**UNITED STATES DISTRICT COURT**
**WESTERN DISTRICT OF TEXAS**
**WACO DIVISION**

| | |
|---|---|
| NOBOTS LLC,<br>Plaintiff,<br>vs.<br>GOOGLE, LLC,<br>Defendant. | Case No. 6:21-cv-1290<br><br>**JURY TRIAL DEMANDED** |

# COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Nobots LLC ("Nobots") makes the following allegations against Google, LLC ("Google"), who without authority makes, distributes, offers for sale, and/or sells in the United States products and/or operating system software for products that infringe the Asserted Patents.

## PARTIES

1. Plaintiff Nobots LLC is a limited liability company organized and existing under the laws of the State of Washington with a place of business at 13946 147th Place SE, Renton, Washington 98059. Nobots is the owner of all rights, title, and interest in and to United States Patent No. 9,595,008 (the "'008 Patent") and United States Patent No. 10,423,885 (the "'885 Patent") (together, the "Asserted Patents").

2. Defendant Google, LLC is a limited liability company organized under the laws of Delaware. Google maintains regular and established places of business throughout this District, including at 100 Congress Avenue, Austin, Texas, 78701; 901 E. Fifth Street, Austin, Texas, 78701; 500 West Second Street, Austin, Texas, 78701; 601 West Second Street, Austin, Texas, 78701; and 110 East Houston Street, San Antonio, Texas, 78205. Google may be served with

process through its registered agent, the Corporation Service Company, at 211 East 7th Street, Suite 620, Austin, Texas, 78701. Google is registered to do business in the State of Texas and has been since at least November 17, 2006.

3. Google also owns personal property throughout this District, including at 807 Ruby Drive, Austin, Texas, 78753; 10200 MC Kalla Place, Austin, Texas, 78758; 500 Chicon Street B, Austin, Texas, 78702; 500 West Second Street, Austin, Texas, 78701; 201 Colorado Street, Austin, Texas, 78701; 4100 Smith School Road, Austin, Texas, 78744; 701 E Parmer Lane, Austin, Texas, 78753; 845 Interchange Boulevard, Austin, Texas, 78721; 500 West Second Street 1450, Austin, Texas, 78701; 9606 N. Mo-Pac Expressway 700, Austin, Texas, 78759; 304 E. 24th Street, Austin, Texas, 78705; 100 East Houston Street, San Antonio, Texas, 78205; 8862 Garnett, San Antonio, Texas, 74221; 5903 Distribution, San Antonio, Texas, 78218; 819 S Laredo, San Antonio, Texas, 78204; 2350 South Midkiff Road, Midland, Texas, 79701; 500 West Overland Avenue, El Paso, Texas, 79901; 501 West Overland Avenue, El Paso, Texas, 79901; 4140 Rio Bravo Street, El Paso, Texas, 79902.

4. Google does business in this District and across the State of Texas. It has over 1,700 full-time employees in Texas. On information and belief, the majority of those employees are located in this District. Google proudly touts that it provided $26.45 billion of economic activity for 162,400 Texas businesses, nonprofits, publishers, creators, and developers in 2020, and that 1.43 million Texas businesses connect directly with their customers using Google products, including those that infringe and unlawfully profit off the inventions claimed in the Asserted Patents. This year, Google announced its plans to invest $50 million in Texas in 2021 in office space and data centers alone. Google also proudly touts that it has awarded over $10 million in grants to nonprofits and organizations based in Texas, has donated over $10 million in charitable

giving to Texas nonprofits, and has invested more than $1 billion in renewable energy in Texas. For these and other reasons, and to generate additional business in and tax incentives from the State of Texas, Google proudly calls this District, "Our home in the Lone Star State," for which "Google is proud to have roots in Texas, with our Austin office housing teams focused on Android, Google Cloud, finance, and more," including designing, implementing, and monetizing those methods and products that infringe the Asserted Patents.[1]

5. In addition to its offices and employees in this District, Google also has places of business and employees and agents conducting its business throughout the State of Texas, including through methods and practices that unlawfully infringe and make money off the inventions claimed in the Asserted Patents, such as at its office in Dallas, its data center in Midlothian, and its brand-new office in Houston (built in 2021).

6. On information and belief, Google's in-house legal department also has a substantial presence in Austin, Texas. Google's Careers website includes job postings for both "Litigation Counsel, Patent Litigation" and "Litigation Paralegal" roles with the option to work in Austin.[2] Given the location of Google legal personnel in Austin, on information and belief, documents, materials, and potential witnesses relevant to this action are located in this District.

7. Google has placed or contributed to placing infringing products, such as Google reCAPTCHA, into the stream of commerce via established distribution channels knowing or understanding that such products would be sold and used in the United States, including in this District. Google also has derived substantial revenue from infringing acts in this District, including

---

[1] *See, e.g.*, Economic Impact Report Texas, *Google Helps Texas Businesses Move Toward Their Goals* (accessed Nov. 11, 2021), available at: https://economicimpact.google.com/state/tx/

[2] *See, e.g.*, Google Careers, *Litigation Counsel, Patent Litigation* (accessed Oct. 3, 2021), available at: https://careers.google.com/jobs/results/129929351756948166-litigation-counsel-patent-litigation/?category=LEGAL&company=Google&company=YouTube&hl=en&jlo=en-US&location=Austin,%20TX,%20USA.

from development, distribution, and sale of the infringing methods, such as reCAPTCHA.

8. On information and belief, Google designs, manufactures, distributes, imports, offers for sale, and/or sells in the State of Texas and this District products and/or operating system software for products that infringe the Asserted Patents.

## JURISDICTION AND VENUE

9. This is an action for patent infringement arising under the patent laws of the United States. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Google because it conducts business in and has committed acts of patent infringement in this District and throughout the State of Texas, and has established minimum contacts with this forum state such that the exercise of jurisdiction over Google would not offend the traditional notions of fair play and substantial justice.

11. Upon information and belief, Google transacts substantial business with entities and individuals in the State of Texas and this District by, among other things, designing, using, offering to sell, distributing, and selling products and/or operating system software for products that infringe the Asserted Patents, including the infringing reCAPTCHA methods that Google purposefully uses, sells, offers for sale, and directs into the State of Texas and this District as alleged herein, as well as by providing service and support to reCAPTCHA customers in this District,[3] and/or inducing others to commit acts of patent infringement in this District.

12. Google places the accused methods into the stream of commerce via authorized and established distribution channels with the knowledge and expectation that they will be used and sold in the State of Texas and this District, and does not otherwise permit the use, distribution, or

[3] *See, e.g., Honor Code Reporting Form*, Baylor Univ., https://cm.maxient.com/reportingform.php?BaylorUniv&layout_id=5 (last visited Nov. 5, 2021) (reflecting that the page is protected by reCAPTCHA v2 Invisible, one of the infringing methods of reCAPTCHA).

sale of the accused methods outside of these authorized and established distribution channels.

13. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because Google has committed acts of infringement in this District and has regular and established places of business in this District, including at 100 Congress Avenue, Austin, Texas, 78701; 901 E. Fifth Street, Austin, Texas, 78701; 500 West Second Street, Austin, Texas, 78701; 601 West Second Street, Austin, Texas, 78701; and 110 East Houston Street, San Antonio, Texas 78205. *See In re Cray Inc.*, 871 F.3d 1355, 1362-63 (Fed. Cir. 2017).

14. Furthermore, Google designs, uses, distributes, sells, and/or offers for sale the accused reCAPTCHA methods to consumers, businesses, education facilities, and government organizations located in this District, such as Baylor University, Board & Brush, Billy Bob's Burgers, LeafFilter, and Roots Waco, all located in Waco, Texas. For example, Baylor University's website reflects that it is protected by reCAPTCHA v2 Invisible,[4] an accused method of reCAPTCHA discussed in further detail in paragraph 41, *infra*. When consumers in this District, and across the State of Texas, access the websites and apps of such businesses in this District, Google subjects these businesses and consumers in this District to Google's privacy policies and uses Google's infringing reCAPTCHA methods and products to collect personal information and data from the consumers in this District for Google's own use and profit.

15. Upon information and belief, a substantial number of Google employees based in or who regularly conduct Google business from this District have knowledge, information, documents, and things relevant to this action and are potential witnesses to this action, including as to Google's infringing activities and Nobots's damages. For instance, Bhanchand Prasad, a

[4] *See id.*

reCAPTCHA Security Customer Engineer at Google Cloud, is located in Austin, Texas.[5] As another example, Marty Sedlacek, Head of Solutions Sales at Google Cloud, who is responsible for corporate strategy in support of all Google Cloud technologies, including Google reCAPTCHA, also is located in Austin, Texas.[6] As another example, Zach Jordan, Head of Sales, Digital Enterprise, at Google Cloud, who oversees Google Cloud sales to enterprise clients, also is located in Austin, Texas.[7] As another example, Jen Person, Senior Development Advocate for Google Cloud, who is responsible for driving customer success and educating developers about Google Cloud, including reCAPTCHA, also is located in Austin, Texas.[8]

## THE ASSERTED PATENTS

16. This Complaint asserts causes of action for infringement of United States Patent No. 9,595,008 and United States Patent No. 10,423,885. The Asserted Patents are valid and enforceable United States Patents, the entire right, title, and interest to which Nobots owns by assignment.

17. The Asserted Patents improve upon and teach novel "CAPTCHA" (Completely Automated Public Turing test to tell Computers and Humans Apart) methods for assessing a confidence level that an operator of a computing device interacting with a server is a human being

---

[5] *See Bhanchand Prasad*, LinkedIn, https://www.linkedin.com/in/bhanchand-prasad (last visited Nov. 13, 2021).

[6] *See Marty Sedlacek*, LinkedIn, https://www.linkedin.com/in/marty-sedlacek-0b4393/ (last visited Nov. 13, 2021); *see also, e.g.*, Sedlacek, Marty [@martyjsedlacek], "See how Caribou Coffee uses reCAPTCHA Enterprise to create safe and frictionless digital experiences @googlecloud." *Twitter*, Sept. 2, 2021, https://twitter.com/search?lang=en&q=(recaptcha%20OR%20security%20OR%20bot)%20(from%3Amartyjsedlacek)&src=typed_query (last visited Nov. 13, 2021)

[7] *See Zach Jordan*, LinkedIn, https://www.linkedin.com/in/zachjordan1/ (last visited Nov. 13, 2021).

[8] *See Jen Person*, Developer Advocates, https://cloud.google.com/developers/advocates/jen-person (last visited Nov. 13, 2021); *see also, e.g.*, Jen Person, *reCAPTCHA Enterprise, Network Connectivity Center, & More*, YouTube (Nov. 8, 2021), available at https://www.youtube.com/watch?v=pJNSsyojkys (last visited Nov. 13, 2021).

rather than an autonomic computer application employing various algorithms and routines (a "bot") and protecting websites and applications from fraudulent activity, spam, and abuse without creating friction for human users.

18. On March 14, 2017, the U.S. Patent and Trademark Office duly and legally issued the '008 Patent, which is entitled "Systems, Methods, Apparatus for Evaluating Status of Computing Device User." A true and correct copy of the '008 Patent is attached as **Exhibit A**.

19. The '008 Patent generally claims methods for assessing a confidence level that an operator of a client computing device interacting with a server is a human rather than a bot, by presenting issued data from the 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.

20. To the extent applicable, Nobots has complied with 35 U.S.C. § 287(a) with respect to the '008 Patent.

21. On September 24, 2019, the U.S. Patent and Trademark Office duly and legally issued the '885 Patent, which is entitled "Systems, Methods and Apparatus for Evaluating Status of Computing Device User." A true and correct copy of the '885 Patent is attached as **Exhibit B**.

22. The '885 Patent generally claims methods for testing for the presence of biometric data associated with an operator of a computing device attempting to access a server and controlling access to the server by denying access to the computing device when the biometric data is not present and/or not denying access of the computing device when some biometric data is present.

23. To the extent applicable, Nobots has complied with 35 U.S.C. § 287(a) with respect to the '885 Patent.

24. Nobots owns all rights, title, and interest in and to the Asserted Patents, including the sole right to sue for any infringement, and possesses all rights of recovery.

## FACTUAL ALLEGATIONS

25. Fraudulent web activities cost enterprises billions of dollars each year. Security teams need to keep bots out of their websites and applications while ensuring that their human customers can always get in. In an effort to block these bots, builders of websites and apps have created a variety of security methods to determine if the user is a bot or a human. The object is to create a test that a bot cannot easily parse but that is passable by a human.

26. Carnegie Mellon University coined the term "CAPTCHA" (Completely Automated Public Turing test to tell Computers and Humans Apart) for these types of tests. Initial efforts required a user to simply enter an alphanumeric string into an input field. However, as character-recognition engines became more available, such tests became easily defeated.

27. In 2007, Timothy P. Heikell invented CAPTCHA security methods that use information such as, without limitation, biometric data, browser cookies, destination IP histories, originating IP address, originating IP address traffic data, originating IP address physical location, third-party data regarding abusers, etc., and a confidence score analysis to prevent fraud and keep bots out of websites and apps while allowing desired users to gain access to offered content, through methods which can easily be implemented, automatically, without requiring additional user input and thus without bothering, frustrating, or stopping safe or desired users.

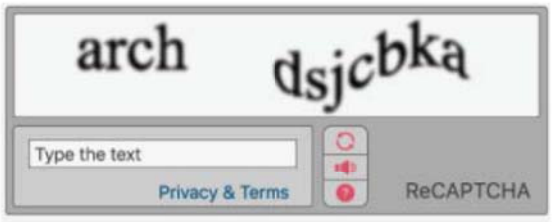
28. These novel and now-popular methods claimed in the Asserted Patents significantly improve upon prior CAPTCHA security methods, satisfy long-felt needs of enterprises and consumers alike, and are now wildly commercially successful for Google, who reportedly employs them hundreds of millions of times every day.

29. For many years after 2007, however, the most popular websites in the world, including Google, Yahoo, YouTube, Microsoft's Live ID, MySpace, Facebook, Wikipedia, and Craigslist, continued to use prior art CAPTCHA security methods. Initial efforts required a user to simply enter an alphanumeric string into an input field, requiring the user to type the letters, digits, or characters of a distorted image appearing on the screen. These prior art methods provided rudimentary security, were dependent on user input and proficiency, and could not be implemented in all settings or for all users. For example, users with certain disabilities, such as those who are visually impaired or have dyslexia, and users who are not native English speakers may have trouble with parsing through the distorted text employed by prior art CAPTCHA methods.

30. In 2009, Google acquired reCAPTCHA, a company that had provided CAPTCHAs to help protect more than 100,000 websites from spam and fraud.[9] Google reportedly acquired the reCAPTCHA technology for between $10 million and $100 million.[10]

31. For many years thereafter, the reCAPTCHA utility that Google used involved a challenge-response test to determine whether or not a user was a human. As depicted in Figure 1, one test presented distorted text that a user needed to enter to prove the user was human.

**Figure 1**




[9] *Teaching Computers to Read: Google Acquires reCAPTCHA*, Google Blog (Sept. 16, 2009), available at https://googleblog.blogspot.com/2009/09/teaching-computers-to-read-google.html (last accessed on Nov. 13, 2021).

