps of claim 1 were already well known and conventional, such that claim 18 amounts to nothing more than an instruction to repeat conventional steps and compare the results. *See, e.g.*, Willner II, Kitts I, O’Connell I. Those are the abstract ideas themselves, which do not suffice to transform patent-ineligible subject matter into patent-eligible subject matter at step two of *Alice*. *See Mobile Acuity, Ltd. v. Blippar Ltd.*, 110 F.4th 1280, 1294 (Fed. Cir. 2024) (“[T]he abstract idea cannot supply the inventive concept that renders the invention significantly more than the abstract idea at step two.” (internal quotation marks omitted)).

In conclusion, claim 18 fails both steps of the *Alice* inquiry. At step one, the claim is directed to the combination of two abstract ideas—repeating conventional steps and comparing results. And at step two, the claim offers no inventive concept that could transform it into patent-eligible subject matter. Claim 18 is thus invalid under § 101.

2. The ’014 patent

(a) *Alice* Step One

As set forth in detail in Exhibit F, the Asserted Claims of the ’014 patent, like those of the ’008 patent, are directed to systems for telling humans and computers apart.

Claim 16, which is illustrative, recites a “non-transitory machine readable medium” containing instructions for: (1) collecting data from a client computer (including “active data” and “passive data”); (2) analyzing that data in conjunction with “model data” derived from prior human interactions; (3) generating a “first analysis value” indicating whether the user is human;

(4) determining whether that value satisfies a threshold; and (5) requesting additional data if it does not. A person of ordinary skill in the art would recognize that claim 16 merely describes collecting data, analyzing that data, and applying an unspecified algorithm to allow or deny access to a webpage based on the outcome of the analysis. The steps recited in claim 16 are broad enough to read on both a computer performing the claimed method or a human performing it with a pen and paper.

As discussed above, the '014 patent acknowledges that the underlying concept—distinguishing human users from automated programs—long predates the alleged invention. '008 patent at 1:10–13; *see id.* 1:57–60. The claims do not depart from this abstract idea. At bottom, they recite a generalized process of (1) gathering information about a user, (2) comparing that information to prior data or expected patterns of human behavior, and (3) producing a score or value used to determine whether to grant access or request further verification. The specification confirms this high-level formulation, explaining that the invention involves comparing collected data to “model data relating to human interaction” and generating “a value that represents the likelihood” that the user is human. *See id.* at Abstract.

While the '014 patent generally describes collecting different types of “active data” (e.g., mouse movements or keystrokes) and “passive data” (e.g., cookies or IP addresses), these are simply types of information that were already commonly collected and analyzed in the prior art. *See, e.g.*, '008 patent at 4:6–17 (“Such monitoring and retaining means for acquiring data from the computing device comprises, without limitation, modification of (an) existing program(s) (e.g., such means are included in available browsers), a covert program (e.g., many malware applications log keystrokes and periodically pass them to remote servers for malicious purposes; similar technology can be used to exploit necessary aspects of the invention embodiments), or a

servlet/Java applet.”). The ’014 patent provides no specific algorithm for how to perform the claimed analysis or generate the claimed “analysis value,” instead relying on the knowledge of a person of ordinary skill in the art to implement these functions. The claimed “model data” is likewise described only at a high level as “data indicative of human interaction,” *id.* at 2:54–3:17, without any concrete implementation. In substance, the claims amount to nothing more than applying known data-collection and comparison techniques to the longstanding problem of distinguishing humans from bots.

Moreover, the ’014 patent claims rely only on generic computer components—such as a “client computer,” “server,” and “machine readable medium”—performing their ordinary functions. There are no special-purpose structures, no improvement to the functioning of the computer itself, and no specific technological solution to a technical problem. Instead, the computer is used merely as a tool to automate the abstract process of evaluating user behavior and making a determination based on that evaluation.

Setting aside these generic computer components, as the Court will do under *Alice*, the claims are no different from collecting data, comparing the data to known patterns, and assigning a score based on that comparison—activities that have long been performed in a wide variety of contexts, including standardized testing and fraud detection. Indeed, the claimed steps can be performed mentally or with pen and paper, further confirming their abstract nature. *See CyberSource*, 654 F.3d at 1372.

The application of this abstract idea in the context of Internet-based client-server interactions does not render the claims any less abstract. Limiting the claims to evaluating users seeking access to a website merely confines the abstract idea to a particular technological environment. *See Bilski*, 561 U.S. at 612; *Affinity Labs of Texas*, 838 F.3d at 1259. Courts have

repeatedly held that claims directed to analyzing user data to detect fraud or control access—precisely what is claimed here—are abstract. *See, e.g., FairWarning IP*, 839 F.3d at 1093; *Elec. Power Grp.*, 830 F.3d at 1353–54.