[10] Alison Griswold, *How Luis Von Ahn Turned countless Hours of Mindless Activity Into Something Valuable*, Business Insider (Mar. 13, 2014), available at https://www.businessinsider.com/luis-von-ahn-creator-of-duolingo-recaptcha-2014-3 (last accessed on Nov. 13, 2021).

32. Such tests were successful for a period of time in preventing non-adaptive software from recognizing the imaged characters, but people intent on abusing websites soon designed ways to circumvent the CAPTCHA, such as through specially tuned character recognition programs. As bots and fraudsters became more sophisticated, the desire to defeat the bots and prevent fraud resulted in images that were so distorted that some human users could not decipher the images.

33. Another attempt at a solution, also depicted in Figure 1 above, was to add a link to a sound file that would speak the distorted characters to the user, but this attempt at a solution also failed when these sound files also needed to be drastically distorted to protect against being discerned by increasingly sophisticated bots employing speech pattern matching algorithms. This attempt at a solution also could not easily be implemented for all users or in all settings because, for example, not all users have functioning audio equipment and environments such as libraries, government utilities, and work settings may not permit or enable such auditory methods.

34. Despite their widespread use, these prior art security methods proved ineffective and frustrating. Because computer artificial intelligence quickly improved in responding to the type of challenge-response test depicted in Figure 1, such techniques became ineffective at eliminating bots. And the desire to defeat these increasingly intelligent bots also resulted in images that were so distorted that human users, especially those with visual or hearing deficiency or imparity, became unable to pass the tests. The end result was that the prior art CAPTCHA methods were neither keeping out bots and preventing fraud, nor permitting human users to get in and access the desired content, at least not without blocking or frustrating significant human users.

35. What was needed was a more robust form of security—one that was neither easily defeated by bots, nor would keep out or frustrate human users trying to access the enterprises' websites and applications. As claimed in the Asserted Patents, Mr. Heikell solved this long-felt

need by inventing, way back in 2007, new and improved CAPTCHA security methods, which shifted the burden of proof for assessing the likely user status of a computing device from the user side to the server side of the equation, by analyzing biometric and other available data of the user in response to data issued by the server and yielding a probability value, or confidence score, that the user is a human being rather than a bot.

36. For example, in exemplary embodiments, this assessment method comprises comparing acquired or available data relating to the operation of the computing device to suitable models embodying human user derived data, or model data, indicative of human interaction with a computing device. Operating in the background, and without the need for the user to decipher or pass any challenge-response tests, the methods monitor at least some data generated by the user trying to access the website or application (e.g., mouse movements, key stroke combinations, browser cookies, IP addresses), compare the data generated by the user to model data indicative of a human interaction, and generate 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 a bot.

37. Nobots's inventions are incredibly valuable and significantly improved upon the prior art CAPTCHA security methods. Focusing on biometric and/or passive data (such as, e.g., browser cookies or IP information) passed from the computing device, rather than on answers to prior art challenge-response tests, achieves the objective of keeping bots out and permitting access by human users, while enhancing and without frustrating the human user experience on the website or app. Because a given dataset for each human person is unique, and not easily replicated by bots, security is enhanced without increasing the likelihood that desired human users will "fail" the assessment as was common with the prior art challenge-response methods. The user experience also is enhanced because the assessment can occur and a confidence level can be generated without

requiring any incremental inputs from the user. For example, both biometric data and passive user data can be monitored and compared in the background without prompting the user for such data.

38. By yielding a probability value or confidence level that an operator of a client computing device is a human user rather than a bot, instead of the prior art method of yielding a binary conclusion of bot or not, exemplary embodiments of the CAPTCHA security methods claimed in the Asserted Patents also enable a program or administrator on the website or application to permit or deny access and/or operation to the computing device along a sliding scale, rather than binary "in" or "out." In such an exemplary embodiment, if no biometric activity is recorded, there is a very high probability that the user is actually a bot; if substantial and robust biometric activity is recorded, there is a very high probability that the user is actually a human; and when the claimed methods yield a confidence level between these two probability levels, the administrator of the server is empowered to choose which confidence values, in which circumstances, must be generated in order for the operator of the client computing device to be permitted access to the subject website or app. By avoiding the "there is only one right answer" phenomenon inherent in the prior art, such embodiments also simultaneously enhance security without unnecessarily impairing the user experience because the old mode one-sized-fits-all methods are replaced by a more dynamic security regime in which each website (e.g., social media websites versus bank websites) and even pages within websites (e.g., home pages versus credit card checkout pages) can define (and change) the confidence value which must be generated to permit access to their site.

39. The methods taught by the Asserted Patents also are easily implemented, automatically, without incremental user input, for all human users, in all settings, for use in websites and apps alike. The recited comparisons can take place locally on the computing device,

remotely on the originating server, or on a server dedicated to performing such actions. Because the exemplary embodiments can be accomplished exclusively from the server side, it is not necessary to distribute or install in the conventional sense client-side software, and existing available browsers and operating systems provide the means necessary to carry out the invented methods. For example, neither biometric nor passive user data is affected by visual or hearing deficiency or imparity, or even just by a lack of human user literacy or proficiency. Auditory and visual challenges can be eliminated entirely.

40. In December 2014, more than seven years after Mr. Heikell invented these revolutionary CAPTCHA security methods and filed for patent protection in the Asserted Patents, Google implemented and began using, distributing, offering for sale, and selling reCAPTCHA v2, which practiced Mr. Heikell's inventions. Eliminating the need for a user to read and decipher distorted text, as required by reCAPTCHA and demonstrated in Figure 1 above, reCAPTCHA v2 instead required users to select a checkbox next to the words "I am not a robot," as depicted in Figure 2 below. When the checkbox was selected, a web request was made to Google, which then evaluated the likelihood that the user was a human or a bot based on a comparison of model data and the computing device's passive data and/or interactions with the web page. In certain cases, as depicted in Figure 3 below, Google's reCAPTCHA v2 required users to complete an additional or different test, in which the user was asked to, for example, select from a group of images a subset of those images with certain characteristics. This method of reCAPTCHA also includes the use of event listeners to monitor for biometric data. Although each of these methods started to rely on comparisons of monitored data and model data, as taught by the Asserted Patents, Google reCAPTCHA v2 remained dependent on the prior art challenge-response, user-focused security regime.

**Figure 2**

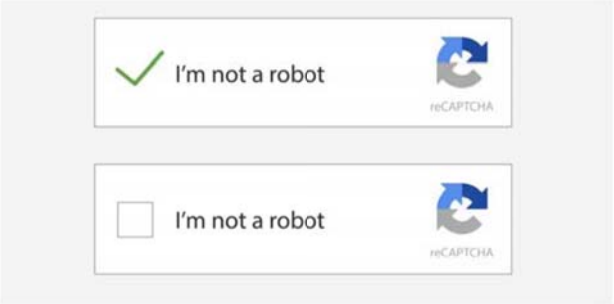
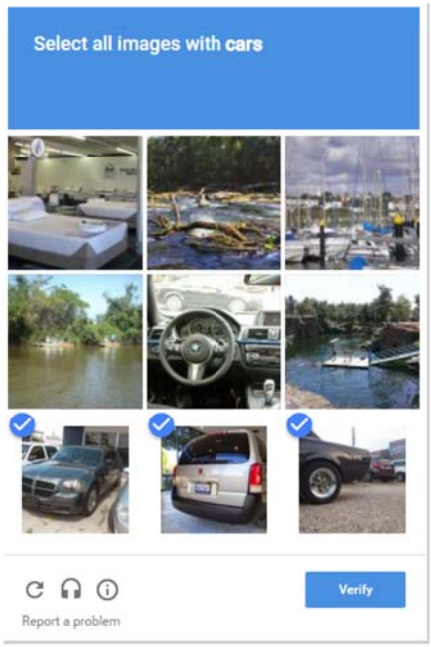



**Figure 3**




41. On March 14, 2017, the United States Patent and Trademark Office issued the '008 Patent, entitled "Systems, Methods, Apparatus for Evaluating Status of Computing Device User." That same month, Google launched reCAPTCHA v2 Invisible or "Invisible reCAPTCHA." In Google's words, "To stay one step ahead of the bad guys, reCAPTCHA needed to keep evolving to ensure the most delightful user experience. And now we're taking it even further. Can you see it? Of course not. It's invisible. Powering these advances is a combination of machine learning and advanced risk analysis that adapt to new and emerging threats. So whether on desktop or mobile, reCAPTCHA still means no frustration. People get to where they're going faster and everyone

stays happy, except bots."[11] The infringing methods employed by Google's Invisible reCAPTCHA were immediately and contemporaneously praised as "new" and "better" technology, allegedly developed by Google—and not by Mr. Heikell nearly a decade earlier, as actually was the case.[12]

42. On January 11, 2018, the United States Patent and Trademark Office published Patent Application US 2018/0012138 A1, which would later issue as the '885 Patent.

43. On October 29, 2018—more than eleven years after Mr. Heikell made his patented inventions, nineteen months after the '008 Patent issued, and ten months after the '885 Patent application was published—Google launched reCAPTCHA v3, which Google again heralded as "the new way to stop bots" because it works "without user interaction" and "returns a score so you can choose the most appropriate action for your website,"[13] even though these methods had been invented by Mr. Heikell way back in 2007. As Google put it at the time, "Now with reCAPTCHA v3, we are fundamentally changing how sites can test for human vs. bot activities by returning a score to tell you how suspicious an interaction is and eliminating the need to interrupt users with challenges at all. reCAPTCHA v3 runs adaptive risk analysis in the background to alert you of

---

[11] *See* Google Search Central, *reCAPTCHA: Tough on Bots, Easy on Humans*, YouTube (May 19, 2016), available at https://www.youtube.com/watch?v=GeibaHfYW9o&t=18s (last accessed on Nov. 14, 2021).

[12] *See, e.g.*, Ayesha Ahmad, *No More Blurry Images to Prove You're a Human – Google Introduced Invisible reCAPTCHA*, MustTech News (Mar. 21, 2017), available at https://www.musttechnews.com/google-introduces-invisible-recaptcha/ (last accessed Nov. 14, 2021); Shona Ghosh, *Google Has Killed Off reCAPTCHA As You Know It*, Business Insider (Mar. 13, 2017), available at https://www.businessinsider.com/googles-recaptcha-is-now-invisible-2017-3 (last accessed Nov. 14, 2021); Rob Verger, *Google Just Made the Internet A Tiny Bit Less Annoying*: *See ya, CAPTCHA!*, Popular Science (Mar. 11, 2017), available at https://www.popsci.com/google-invisible-recaptcha/#page-3 (last accessed Nov. 14, 2021); Ron Amadeo, *Google's reCAPTCHA Turns 'Invisible,' Will Separate Bots From People Without Challenges*, Ars Technica (Mar. 9, 2017), available at https://arstechnica.com/gadgets/2017/03/googles-recaptcha-announces-invisible-background-captchas/ (last accessed Nov. 14, 2021).

[13] *See* Wei Lu, *Introducing reCAPTCHA v3: the new way to stop bots*, Google Search Central Blog (Oct. 29, 2018), available at https://developers.google.com/search/blog/2018/10/introducing-recaptcha-v3-new-way-to (last accessed Nov. 30, 2021).

suspicious traffic while letting your human users enjoy a frictionless experience on your site."[14]

44. At all times since the Asserted Patents issued, and through the present and continuing forward, Google has continuously implemented, used, distributed, offered for sale, and sold CAPTCHA security methods that infringe the Asserted Patents—including, without limitation, Google reCAPTCHA v2 Checkbox, Google reCAPTCHA v2 Invisible, Google reCAPTCHA v3, and Google reCAPTCHA Enterprise. Google has acted and continues to act unlawfully, without Nobots's consent or authorization, and without paying Nobots a reasonable royalty for Google's substantial use of Nobots's novel and valuable inventions.

## COUNT ONE
## INFRINGEMENT OF U.S. PATENT NO. 9,595,008

45. Nobots repeats and incorporates by reference each preceding paragraph as if fully set forth herein and further states:

46. Google has infringed and continues to infringe at least claim 1 of the '008 Patent in violation of 35 U.S.C. § 271, either literally or through the doctrine of equivalents, by making, using, selling, or offering for sale in the United States, and/or importing into the United States, without authorization, utilities that practice at least Claim 1 of the '008 Patent. Google is liable for its infringement of the '008 Patent pursuant to 35 U.S.C. § 271(a), (b), and (c).

47. More specifically, Google designs, implements, imports, offers for sale, and/or sells CAPTCHA security methods that assess 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, or bot, based on a comparison of monitored user data and generates a value representing a confidence level that a human, and not a bot, is operating the client computing device.

48. Claim 1 is illustrative of the '008 Patent. It recites "[a] method for assessing a

[14] *Id.*

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:

a) a single user of a client computing devices requesting data from a server;

b) the server presenting data issued by the server to the client computing device;

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

d) comparing the monitored data to model data relating to human interaction with or in response to the issued data;

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."

49. Each of the accused reCAPTCHA methods meet every element of this claim.[15] As described above, each of the three improved reCAPTCHA methods implemented by Google is a method for assessing a confidence level that a user of a client computing device interacting with a server is a human being rather than an autonomic computer application. Google itself explains that reCAPTCHA "protects your site from spam and abuse. It uses advanced risk analysis techniques to tell humans and bots apart."[16]

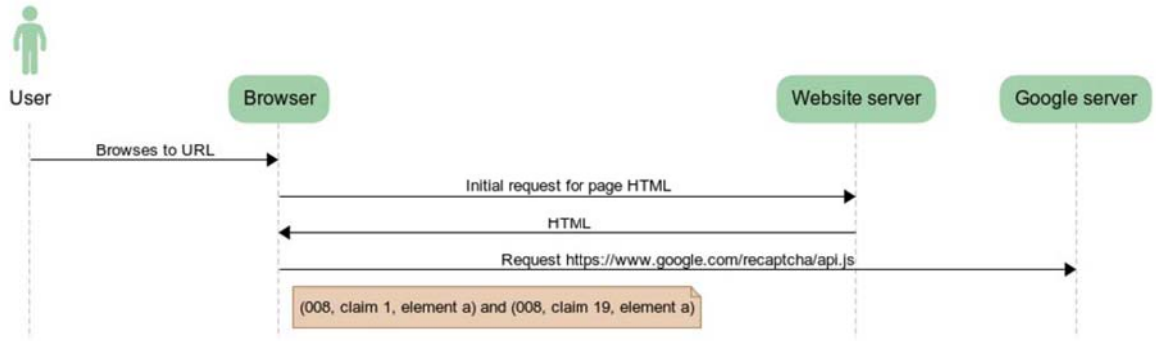
50. Each of the accused reCAPTCHA methods requires that one or more single users of a client computing device request data from a server. For example, reCAPTCHA involves a user submitting a form to a web site. To do this, the user's browser must make a request to the web

[15] This description of infringement is illustrative and not intended to be an exhaustive or limiting explanation of every manner in which Google's products infringe the '008 Patent.

[16] *See What is reCAPTCHA?*, reCAPTCHA, https://developers.google.com/recaptcha (last visited Nov. 5, 2021).

site's server. The server then responds with HTML provided by Google that includes a script tag instructing the browser to make a request to google.com to download the reCAPTCHA JavaScript. This is illustrated in Figure 4 below.

**Figure 4**




51. Figure 5 below shows sample code on Google's reCAPTCHA website depicting this script:

**Figure 5**

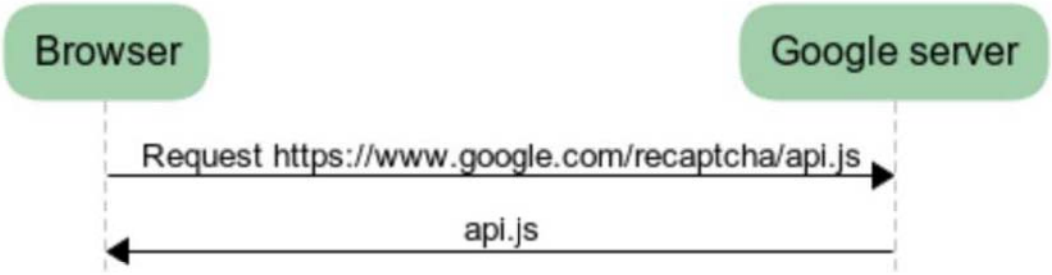
```
<html>
  <head>
    <title>reCAPTCHA demo: Simple page</title>
    <script src="https://www.google.com/recaptcha/api.js" async defer></script>
  </head>
  <body>
    <form action="?" method="POST">
      <div class="g-recaptcha" data-sitekey="your_site_key"></div>
      <br/>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>
```

**Source:** *reCAPTCHA v.2*, reCAPTCHA, https://developers.google.com/recaptcha/docs/display (last visited Nov. 5, 2021).

52. Each of the accused reCAPTCHA methods also requires that the server respond by presenting data issued by the server to the client computing device. For example, when the sample code in Figure 5 from Google's reCAPTCHA website is executed, one or more Google servers

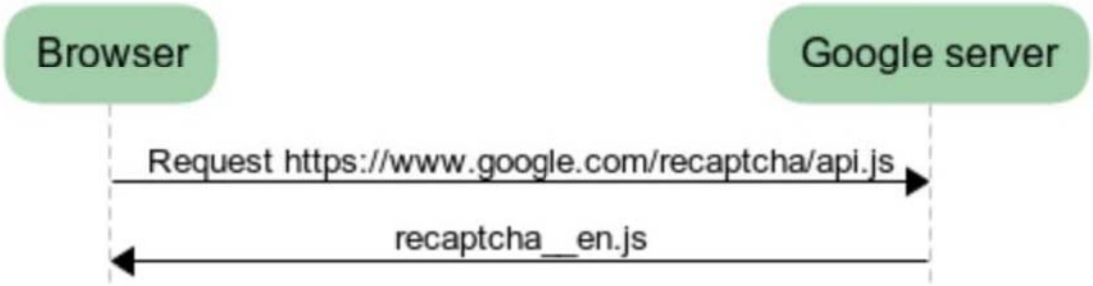
responds by sending the browser JavaScript code to the client computing device. In particular, and as depicted in Figure 6 below, the server responds with a JavaScript file called api.js.

**Figure 6**




53. Subsequently, one or more Google servers present additional data, including a JavaScript file such as "recaptcha_en.js."[17] This is depicted in Figure 7, below.

**Figure 7**

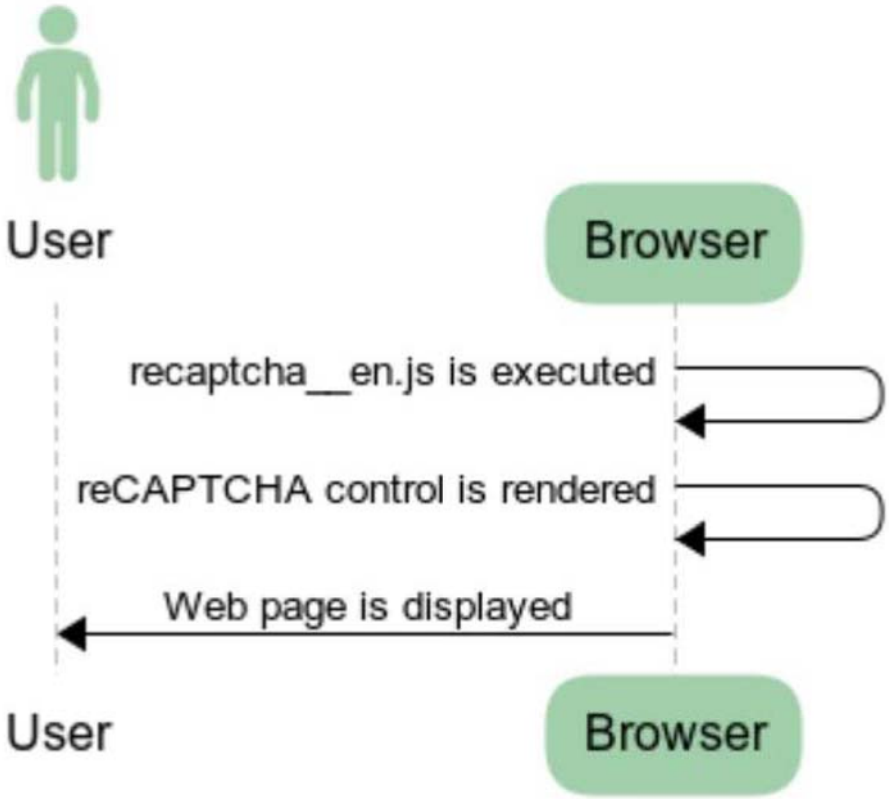



54. Each of the accused reCAPTCHA methods requires monitoring at least some data generated by the user at the client computing device in response to the issued data. For example, the JavaScript code Google transmits to the user adds what are known as "event listeners," code that is executed upon the occurrence of certain actions, such as the activation of an on-screen button, the movement of a mouse pointer, the scrolling of a web page, the placement of a cursor

[17] The "en" in the file name defines the language that will be used when the widget is rendered and can change; for instance, were French to be used, then the "en" would be "fr" instead.

in or out of a form field, and the like.[18] Such "event listeners" allow Google to monitor and track keyboard, mouse, touch, scroll and, resize events and movements. Figure 8 below depicts the creation of event listeners upon the execution of "reCAPTCHA_en.js."

**Figure 8**




55. The operation of event listeners is further demonstrated by Figures 9 and 10 below, which show how the use of reCAPTCHA v2 Checkbox allows for mouse movements to be tracked.

[18] *See, e.g., JavaScript: Events and Listeners*, I'd Rather be Writing, https://idratherbewriting.com/events-and-listeners-javascript/ (last visited Nov. 5, 2021).

**Figure 9**

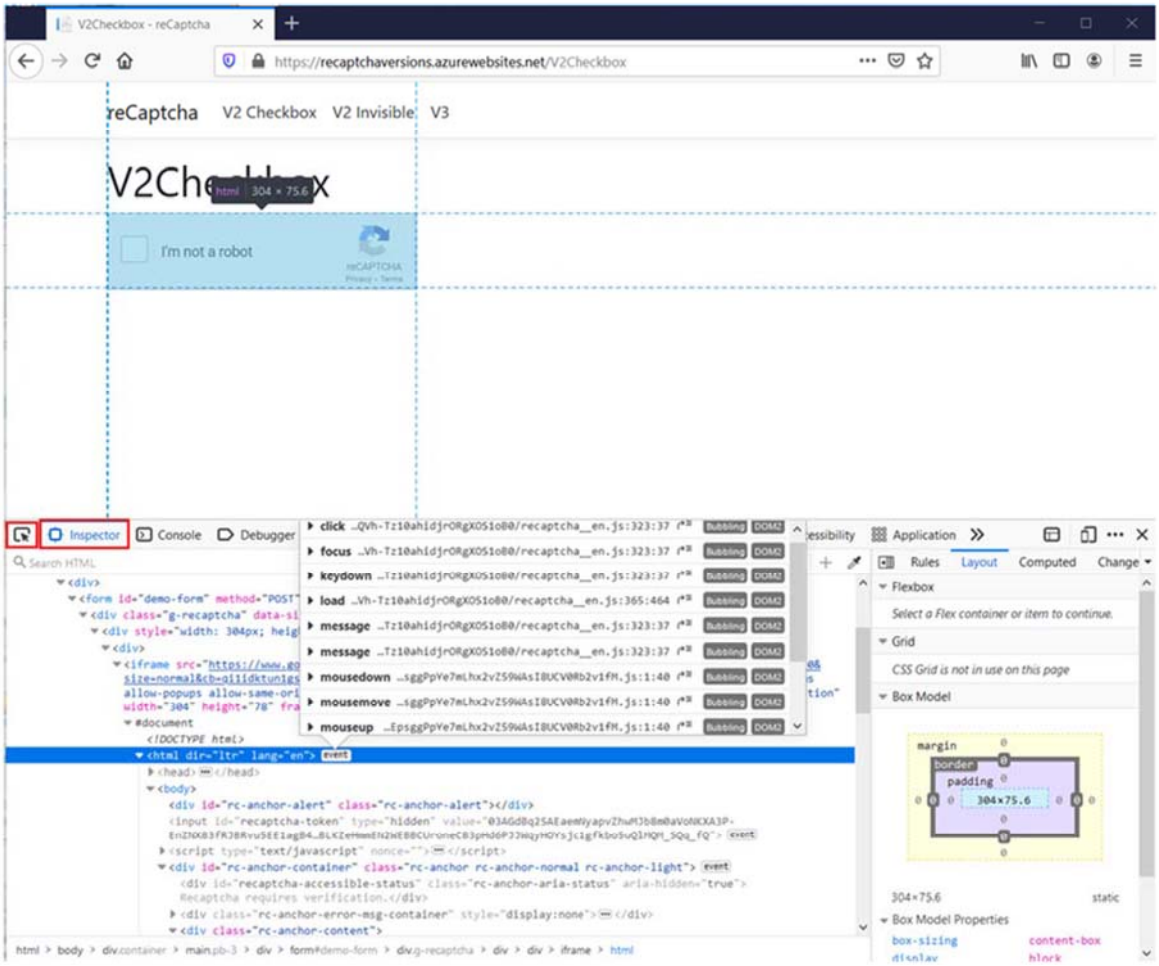
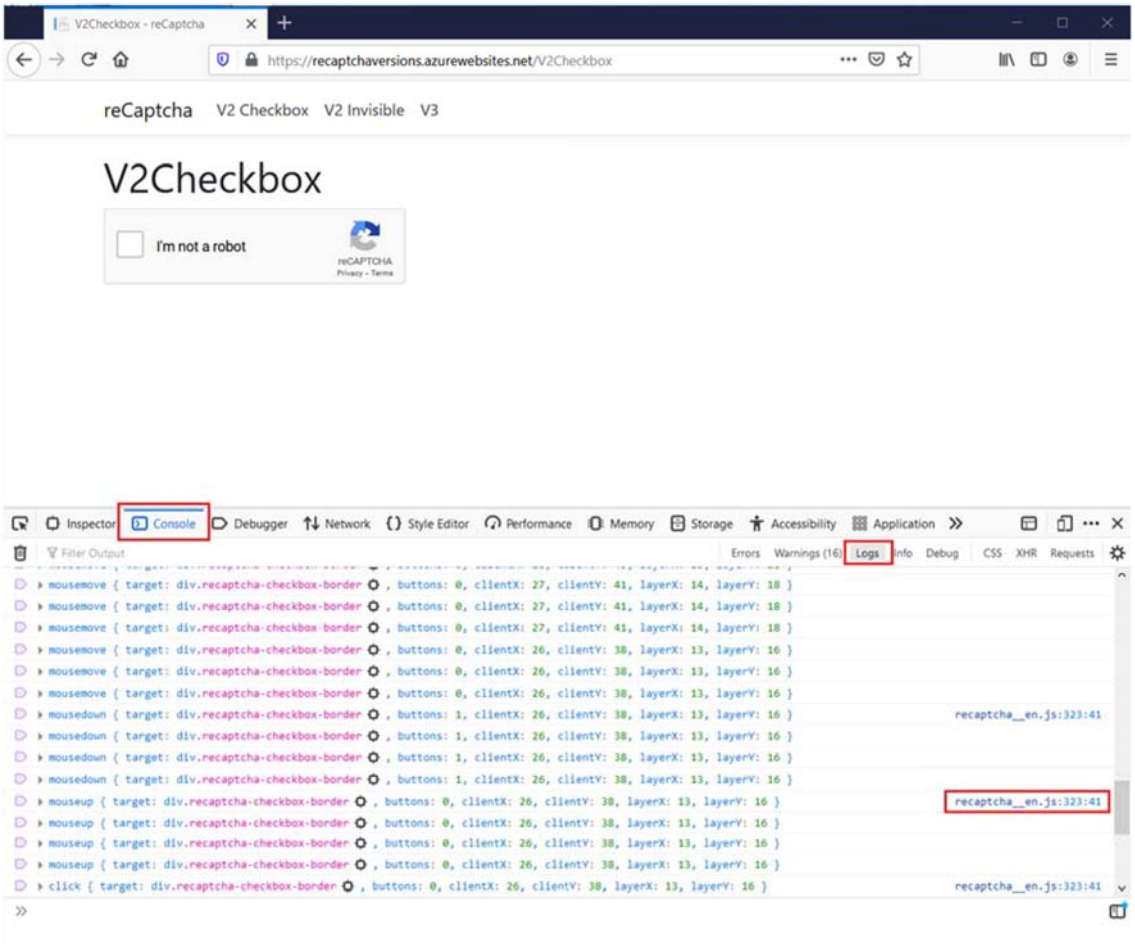

V2Checkbox - reCaptcha
https://recaptchaversions.azurewebsites.net/V2Checkbox
reCaptcha
V2 Checkbox
V2 Invisible
V3
I'm not a robot
Inspector
Console
Debugger
Application
Rules
Layout
Computed
Change
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
padding
304×75.6
Box Model Properties

**Figure 10**



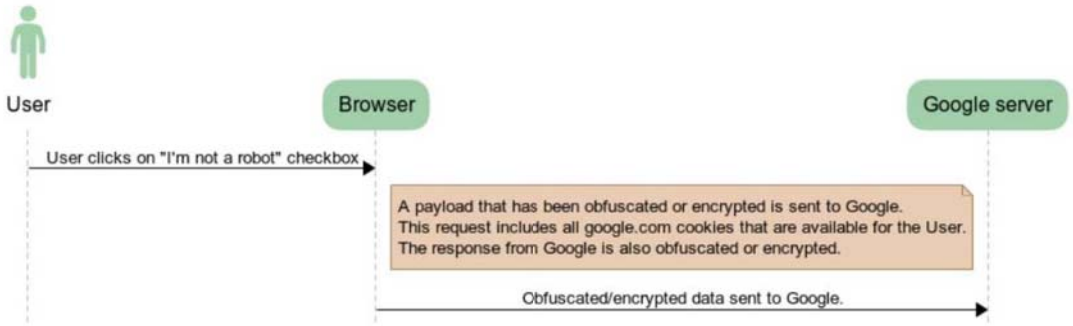

56. Google has also made various statements indicating that it engages in monitoring with "event listeners." For instance, Vinay Shet, the former Google Product Manager of reCAPTCHA, told Wired.com that "the tiny mouse movement a user's mouse makes as it hovers and approaches a checkbox can help reveal an automated bot."[19]

57. Each of the accused reCAPTCHA methods compares the monitored data to model data relating to human interaction with the issued data or in response to the issued data. For example, as depicted in Figure 11 below, a payload generated by the JavaScript event listeners is

[19] *See* Andy Greenberg, *Google Can Now Tell You're Not a Robot with Just One Click*, Wired (Dec. 3, 2014), https://wired.com/2014/12/google-one-click-recaptcha.