The remaining claims do not change this analysis. Independent claims 1 and 22 recite the same abstract idea in slightly different form, with claim 1 expressly adding that, if a user fails an initial analysis, the system may provide a CAPTCHA test and perform a second round of analysis based on the user’s response. But that additional step merely reflects the well-known, longstanding practice of escalating verification—i.e., applying additional or more rigorous tests when an initial assessment is inconclusive or suggests potential fraud. For example, in computer systems well before the priority date of the ’014 patent, if a user failed an initial login attempt, access might not have been granted but instead escalated to additional verification, such as answering security questions or providing a one-time authentication code. Likewise, in everyday interactions, identity is often confirmed through successive checks—for instance, if an individual cannot initially provide satisfactory identification, a police officer may ask follow-up questions or request additional documentation, with a correct response to those secondary inquiries confirming identity despite the initial uncertainty. The patent itself acknowledges that CAPTCHA techniques were already well-known and widely used to distinguish humans from automated programs, including increasingly complex or repeated challenges.

The dependent claims likewise add only insignificant and routine limitations. For example, claims 5, 9, 11–15, 17–18, 24, and 28–30 merely specify the types of data to be collected or analyzed—such as mouse movements, keystrokes, cookies, and IP addresses—i.e., conventional categories of information used to distinguish human from automated activity. Claims 4, 6–8, 10, 19, and 23 recite generic implementation details, such as using JavaScript or

other code to collect data, decrypting data, or allowing a website operator to set thresholds or criteria—again reflecting routine computer functionality. Claims 2, 3, 20–21, and 25–27 merely require repeating the same analysis, including through additional CAPTCHA challenges or successive rounds of scoring, which is nothing more than iterative application of the same abstract idea using admitted prior-art techniques. None of these limitations alters the fundamental character of the claims, which remain directed to collecting and analyzing user data to determine whether the user is human or a bot and controlling access based on that determination.

Accordingly, the '014 patent claims are directed to an abstract idea and are ineligible under Alice step one.

(b) *Alice Step Two*

Where the claims at issue are directed to a patent-ineligible concept, such as an abstract idea, the Court must “examine the elements of the claim to determine whether it contains an ‘inventive concept’ sufficient to ‘transform’ the claimed abstract idea into a patent-eligible application.” *Alice*, 573 U.S. at 221 (internal quotation marks omitted). Here, the elements of claim 16 and the other asserted claims of the '014 patent, taken individually or as an ordered combination, do not contain a sufficiently transformative inventive concept. The claims do not purport to improve the functioning of a computer or any other technology. Instead, they use generic computer components as tools to implement the abstract idea of evaluating user data to determine whether the user is human or a bot.

The claims recite only conventional computer components—such as a “client computer,” a “server,” and a “non-transitory machine readable medium”—performing their ordinary functions of collecting, transmitting, storing, and analyzing data. The specification confirms that these components are used in a routine manner and provides no specialized architecture or

technological improvement. Any alleged “analysis” of user data is described only at a high level, with no specific algorithm or technique for generating the claimed “analysis value.” Instead, the patent leaves such implementation details to the knowledge of a person of ordinary skill in the art, confirming that these steps were well-understood and conventional.

Nor do the claims supply an inventive concept through their use of “active data,” “passive data,” or “model data.” These are merely categories of information—such as mouse movements, keystrokes, cookies, and IP addresses—that were already commonly collected and analyzed in the prior art. The claims do not recite any new source of data, any unconventional way of collecting that data, or any specific improvement in how the data is analyzed. Rather, they simply instruct that such data be gathered and compared, which is insufficient under *Alice*. See *Elec. Power Grp.*, 830 F.3d at 1355.

The additional limitation in claim 1 of providing a CAPTCHA test if an initial analysis fails likewise does not constitute an inventive concept. As discussed above, the patent itself acknowledges that CAPTCHA techniques were well-known and widely used to distinguish humans from automated programs. The claimed use of a CAPTCHA merely applies this conventional technique as a second step in the same abstract process of user verification. Requiring additional or repeated verification steps—such as administering further challenges or collecting additional data—is a routine and conventional approach that does not transform the claims into patent-eligible subject matter.

Similarly, the dependent claims add only well-understood, routine, and conventional features. Limitations concerning the use of JavaScript or other code to collect data, the decryption of data, the specification of particular data types, or the setting of thresholds by a website operator all reflect standard computing practices. Likewise, requiring multiple rounds of

analysis or additional CAPTCHA challenges merely repeats the same abstract idea using conventional techniques. Considered individually or as an ordered combination, these limitations do not provide “significantly more” than the abstract idea itself.

The mere fact that the claimed systems purport to improve the accuracy or efficiency of distinguishing humans from bots, or to operate at a speed or scale not achievable by humans, is insufficient to demonstrate an inventive concept. The Federal Circuit has repeatedly rejected such arguments where the alleged improvement is not tied to a specific technological solution. *See, e.g., Vehicle Intelligence*, 635 F. App’x at 920 (rejecting claims that purported to provide “faster, more accurate and reliable” analysis). Here, the claims do not specify how any such improvement is achieved, instead reciting only the desired result of more effectively distinguishing humans from bots.

At most, the claims require that the abstract idea be implemented on a generic computer system. But “after Alice, there can remain no doubt: recitation of generic computer limitations does not make an otherwise ineligible claim patent-eligible.” *DDR Holdings*, 773 F.3d at 1256. Nor does limiting the claims to Internet-based interactions or website access confer eligibility. *See FairWarning*, 839 F.3d at 1097. In short, there is nothing in the asserted claims—either individually or in combination—that transforms the abstract idea into a patent-eligible application. The claims merely apply conventional data collection and analysis techniques, using generic computer components, to the longstanding problem of distinguishing humans from automated programs. They therefore fail *Alice* step two.

IV. Accompanying Document Production

Pursuant to the original Scheduling Order in this action (Dkt. 38), Google produced with its Preliminary Invalidity and Subject-Matter Eligibility Contentions prior art bearing the following Bates numbers: GOOG-NOBOTS-PA-00000001 – GOOG-NOBOTS-PA-00013877.

May 2, 2022. In addition, Google produced d with its Second Preliminary Invalidity and Subject-Matter Eligibility Contentions additional prior art bearing Bates numbers GOOG-NOBOTS-PA-00014200 – GOOG-NOBOTS-PA-00015339.

Google reserves the right to supplement its production of documents as the case progresses, including, but not limited to, producing or making additional documents or source code available for inspection. Google also reserves the right to seek third-party discovery relevant to the prior art once fact discovery opens in this case.

Dated: May 13, 2026

Heather E. Takahashi (admitted to WDTX)
heather.takahashi@mto.com
Rebecca Ho (pro hac vice)
rebecca.ho@mto.com
Kevin Chiu (pro hac vice)
kevin.chiu@mto.com
MUNGER, TOLLES & OLSON LLP
350 South Grand Avenue, Fiftieth Floor
Los Angeles, California 90071
Telephone: 213-683-9100
Facsimile: 213-687-3702

/s/ Heather E. Takahashi
Darryl J. Adams (TX Bar No. 00796101)
dadams@sgbfirm.com
Brian C. Banner (TX Bar No. 24059416)
bbanner@sgbfirm.com
SLAYDEN GRUBERT BEARD PLLC
401 Congress Ave., Suite 1650
Austin, Texas 78701
Telephone: 512-402-3569
Facsimile: 512-402-6865

Evan Mann (pro hac vice)
evan.mann@mto.com
MUNGER, TOLLES & OLSON LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
Telephone: 415-512-4000
Facsimile: 415-512-4077

Attorneys for Defendant Google LLC

Deleted: At this time

Deleted: s

Deleted: these

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font color: Black

Formatted: Font color: Black

Deleted: April 15

Moved (insertion) [1]

Moved up [1]:)¶
heather.takahashi@mto.com¶
Rebecca Ho (pro hac vice)¶
rebecca.ho@mto.com¶
Kevin Chiu (pro hac vice)¶
kevin.chiu@mto.com¶
MUNGER, TOLLES & OLSON LLP¶
350 South Grand Avenue, Fiftieth Floor¶
Los Angeles, California 90071¶
Telephone: 213-683-9100¶
Facsimile: 213-687-3702

Deleted: Heather E. Takahashi (pro hac vice

Deleted: ¶
¶

Deleted: ¶

Formatted: Space After: 8 pt, Line spacing:
Multiple 1.08 li, Hyphenate

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document was served by electronic mail on all counsel of record who are deemed to have consented to electronic service in accordance with Local Rule CV-5. I declare under penalty of perjury that the foregoing is true and correct.

Dated: [May 13](#), 2026

/s/ Heather E. Takahashi
Heather E. Takahashi

Formatted: Space After: 8 pt, Line spacing: Multiple 1.08 li, Hyphenate

Deleted: (and accompanying claim chart exhibits)

Deleted: April 15