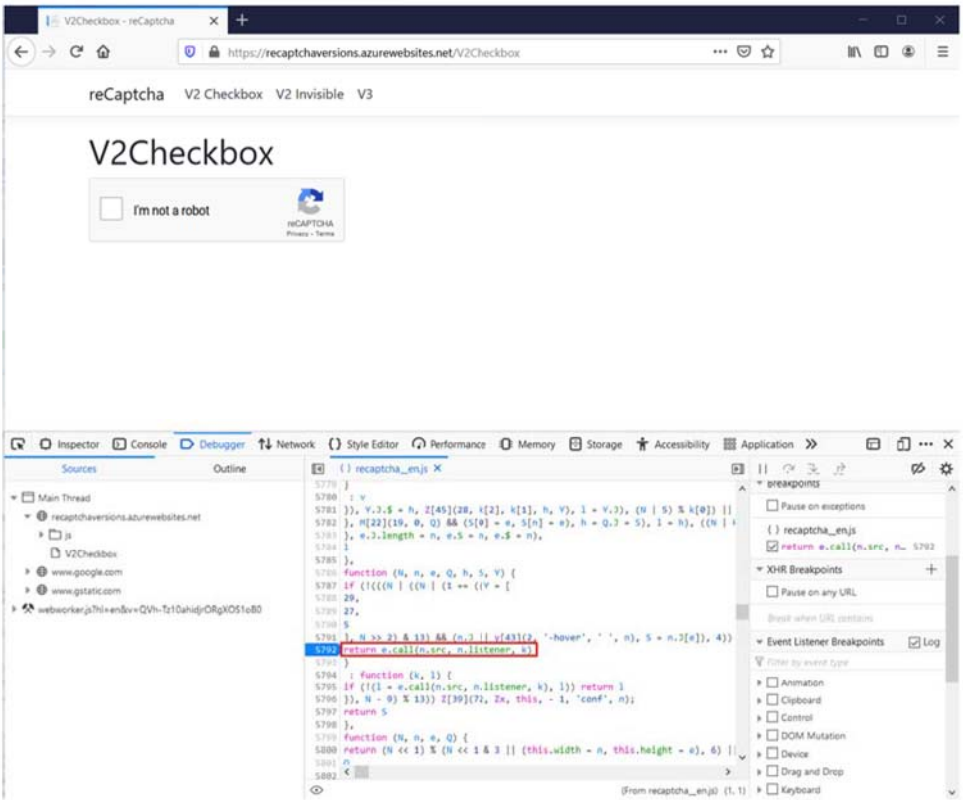
transmitted to Google, which applies the data in the payload to the reCAPTCHA algorithm that compares such data to model data relating to human interactions in order to determine whether the user is to be treated as a human or bot.

**Figure 11**



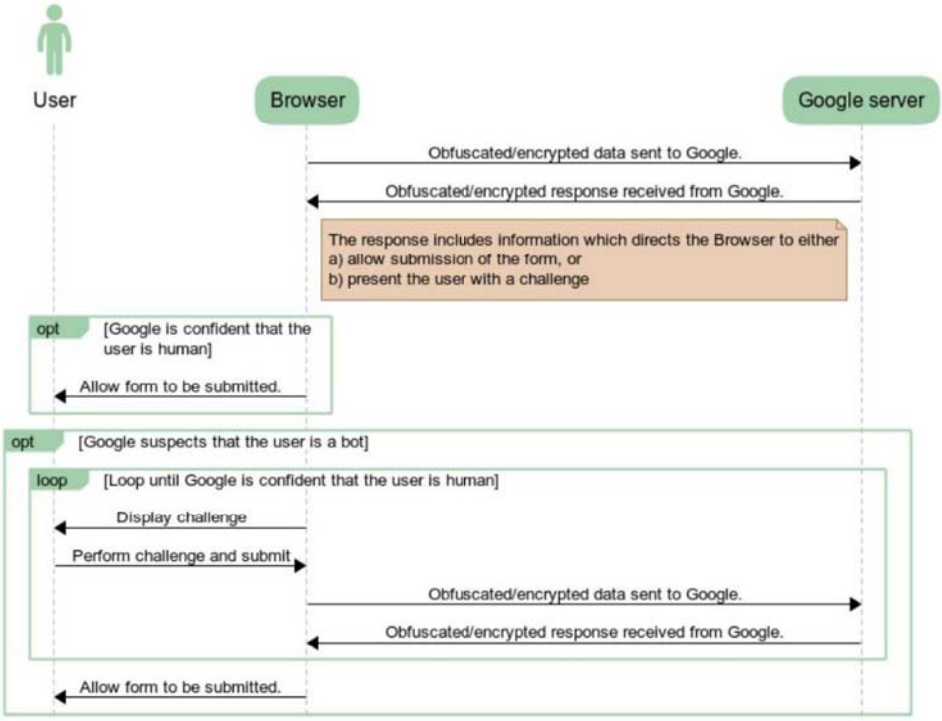

58. Figure 12 below shows that in the context of the reCAPTCHA v2 Checkbox version, the "recaptcha_en.js" code is utilized when the event handler calls Google's function.

**Figure 12**



59. For example, when the user clicks on the checkbox, a POST request with an obfuscated payload that contains the event listener data depicted above in Figures 9 and 10 is transmitted to Google, which uses this data to determine whether it believes the user is a human. This process is depicted in Figure 13 below.

**Figure 13**




60. Further, the data is used by Google's risk-analysis engine to evaluate whether the user is a human or potentially a bot by comparing the monitored data to model data. If it is potentially a bot, Google may issue additional challenges, as depicted in Figure 14 below.

**Figure 14**

However, CAPTCHAs aren't going away just yet. In cases when the risk analysis engine can't confidently predict whether a user is a human or an abusive agent, it will prompt a CAPTCHA to elicit more cues, increasing the number of security checkpoints to confirm the user is valid.


**Source:** Vinay Shet, *Are You a Robot? Introducing "No CAPTCHA reCAPTCHA,"* Google Security Blog (Dec. 3, 2014), https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html.

61. Google's comparison of monitored to model data is further demonstrated by Google's websites, screenshots of which are contained in Figures 15 and 16 below, and which reflect that Google uses prior interactions with a website as part of its analysis:

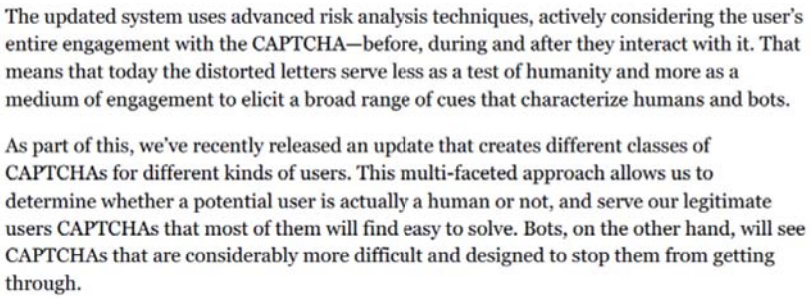
**Figure 15**

Placement on your website

reCAPTCHA v3 will never interrupt your users, so you can run it whenever you like without affecting conversion. reCAPTCHA works best when it has the most context about interactions with your site, which comes from seeing both legitimate and abusive behavior. For this reason, we recommend including reCAPTCHA verification on forms or actions as well as in the background of pages for analytics.

**Source**: *reCAPTCHA v.3*, reCAPTCHA, https://developers.google.com/recaptcha/docs/v3 (last visited Nov. 5, 2021).

**Figure 16**



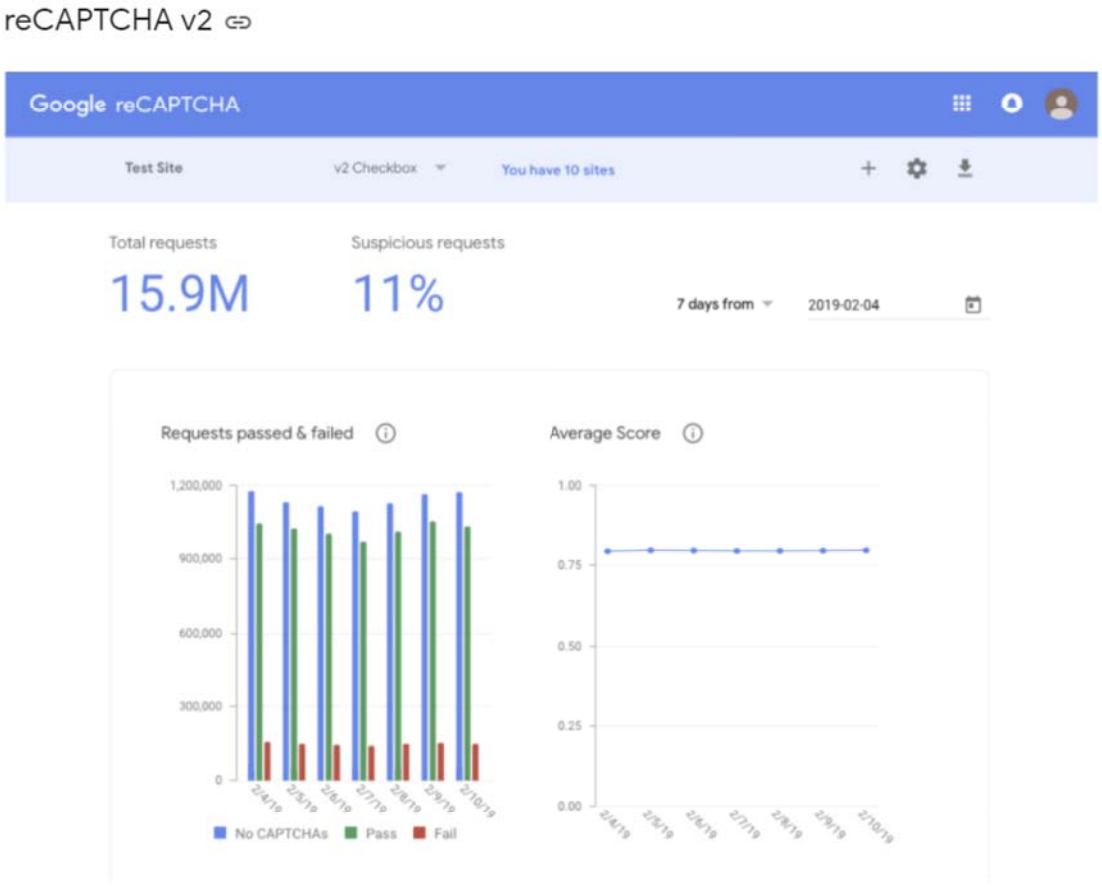
The updated system uses advanced risk analysis techniques, actively considering the user's entire engagement with the CAPTCHA—before, during and after they interact with it. That means that today the distorted letters serve less as a test of humanity and more as a medium of engagement to elicit a broad range of cues that characterize humans and bots.

As part of this, we've recently released an update that creates different classes of CAPTCHAs for different kinds of users. This multi-faceted approach allows us to determine whether a potential user is actually a human or not, and serve our legitimate users CAPTCHAs that most of them will find easy to solve. Bots, on the other hand, will see CAPTCHAs that are considerably more difficult and designed to stop them from getting through.

**Source**: Vinay Shet, *reCAPTCHA Just Got Easier (But only if You're Human)*, Google Security Blog (Oct. 25, 2013), https://security.googleblog.com/2013/10/recaptcha-just-got-easier-but-only-if.html.

62. Each of the accused reCAPTCHA methods generates a value representing a confidence level that the monitored data is the result of human interaction on the client computing device, rather than that of an autonomic user, with the issued data or in response to the issued data. For example, in the reCAPTCHA v2 methods, one or more Google servers input the monitored data into the reCAPTCHA algorithm (which Google terms its "risk analysis engine"). The algorithm then outputs a value between 0.0 and 1.0, with 0.0 indicating that Google believes the user is a bot and 1.0 indicating that Google believes the user is a human. Additional challenges may be issued if Google is not confident. Sample results are depicted in Figure 17 below.

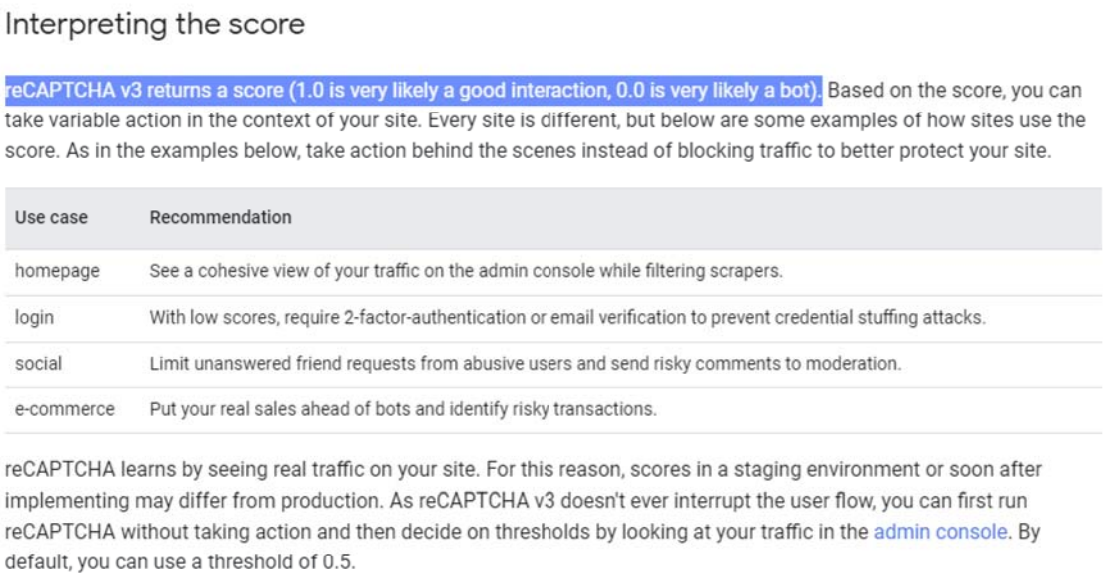
**Figure 17**




**Source**: *Analytics*, reCAPTCHA, https://developers.google.com/recaptcha/docs/analytics (last visited Dec. 6, 2021).

63. In the reCAPTCHA v3 version, a value between 0.0 and 1.0 also is returned, with a 0.0 signifying that Google is confident that the user is a bot and a 1.0 signifying that Google is confident that the user is a human, as explained in Figure 18 below. In the event that Google is not confident, additional challenges – such as two-factor authentication or email verification – may be issued. Sample results are depicted in Figure 19 below.

**Figure 18**



Interpreting the score

reCAPTCHA v3 returns a score (1.0 is very likely a good interaction, 0.0 is very likely a bot). Based on the score, you can take variable action in the context of your site. Every site is different, but below are some examples of how sites use the score. As in the examples below, take action behind the scenes instead of blocking traffic to better protect your site.

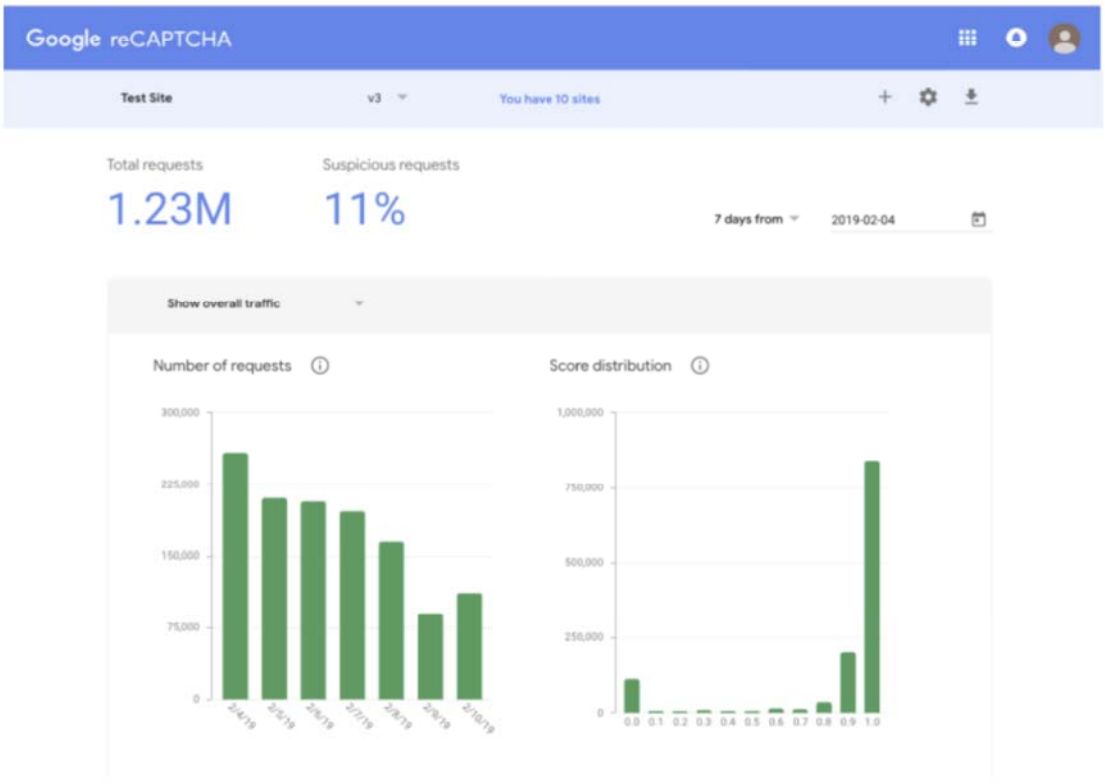
| Use case | Recommendation |
|---|---|
| homepage | See a cohesive view of your traffic on the admin console while filtering scrapers. |
| login | With low scores, require 2-factor-authentication or email verification to prevent credential stuffing attacks. |
| social | Limit unanswered friend requests from abusive users and send risky comments to moderation. |
| e-commerce | Put your real sales ahead of bots and identify risky transactions. |

reCAPTCHA learns by seeing real traffic on your site. For this reason, scores in a staging environment or soon after implementing may differ from production. As reCAPTCHA v3 doesn't ever interrupt the user flow, you can first run reCAPTCHA without taking action and then decide on thresholds by looking at your traffic in the admin console. By default, you can use a threshold of 0.5.

**Source**: *reCAPTCHA v.3*, reCAPTCHA, https://developers.google.com/recaptcha/docs/v3 (last visited Nov. 5, 2021).

**Figure 19**

reCAPTCHA v3




**Source**: *Analytics*, reCAPTCHA, https://developers.google.com/recaptcha/docs/analytics (last visited Dec. 6, 2021).

64. Google makes, distributes, uses, imports, offers for sale, and/or sells utilities and products, such as reCAPTCHA v2 Checkbox, reCAPTCHA v2 Invisible, reCAPTCHA v3, and reCAPTCHA Enterprise, that infringe at least Claim 1 of the '008 Patent.

65. Google has sold, and continues to sell and offer for sale, these utilities in the United States, through Google websites (https://cloud.google.com/recaptcha-enterprise), including to companies throughout the State of Texas and this District.[20]

[20] *See, e.g.*, *Honor Code Reporting Form*, Baylor Univ., https://cm.maxient.com/reportingform.php?BaylorUniv&layout_id=5 (last visited Nov. 5, 2021) (reflecting that the page is protected by reCAPTCHA v2 Invisible, one of the infringing methods of reCAPTCHA).

66. Google committed and is committing the foregoing infringing activities without license from Nobots. Google's acts of infringement have damaged Nobots, as owner and assignee of the '008 Patent. Nobots is entitled to recover from Google the damages it has sustained as a result of Google's wrongful acts in an amount subject to proof at trial. Google's infringement of Nobots's rights under the '008 Patent is ongoing and will continue to damage Nobots.

67. Beginning no later than the filing of this Complaint, Google has had actual knowledge of the '008 Patent. Google's continued infringement following the filing of this Complaint, despite its knowledge of the '008 Patent and Nobots's infringement allegations, is intentional and deliberate and willful.

68. In addition, Google indirectly infringed, and continues to indirectly infringe, the '008 Patent by actively inducing its infringement in violation 35 U.S.C. § 271(b).

69. Entities, consumers, and businesses who use Google's reCAPTCHA services directly infringe the '008 Patent by using the accused Google reCAPTCHA methods.

70. Google knowingly induced and induces these acts of infringement with the specific intent to encourage them by taking active steps to encourage and facilitate direct infringement by these third parties, in this District and elsewhere in the United States, through its design, construction, and sale of the infringing products, and through its creation and dissemination of promotional and marketing materials, supporting materials, instructions, and/or technical information relating to the reCAPTCHA methods with knowledge and the specific intent that its efforts will result in the direct infringement of the '008 Patent by these third parties.

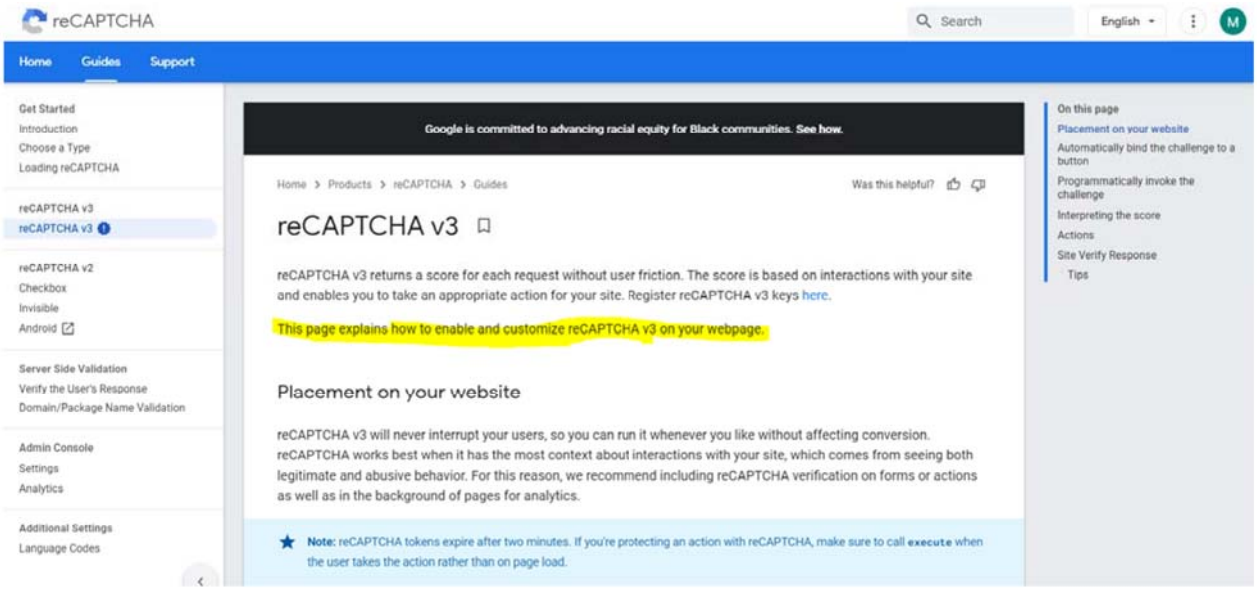
71. Such active steps include, for example, advertising and marketing the infringing utilities to entities, consumers, and businesses[21] and selling such utilities to consumers knowing

[21] *See, e.g.*, Google Cloud, Top 10 Use Cases for reCAPTCHA Enterprise to Defend

that they would be used in the United States.

72. Google user guides for the accused reCAPTCHA methods likewise facilitate infringement, instructing consumers about, among other things, how to "start using reCAPTCHA."[22] By instructing third parties how use the accused utilities for infringing purposes, such as to limit website access using the infringing methods, Google knowingly induces these third parties to commit infringing acts.

**Figure 20**




**Source**: *reCAPTCHA v.3*, reCAPTCHA, https://developers.google.com/recaptcha/docs/v3 (last visited Nov. 5, 2021).

73. In addition, Google has indirectly infringed and continues to indirectly infringe the '008 Patent as a contributory infringer in violation of 35 U.S.C. § 271(c) by selling or offering to

---

Against OWASP Web-Automated Attacks, *available* at https://services.google.com/fh/files/misc/owasp_handbook_again.pdf; *reCAPTCHA Enterprise*, Google Cloud, https://cloud.google.com/recaptcha-enterprise (last visited Nov. 7, 2021); *What Is reCAPTCHA?*, reCAPTCHA, https://developers.google.com/recaptcha (last visited Nov. 7, 2021).

[22] *Developer's Guide*, reCAPTCHA, https://developers.google.com/recaptcha/intro (last visited Nov. 7, 2021).

sell in the United States, or importing into the United States, infringing methods with knowledge that they are especially designed or adapted to operate in a manner that infringes the '008 Patent and despite the fact that the infringing technology is not a staple article of commerce suitable for substantial non-infringing use. Google knowingly incorporates methodology for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than a bot into the accused Google reCAPTCHA methods such that they operate in an infringing manner. By incorporating such methodology into its reCAPTCHA methods, Google contributes to infringing use as consumers grant or deny access to their servers using the confidence levels generated by the accused utilities, which lack substantially noninfringing uses because the accused reCAPTCHA methods are designed and constructed to operate in a manner that infringes the '008 Patent.

74. Google's acts of infringement have caused damage to Nobots, and Nobots is entitled to recover from Google (or any successor entity to Google) the damages sustained by Nobots as a result of Google's wrongful acts in an amount subject to proof at trial.

## COUNT TWO
## INFRINGEMENT OF U.S. PATENT NO. 10,423,885

75. Plaintiff repeats and incorporates by reference each preceding paragraph as if fully set forth herein and further states:

76. Google has infringed and continues to infringe at least Claim 1 of the '885 Patent in violation of 35 U.S.C. § 271, either literally or through the doctrine of equivalents, by making, using, selling, or offering for sale in the United States, and/or importing into the United States, without authorization, utilities that practice at least Claim 1 of the '885 Patent. Google is liable for its infringement of the '885 Patent pursuant to 35 U.S.C. § 271(a), (b), and (c).

77. More specifically, Google designs, constructs, imports, offers for sale, and/or sells

CAPTCHA security methods that test for a presence of biometric data with an operator of a client computing device attempting to access a server and controls access to the server by denying access when the biometric data is not present and/or not denying access when some biometric data is present.

78. Claim 1 is illustrative of the '885 Patent. It recites "[a] method comprising:

a) testing for a presence of biometric data associated with an operator of a computing device attempting to access a server;

b) controlling access to the server by at least one of:

i. denying access of the computing device attempting to access the server when the biometric data is not present; or

ii. not denying access of the computing device attempting to access the server when some biometric data is present."

79. Each of the accused reCAPTCHA methods meets every element of this claim.[23] Each of the accused reCAPTCHA methods requires testing for a presence of biometric data associated with an operator of a computing device attempting to access the server. For example, and discussed previously and depicted in Figures 8-10 above, the "reCAPTCHA_en.js" JavaScript code sent from the Google servers to the user adds "event listeners" to monitor and track keyboard, mouse, touch, scroll, and resize events. This tests for a presence of biometric data associated with an operator of a computing device attempting to access the server and provides Google with biometric data.

80. Each of the accused reCAPTCHA methods controls access to the server by denying access of the computing device attempting to access the server when the biometric data is not

[23] This description of infringement is illustrative and not intended to be an exhaustive or limiting explanation of every manner in which Google's products infringe the '885 Patent.

present. For example, the above-identified biometric data comprise some of the data used by Google's reCAPTCHA algorithm. As discussed previously and depicted in Figures 11, 13, and 15-19 above, for all of the reCAPTCHA v2 and v3 versions, Google's servers input the collected biometric data into its reCAPTCHA algorithm (which Google refers to as its "risk analysis engine"), and the algorithm then outputs a value between 0.0 and 1.0, with 0.0 indicating that Google believes the user is a bot and 1.0 indicating that Google believes the user is a human. Additional challenges may be issued if Google is not confident. The lack of the desired biometric data results in a low score, which can lead to a denial of access.

81. The accused reCAPTCHA methods also control access to the server by not denying access of the computing device attempting to access the server when some biometric data is present. That is, the presence of the desired biometric data results in a high score from the algorithm and allows access.

82. Google makes, distributes, uses, imports, offers for sale, and/or sells utilities and products, such as reCAPTCHA v2 Checkbox, reCAPTCHA v2 Invisible, reCAPTCHA v3, and reCAPTCHA Enterprise, that infringe at least Claim 1 of the '885 Patent.

83. Google has sold, and continues to sell and offer for sale, these utilities in the United States, including through Google websites (https://cloud.google.com/recaptcha-enterprise), to companies throughout the State of Texas and in this District.[24]

84. Google committed and is committing the foregoing infringing activities without license from Nobots. Google's acts of infringement have damaged Nobots, as owner and assignee of the '885 Patent. Nobots is entitled to recover from Google the damages it has sustained as a

[24] *See, e.g., Honor Code Reporting Form*, Baylor Univ., https://cm.maxient.com/reportingform.php?BaylorUniv&layout_id=5 (last visited Nov. 5, 2021) (reflecting that the page is protected by reCAPTCHA v2 Invisible, one of the infringing methods of reCAPTCHA).

result of Google's wrongful acts in an amount subject to proof at trial. Google's infringement of Nobots's rights under the '885 Patent is ongoing and will continue to damage Nobots.

85. Beginning no later than the filing of this Complaint, Google has had actual knowledge of the '885 Patent. Google's continued infringement following the filing of this Complaint, despite its knowledge of the '885 Patent and Nobots's infringement allegations, is intentional and deliberate and willful.

86. In addition, Google indirectly infringed, and continues to indirectly infringe, the '885 Patent by actively inducing its infringement in violation 35 U.S.C. § 271(b).

87. Entities, consumers, and businesses who use Google's reCAPTCHA services directly infringe the '885 Patent by using the accused Google reCAPTCHA methods.

88. Google knowingly induced and induces these acts of infringement with the specific intent to encourage them by taking active steps to encourage and facilitate direct infringement by these third parties, in this District and elsewhere in the United States, through its design, construction, and sale of the infringing products, and through its creation and dissemination of promotional and marketing materials, supporting materials, instructions, and/or technical information relating to the reCAPTCHA methods with knowledge and the specific intent that its efforts will result in the direct infringement of the '885 Patent by these third parties.

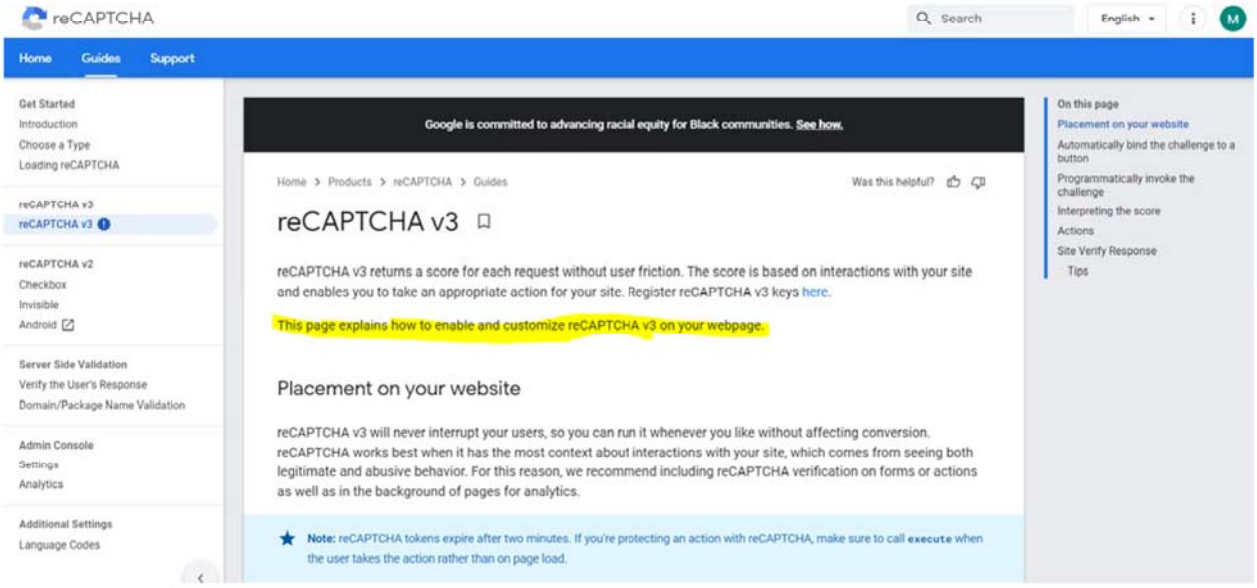
89. Such active steps include, for example, advertising and marketing the infringing utilities to entities, consumers, and businesses[25] and selling such utilities to consumers knowing and intending that they would be used in the United States.

---

[25] *See, e.g.*, Google Cloud, Top 10 Use Cases for reCAPTCHA Enterprise to Defend Against OWASP Web-Automated Attacks, *available* at https://services.google.com/fh/files/misc/owasp_handbook_again.pdf; *reCAPTCHA Enterprise*, Google Cloud, https://cloud.google.com/recaptcha-enterprise (last visited Nov. 7, 2021); *What Is reCAPTCHA?*, reCAPTCHA, https://developers.google.com/recaptcha (last visited Nov. 7, 2021).

90. Google user guides for the accused reCAPTCHA methods likewise facilitate infringement, instructing consumers about, among other things, how to "start using reCAPTCHA."[26] By instructing third parties how use the accused utilities for infringing purposes, such as to limit website access using the infringing methods, Google knowingly induces these third parties to commit infringing acts:

**Figure 21**




**Source**: *reCAPTCHA v.3*, reCAPTCHA, https://developers.google.com/recaptcha/docs/v3 (last visited Nov. 5, 2021).

91. In addition, Google has indirectly infringed and continues to indirectly infringe the '885 Patent as a contributory infringer in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, infringing methods with knowledge that they are especially designed or adapted to operate in a manner that infringes the '885 Patent and despite the fact that the infringing technology is not a staple article of commerce suitable for

[26] *Developer's Guide*, reCAPTCHA, https://developers.google.com/recaptcha/intro (last visited Nov. 7, 2021).

substantial non-infringing use. Google knowingly incorporates methodology for assessing a confidence level that an operator of a client computing device interacting with a server is a human being rather than a bot based on biometric data into the accused Google reCAPTCHA methods such that they operate in an infringing manner. By incorporating such methodology into its reCAPTCHA methods, Google contributes to infringing use as consumers grant or deny access to their servers using the confidence levels generated by the accused utilities, which lack substantially non-infringing uses because the accused reCAPTCHA methods are designed and constructed to operate in a manner that infringes the '885 Patent.

92. Google's acts of infringement have caused damage to Nobots, and Nobots is entitled to recover from Google (or any successor entity to Google) the damages sustained by Nobots as a result of Google's wrongful acts in an amount subject to proof at trial.

## DEMAND FOR JURY TRIAL

93. Plaintiff Nobots hereby demands a jury trial for all issues so triable.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff Nobots LLC requests entry of judgment in its favor and against Defendant Google as follows:

A. Declaring that Google has infringed United States Patent No. 9,595,008;

B. Declaring that Google has infringed United States Patent No. 10,423,885;

C. Declaring that Google's infringement of United States Patent No. 9,595,008 has been willful and deliberate, at least from the filing of this Complaint;

D. Declaring that Google's infringement of United States Patent No. 10,423,885 has been willful and deliberate, at least from the filing of this Complaint;

E. Awarding damages to Plaintiff in an amount no less than a reasonable royalty for

Google's infringement of United States Patent No. 9,595,008 and United States Patent No. 10,423,885, together with treble damages for willful infringement, prejudgment and post-judgment interest, and costs, as permitted under 35 U.S.C. § 284;

F. Awarding attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law;

G. Ordering Google to pay supplemental damages to Nobots, including any ongoing royalties and interest, with an accounting, as needed; and

H. Awarding such other costs and further relief as the Court may deem just and proper.

Dated: December 10, 2021

Respectfully submitted,

/s/ *Charles L. Ainsworth*

Charles L. Ainsworth (Texas 00783521)
Robert Christopher Bunt (Texas 00787165)
PARKER, BUNT & AINSWORTH, P.C.
100 East Ferguson, Suite 418
Tyler, Texas 75702
Tel: (903) 531-3535
Email: charley@pbatyler.com
Email: rcbunt@pbatyler.com

Matthew R. Berry
Andres Healy
John E. Schiltz
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, WA 98101-3000
Tel: (206) 516-3880
Fax: (206) 516-3883
Email: mberry@susmangodfrey.com
Email: ahealy@susmangodfrey.com
Email: jschiltz@susmangodfrey.com

Komal S. Patel
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor

New York, NY 10019
Phone: (212) 336-8330
Fax: (212) 336-8340
Email: kpatel@susmangodfrey.com

***Attorneys for Nobots LLC***

JS 44 (Rev. 10/20)

# CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

**I. (a) PLAINTIFFS**

NOBOTS LLC

**(b)** County of Residence of First Listed Plaintiff _____
*(EXCEPT IN U.S. PLAINTIFF CASES)*

**(c)** Attorneys *(Firm Name, Address, and Telephone Number)*
Charles Ainsworth, Parker Bunt & Ainsworth, PC
100 E. Ferguson, Ste. 418, Tyler ,TX 75702.
903-531-3535

**DEFENDANTS**

GOOGLE LLC

County of Residence of First Listed Defendant _____
*(IN U.S. PLAINTIFF CASES ONLY)*
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

**II. BASIS OF JURISDICTION** *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

**III. CITIZENSHIP OF PRINCIPAL PARTIES** *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
*(For Diversity Cases Only)*

| | PTF | DEF | | PTF | DEF |
|---|---|---|---|---|---|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated *or* Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated *and* Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

**IV. NATURE OF SUIT** *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

**CONTRACT**
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

**REAL PROPERTY**
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

**TORTS**

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

**CIVIL RIGHTS**
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

**PRISONER PETITIONS**

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

**FORFEITURE/PENALTY**
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

**LABOR**
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

**IMMIGRATION**
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

**BANKRUPTCY**
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

**PROPERTY RIGHTS**
- ☐ 820 Copyrights
- ☒ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

**SOCIAL SECURITY**
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

**FEDERAL TAX SUITS**
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

**OTHER STATUTES**
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

**V. ORIGIN** *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
35 U.S.C. § 271

Brief description of cause:
Patent Infringement

**VII. REQUESTED IN COMPLAINT:**

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

**DEMAND $**

CHECK YES only if demanded in complaint:
**JURY DEMAND:** ☒ Yes ☐ No

**VIII. RELATED CASE(S) IF ANY** *(See instructions):*

JUDGE _____ DOCKET NUMBER _____

DATE
Dec 13, 2021

SIGNATURE OF ATTORNEY OF RECORD
Charles Ainsworth

Digitally signed by Charles Ainsworth
DN: cn=Charles Ainsworth, o=Parker Bunt & Ainsworth, ou, email=charley@pbatyler.com, c=US
Date: 2021.12.10 10:10:49 -06'00'

**FOR OFFICE USE ONLY**

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

# INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

**I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

**(b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

**(c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

**II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

**III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

**IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

**V. Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
**PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7.** Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

**VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

**VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

**VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.

# EXHIBIT A

US009595008B1

(12) **United States Patent**
**Heikell**

(10) **Patent No.: US 9,595,008 B1**
(45) **Date of Patent: Mar. 14, 2017**

(54) **SYSTEMS, METHODS, APPARATUS FOR EVALUATING STATUS OF COMPUTING DEVICE USER**

(76) Inventor: **Timothy P. Heikell**, Seattle, WA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 780 days.

(21) Appl. No.: **12/313,502**

(22) Filed: **Nov. 19, 2008**

**Related U.S. Application Data**

(60) Provisional application No. 61/003,743, filed on Nov. 19, 2007.

(51) **Int. Cl.**

| | |
|---|---|
| ***G06F 9/44*** | (2006.01) |
| ***G06F 7/02*** | (2006.01) |
| ***G06N 7/06*** | (2006.01) |
| ***G06N 7/00*** | (2006.01) |

(52) **U.S. Cl.**
CPC ..... ***G06N 7/005*** (2013.01)

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 8,694,244 | B2 * | 4/2014 | Schalk | G01C 21/26 340/995.12 |
| 8,700,259 | B2 * | 4/2014 | Schalk | G01C 21/3608 701/36 |
| 8,706,405 | B2 * | 4/2014 | Schalk | G01C 21/26 340/995.12 |
| 8,738,287 | B2 * | 5/2014 | Schalk | G01C 21/3608 340/995.12 |
| 8,775,235 | B2 * | 7/2014 | Hedley | G07B 15/06 705/13 |
| 8,775,236 | B2 * | 7/2014 | Hedley | G06Q 30/0283 340/928 |

(Continued)

OTHER PUBLICATIONS

A proactive risk-aware robotic sensor network for Critical Infrastructure Protection Jamieson McCausland; George Di Nardo; Rafael Falcon; Rami Abielmona; Voicu Groza; Emil Petriu 2013 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) Year: 2013 pp. 132-137.*

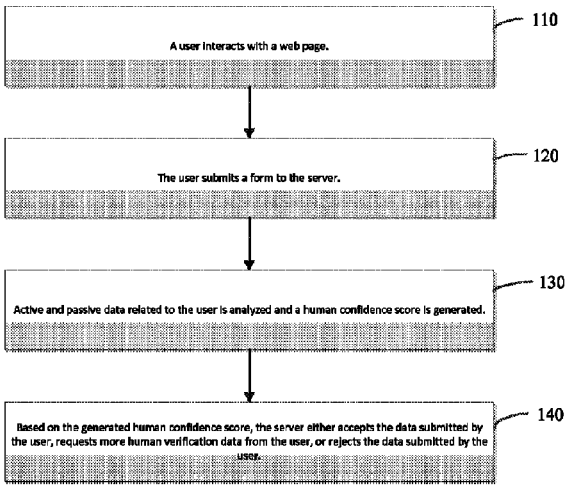
(Continued)

*Primary Examiner* — Michael B Holmes
(74) *Attorney, Agent, or Firm* — Lee & Hayes, PLLC; Bea Koempel-Thomas; Susan Moss

(57) **ABSTRACT**

Methods, systems and apparatus for assessing the likely user status of a client computing device interacting with a server where the computing device is in bi-directional operative communication with the server, wherein the likely user status is one of a human operator or a computer executable program such as a "bot". By presenting issued data from the server to the client computing device and monitoring at least some of the data generated at the client computing device in response to the issued data, a comparison can be made between the monitored data and model data relating to human interaction with or in response to the issued data. The results of the comparison can lead to a value that represents the likelihood that the monitored data results from human interaction with or in response to the issued data. Modeled data includes, but is not limited to, data indicative of human interaction with a computing environment, whether active or passive.

**20 Claims, 4 Drawing Sheets**



(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 8,824,659 | B2 * | 9/2014 | Bushey | G10L 19/0204 379/265.02 |
| 8,825,379 | B2 * | 9/2014 | Schalk | G01C 21/26 340/995.12 |
| 8,903,052 | B2 * | 12/2014 | Moore | H04M 3/493 379/72 |
| 9,088,652 | B2 * | 7/2015 | Bushey | G10L 19/0204 |
| 9,152,381 | B2 * | 10/2015 | Valentino | G06F 7/588 |
| 9,208,461 | B2 * | 12/2015 | Busa | G06Q 10/06 |
| 9,240,078 | B2 * | 1/2016 | Hedley | G07B 15/06 |
| 2008/0225870 | A1 * | 9/2008 | Sundstrom | 370/401 |

OTHER PUBLICATIONS

Trust Assessment from Observed Behavior: Toward and Essential Service for Trusted Network Computing P. Pal; F. Webber; M. Atighetchi; N. Combs Fifth IEEE International Symposium on Network Computing and Applications (NCA'06) Year: 2006 pp. 285-292, DOI: 10.1109/NCA.2006.53 IEEE Conference Publications.*

Testability modeling and analysis of a rocket engine test stand G. Temple; N. Jize; P. Wysocki 2005 IEEE Aerospace Conference Year: 2005 pp. 3874-3895, DOI: 10.1109/AERO.2005.1559694 IEEE Conference Publications.*

* cited by examiner

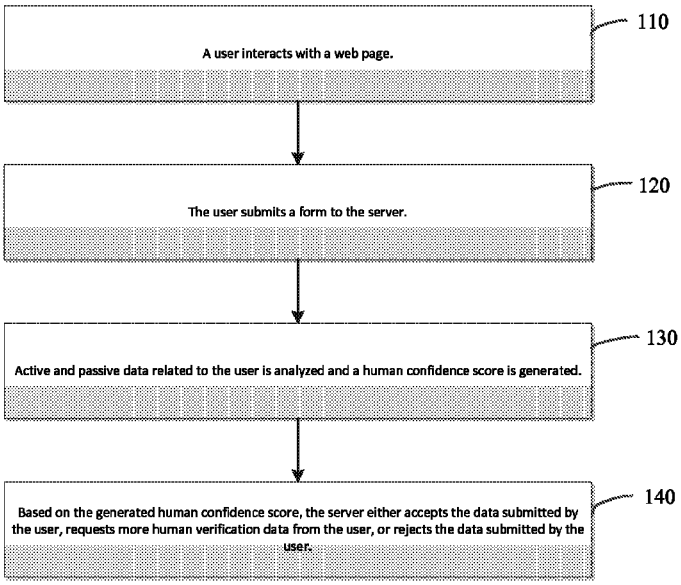

A user interacts with a web page.
110
The user submits a form to the server.
120
Active and passive data related to the user is analyzed and a human confidence score is generated.
130
Based on the generated human confidence score, the server either accepts the data submitted by the user, requests more human verification data from the user, or rejects the data submitted by the user.
140

Fig 1

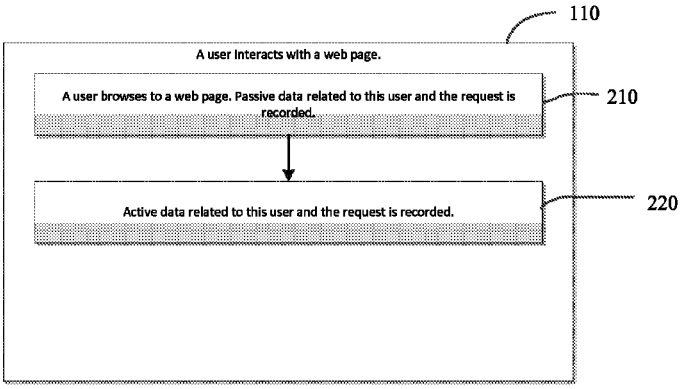

110
A user interacts with a web page.
A user browses to a web page. Passive data related to this user and the request is recorded.
210
Active data related to this user and the request is recorded.
220

Fig 2

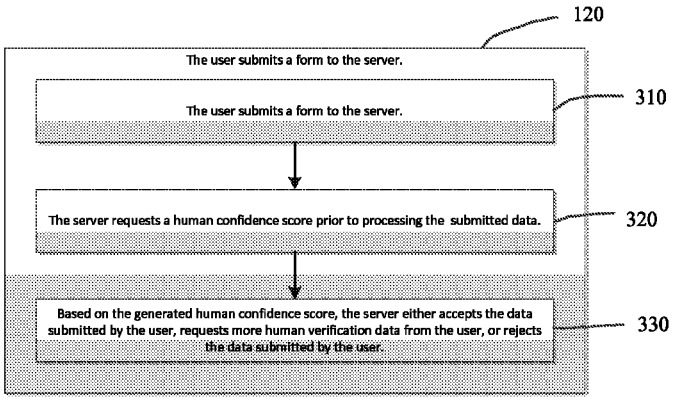

120
The user submits a form to the server.
The user submits a form to the server.
310
The server requests a human confidence score prior to processing the submitted data.
320
Based on the generated human confidence score, the server either accepts the data submitted by the user, requests more human verification data from the user, or rejects the data submitted by the user.
330

Fig 3

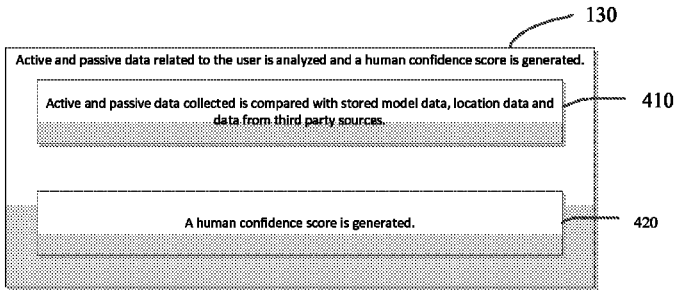

130
Active and passive data related to the user is analyzed and a human confidence score is generated.
Active and passive data collected is compared with stored model data, location data and data from third party sources.
410
A human confidence score is generated.
420

Fig 4

# SYSTEMS, METHODS, APPARATUS FOR EVALUATING STATUS OF COMPUTING DEVICE USER

## BACKGROUND

The Internet is a fantastic tool for constructive web sites to gather users for a common purpose; however, the Internet is also a fantastic tool for abuse of these same web sites. People who want to take advantage of websites do so by creating automated programs employing various algorithms and routines (hereinafter "bots") that create fictitious accounts or access content for a multitude of reasons.

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. However, as 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.

Carnegie Mellon University coined the term "CAPTCHA" (Completely Automated Public Turing test to tell Computers and Humans Apart) for these 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. 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.

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. While perhaps achieving the stated objective, the collateral effect is to exacerbate the existing burden to human users.

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, You Tube, 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.

A positive user experience is critical to the success and increased popularity of a given website. Designers of web sites go to great lengths to ensure their website is as user friendly as possible. 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. Reducing or eliminating the requirement of a user having to decipher CAPTCHA is one more way websites can create a more positive user experience for their visitors and minimize opportunity costs.



## SUMMARY OF THE INVENTION

The invention is generally directed to methods, systems and apparatus for assessing the likely user status of a computing device interacting with a server where computing device is in bi-directional operative communication with the server wherein the status is one of a human operator or a computer executable program (also referred to herein as a "bot"). This assessment comprises comparing acquired and/or available data relating to the operation of the computing device to suitable models embodying human user derived data (model data). In most embodiments, the comparison yields a probability value as to one of the status states **140**, **330**, which then may be used by a program or administrator of the server to permit or deny access and/or operation to the computing device. Because many of the invention embodiments provide a probability result as opposed to a binary result, the invention embodiments avoid the "there is only one right answer" phenomena inherent in prior art CAPTCHA tests. In other words, rather than placing the burden of proof on the user for functionality/access, which if the user is a human invokes the negative consequences of conventional CAPTCHA tests as previously described, the burden is shifted to the server side of the equation.

## BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description is described with reference to the accompanying figures. The use of the same reference numbers in different figures indicates similar or identical components or features.

FIG. **1** illustrates an overview of the process described in this disclosure.

FIG. **2** illustrates in more detail the first step **110** of FIG. **1** (a user interacts with a web page).

FIG. **3** illustrates in more detail the second step **120** of FIG. **1** (the user submits a form to the server).

FIG. **4** illustrates in more detail the third step **130** of FIG. **1** (active and passive data related to the user is analyzed and a human confidence score is generated).

## DETAILED DESCRIPTION OF THE INVENTION

As used herein, "model data", its equivalents and verb forms comprises data indicative of human interaction with a computing environment and that can be received by a computing device that is physically remote from the sample computing environment and equivalents. Model data comprises two main categories: active model data **220** and passive model data **210**. Active model data comprises data acquired from a computing device user's interactions therewith and within the computing environment where such data is not normally stored (logged) or transmitted to a remote location. Such model data includes, without limitation, pointing device vector movements and/or cadence, 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. 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.

Also as used herein, the term "available data", its equivalents and verb forms comprises data associated with a computing device's operation and its interaction with a computing environment, such as the Internet, that is generally recorded within the computing device and/or by other devices that have been affected by the computing device's operation—this is also a type of passive data; the term "acquired data", its equivalents and verb forms comprises data associated with a computing device's operation and its interaction with a computing environment, such as the Internet, that is generally not recorded within the computing device and/or by other devices that have been affected by the computing device's operation, but at least some data of which has/have been recorded and/or transmitted to a remote location, such as a server—this is a type of active data.

In addition to the foregoing, the term "issued data", its equivalents and verb forms comprises data generated by a server or other computing device that is not the same as the computing device for which the assessment as to user status is being performed; "monitored data", its equivalents and verb forms comprises active or passive data, whether available or acquired, obtained from the computing device, or as a result of its external interactions, after the generation of issued data; "interest data", its equivalents and verb forms comprises active or passive data, whether available or acquired, that correlates to any data within model data, whether obtained prior to or after the generation of issued data. Thus, interest data includes time independent available data and acquired data, unless qualified differently.

With the foregoing definitions in mind, operation of the various invention embodiments can be better understood. In a first series of embodiments, a comparison between interest data, acquired prior to delivery of issued data to the client computing device, and model data is performed to ascertain the likely status of the client computing device, i.e., human user or bot **130**, **420**. In a second series of embodiments, a comparison between monitored data, by definition acquired after delivery of issued data to the client computing device, and model data is performed to ascertain the likely status of the client computing device, i.e., human user or bot **130**, **420**. In both series of embodiments, acquired and/or available data may be used for comparison with suitable model data. The recited comparisons can take place locally on the computing device, remotely on the originating server, or on a server dedicated to performing such actions and for which subscriptions may be offered in conjunction with methods for providing services according to the methods, apparatus and systems embodiments described herein.

While available data represents data that is readily harvestable by query, for example, from the computing device or the computing environment in which the device operates, acquired data requires some form of information capture means. In the various embodiments described herein, the computing device is caused to monitor and retain certain data useful as acquired data for comparison purposes. 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**.

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, and/or merely retain the data until requested from, for example, the server, at which time some or all data may be transmitted **120**, **310**. As described above with reference to the comparison actions **130**, **410**, such receiving and/or polling actions can be carried out remotely on the originating server or on a server dedicated to performing such actions, if not performed locally on the computing device.

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. Moreover, the methods, and associated systems and apparatus, described herein are highly transparent to the user, thereby achieving an objective of enhancing the user's experience of a web site employing bot assessment protocols.

## DESCRIPTION OF AN INVENTION EMBODIMENT

A primary objective of bot creation is to autonomously access data and/or functionality of a target server as quickly as possible. By assessing user biometrics having a time domain, the time variable becomes a necessary component to accessing the data and/or functionality of the server. Because such assessment has heretofore been absent as a valid CAPTCHA marker of a human user, and more importantly because proper data input would necessarily slow the process, the likelihood of bot penetration has been significantly reduced.

An embodiment of the invention employs a first layer of testing that simply checks if there were valid mouse movements and/or key strokes inputted by the user of a computing device that is attempting to access a server resource "protected" from bots. This basic "if-then" check is essentially without overhead since there are no computations being carried out. Checking for the existence of the target activity therefore represents a first pass evaluation; if the bot is not programmed to include pseudo biometric data, further access is denied. In other words, if no activity is recorded there is a very high probability that the user is actually a bot.

A fundamental premise of robust biometrics is that a given dataset for each person is unique. Therefore, if the dataset is sufficiently robust, it is impossible to have dupli-

cative input data unless the input data was derived from a machine. Exploiting this premise allows a second level knockout assessment to deny user access if the input data exactly (or statistically sufficiently) matches previously recorded data. Of course, the skilled practitioner employing this method can select (either explicitly or via programming) sample points of a dataset for comparison as opposed to all data, thereby reducing computational overhead and storage issues. Alternatively, if samples are used, an exact match could then invoke a more intensive comparison with the same stored datasets, where again access can be denied when an exact or statistically sufficient match is found.

In the foregoing two assessments, an object has been to ferret out bots in an efficient and low overhead manner by exploiting intrinsic design limitations. However, it is possible that a bot designer could spoof these assessment means by, for example, running many bots in parallel wherein intrinsic delays in CPU processing and bandwidth would introduce inherent time delays associated with the very inputs being assessed. Therefore, more robust assessment means may be employed to ascertain the presence of a bot.

In robust embodiments of the invention, a third layer of testing may be employed that compares recorded pointer movements and key strokes to previously recorded activity for a given input page that was knowingly created by humans. Thus, as input data is collected for a given page, patterns will emerge that are unique to human activity. Subsequently recorded activity that is inconsistent with these patterns would indicate the potential that the user is a bot. Access could then be denied, or further CAPTCHA tests presented. Alternatively, access could be granted since no lock is pick proof and an object of the invention embodiments is to minimize user exposure to CAPTCHA tests.

What is claimed:

**1**. 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:

a) a single user of a client computing device requesting data from a server;

b) the server presenting data issued by the server to the client computing device;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**19**. 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:

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

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

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

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

* * * * *

# EXHIBIT B

US010423885B2

(12) **United States Patent**
**Heikell**

(10) **Patent No.: US 10,423,885 B2**
(45) **Date of Patent: *Sep. 24, 2019**

(54) **SYSTEMS, METHODS AND APPARATUS FOR EVALUATING STATUS OF COMPUTING DEVICE USER**

(71) Applicant: **Timothy P. Heikell**, Renton, WA (US)

(72) Inventor: **Timothy P. Heikell**, Renton, WA (US)

(73) Assignee: **Timothy P. Heikell**, Renton, WA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/457,099**

(22) Filed: **Mar. 13, 2017**

(65) **Prior Publication Data**

US 2018/0012138 A1 Jan. 11, 2018

**Related U.S. Application Data**

(63) Continuation of application No. 12/313,502, filed on Nov. 19, 2008, now Pat. No. 9,595,008.

(60) Provisional application No. 61/003,743, filed on Nov. 19, 2007.

(51) **Int. Cl.**

| | |
|---|---|
| ***G06N 7/00*** | (2006.01) |
| ***G06F 21/50*** | (2013.01) |
| ***G06F 21/31*** | (2013.01) |

(52) **U.S. Cl.**

CPC ..... ***G06N 7/005*** (2013.01); ***G06F 21/316*** (2013.01); ***G06F 21/50*** (2013.01); *G06F 2221/2133* (2013.01)

(58) **Field of Classification Search**

USPC ..... 706/52

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,933,498 | A * | 8/1999 | Schneck | G06F 21/10 705/54 |
| 6,460,141 | B1 * | 10/2002 | Olden | G06F 21/604 726/12 |
| 7,506,170 | B2 * | 3/2009 | Finnegan | G06F 21/31 713/162 |
| 8,694,244 | B2 | 4/2014 | Schalk | |
| 8,700,259 | B2 | 4/2014 | Schalk | |
| 8,706,405 | B2 | 4/2014 | Schalk | |

(Continued)

OTHER PUBLICATIONS

IEEE Combined Web/mobile authentication for secure Web access control A. Al-Qayedi; W. Adi; A. Zahro; A. Mabrouk Published in: 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733) Date of Conference: Mar. 21-25, 2004 IEEE.*

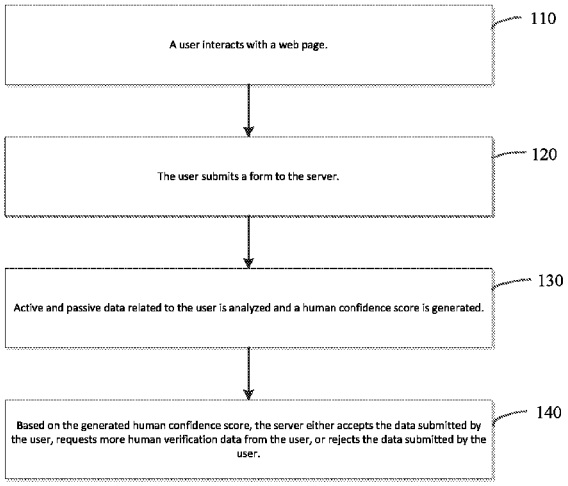
(Continued)

*Primary Examiner* — Michael B Holmes
(74) *Attorney, Agent, or Firm* — Lee & Hayes, P.C.

(57) **ABSTRACT**

Methods, systems and apparatus for assessing the likely status of an operator of a computing device interacting with a server as a human operator or an autonomic computer application, such as a "bot" are described herein. By monitoring at least some data, e.g., biometric data, generated at the client computing device, a comparison can be made between the monitored data and model data relating to human interaction with the computing device. The results of the comparison can lead to a value that represents the likelihood that the monitored data results from human interaction.

**20 Claims, 4 Drawing Sheets**



(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 8,713,657 | B2 * | 4/2014 | Lee | G06F 21/46 726/7 |
| 8,738,287 | B2 | 5/2014 | Schalk | |
| 8,775,235 | B2 | 7/2014 | Hedley et al. | |
| 8,775,236 | B2 | 7/2014 | Hedley et al. | |
| 8,824,659 | B2 | 9/2014 | Bushey et al. | |
| 8,825,379 | B2 | 9/2014 | Schalk | |
| 8,903,052 | B2 | 12/2014 | Moore et al. | |
| 9,047,458 | B2 * | 6/2015 | Etchegoyen | G06F 21/31 |
| 9,088,652 | B2 | 7/2015 | Bushey et al. | |
| 9,152,381 | B2 | 10/2015 | Valentino et al. | |
| 9,208,461 | B2 | 12/2015 | Busa | |
| 9,240,078 | B2 | 1/2016 | Hedley et al. | |
| 9,595,008 | B1 * | 3/2017 | Heikell | G06N 7/005 |
| 2008/0225870 | A1 | 9/2008 | Sundstrom | |
| 2009/0197815 | A1 | 8/2009 | Vincenzi et al. | |
| 2013/0019290 | A1 * | 1/2013 | Lee | G06F 21/46 726/6 |

OTHER PUBLICATIONS

McCausland et al., "A Proactice Risk-Awar Robitic Sensor Network for Critical Infrastructure Protection", IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), Apr. 2013, pp. 132-137.

Office action for U.S. Appl. No. 12/313,502, dated Sep. 16, 2011, Heikell, "Systems, Methods and Apparatus for Evaluating Status of Computing Device User", 9 pages.

Pal et al., "Trust Assessment from Observed Behavior: Toward and Essential Service for Trusted Network Computing", Fifth IEEE International Symposium on Network Computing and Applications (NCA'06), Jul. 2006, pp. 285-292.

Temple et al., "Testability Modeling and Analysis of a Rocket Engine Test Stand", IEEE Aerospace Conference, Jan. 2005, pp. 3874-3895.

"Fingerprint Reader: Replace Passwords with Your Fingerprint" retrieved on the internet on Aug. 16, 2018 at <<https://web.archive.org/web/20061230123302/http:://www.microsoft.com/hardware/houseandkeyboard/productdetails.aspxZpid=036>> 1 page.

"Microsoft Fingerprint Reader" retrieved from the internet on Aug. 16, 2018 at <<https//en.wikipedia.org/wikiMicrosoft_Fingerprint_Reader>>, 2 pages.

"Microsoft Fingerprint Reader" retrieved from the internet on Aug. 16, 2018 at <<https://web.archive.org/web/20060913000000/http://en.wikipedia.org:80/wikiMicrosoft_Fingerprint_Reader>> 1 page.

"Most people have at least 15 username and password combinations to remember" retrieved from the internet on Aug. 16, 2018 at <<https://web.archive.org/web/20050111041404/http://www.microsoft.com:80/hardware/mouseandkeyboard/features/docs/fingerprint.html>> 12 pages.

"Researcher Hacks Microsoft Fingerprint Reader" retrieved from the internet on Aug. 16, 2018 at <<https://www.pcworld.com/article/124978/article.html>> 3 pages.

"Tired of passwords? Replace them with your fingerprint" retrieved from the internet on Aug. 16, 2018 at <<https://web.archive.org/web/20040926002804/http://www.microsoft.com:80hardware;mouseandkeyboard/features/fingerprint.mspx>>, 1 page.

* cited by examiner

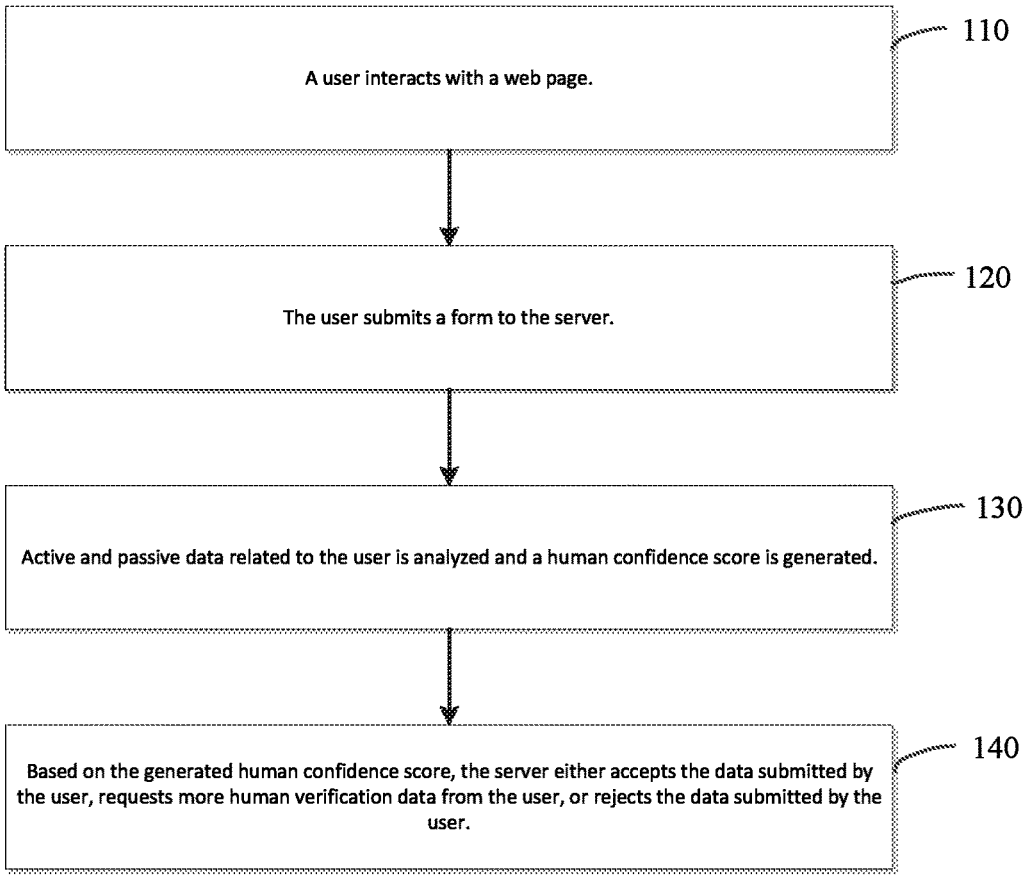

A user interacts with a web page.
110
The user submits a form to the server.
120
Active and passive data related to the user is analyzed and a human confidence score is generated.
130
Based on the generated human confidence score, the server either accepts the data submitted by the user, requests more human verification data from the user, or rejects the data submitted by the user.
140

Fig 1

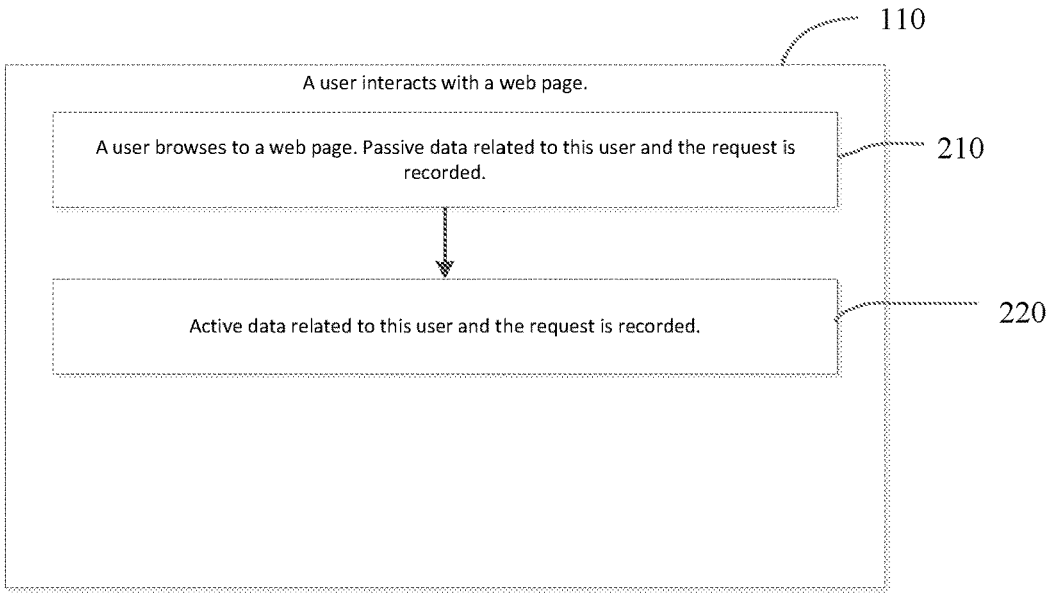

110
A user interacts with a web page.
A user browses to a web page. Passive data related to this user and the request is recorded.
210
Active data related to this user and the request is recorded.
220

Fig 2

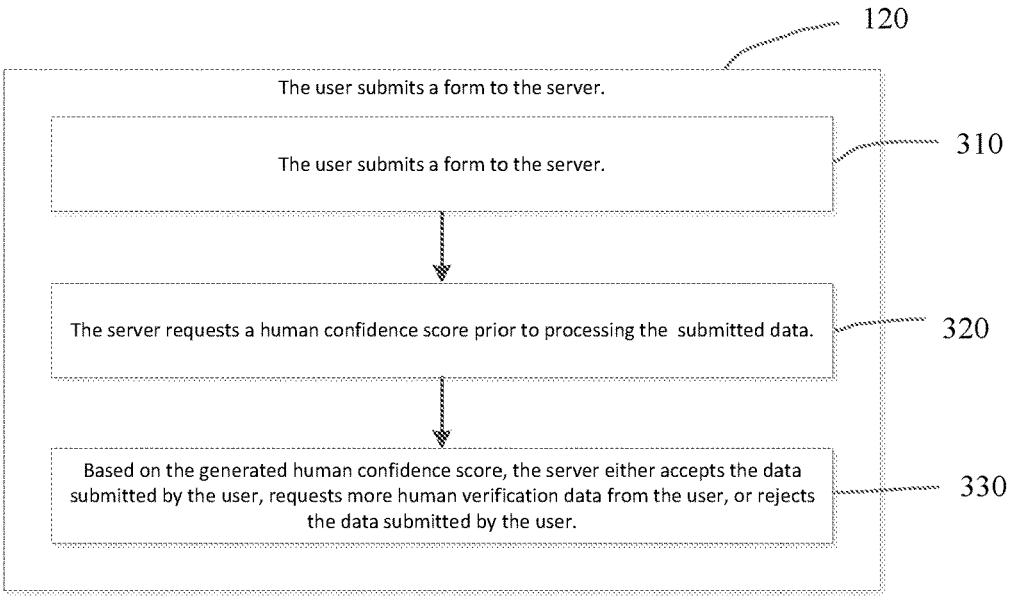

120
The user submits a form to the server.
The user submits a form to the server.
310
The server requests a human confidence score prior to processing the submitted data.
320
Based on the generated human confidence score, the server either accepts the data submitted by the user, requests more human verification data from the user, or rejects the data submitted by the user.
330

Fig 3

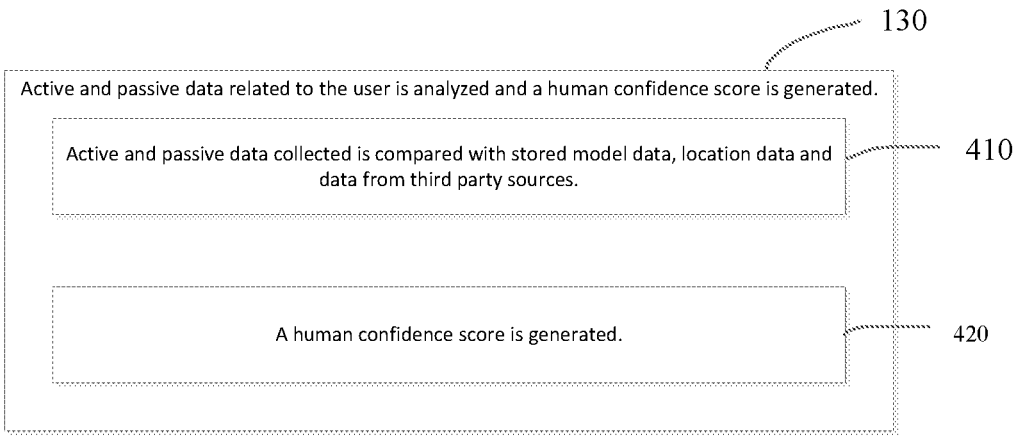

130
Active and passive data related to the user is analyzed and a human confidence score is generated.
Active and passive data collected is compared with stored model data, location data and data from third party sources.
410
A human confidence score is generated.
420

Fig 4

# SYSTEMS, METHODS AND APPARATUS FOR EVALUATING STATUS OF COMPUTING DEVICE USER

This application claims priority to application Ser. No. 12/313,502 filed Nov. 19, 2008, which claims priority to provisional application Ser. No. 61/003,743 filed Nov. 19, 2007, both of which are incorporated herein by reference.

## BACKGROUND

The Internet is a fantastic tool for constructive web sites to gather users for a common purpose; however, the Internet is also a fantastic tool for abuse of these same web sites. People who want to take advantage of websites do so by creating automated programs employing various algorithms and routines (hereinafter "bots") that create fictitious accounts or access content for a multitude of reasons.

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. However, as 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.

Carnegie Mellon University coined the term "CAPTCHA" (Completely Automated Public Turing test to tell Computers and Humans Apart) for these 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. 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.

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. While perhaps achieving the stated objective, the collateral effect is to exacerbate the existing burden to human users.

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, You Tube, 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.



A positive user experience is critical to the success and increased popularity of a given website. Designers of web sites go to great lengths to ensure their website is as user friendly as possible. 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. Reducing or eliminating the requirement of a user having to decipher CAPTCHA is one more way websites can create a more positive user experience for their visitors and minimize opportunity costs.

## SUMMARY OF THE INVENTION

The invention is generally directed to methods, systems and apparatus for assessing the likely user status of a computing device interacting with a server where computing device is in bi-directional operative communication with the server wherein the status is one of a human operator or a computer executable program (also referred to herein as a "bot"). This assessment comprises comparing acquired and/or available data relating to the operation of the computing device to suitable models embodying human user derived data (model data). In most embodiments, the comparison yields a probability value as to one of the status states **140**, **330**, which then may be used by a program or administrator of the server to permit or deny access and/or operation to the computing device. Because many of the invention embodiments provide a probability result as opposed to a binary result, the invention embodiments avoid the "there is only one right answer" phenomena inherent in prior art CAPTCHA tests. In other words, rather than placing the burden of proof on the user for functionality/access, which if the user is a human invokes the negative consequences of conventional CAPTCHA tests as previously described, the burden is shifted to the server side of the equation.

## BRIEF DESCRIPTION OF THE DRAWINGS

The detailed description is described with reference to the accompanying figures. The use of the same reference numbers in different figures indicates similar or identical components or features.

FIG. **1** illustrates an overview of the process described in this disclosure.

FIG. **2** illustrates in more detail the first step **110** of FIG. **1** (a user interacts with a web page).

FIG. **3** illustrates in more detail the second step **120** of FIG. **1** (the user submits a form to the server).

FIG. **4** illustrates in more detail the third step **130** of FIG. **1** (active and passive data related to the user is analyzed and a human confidence score is generated).

## DETAILED DESCRIPTION

As used herein, "model data", its equivalents and verb forms comprises data indicative of human interaction with a computing environment and that can be received by a computing device that is physically remote from the sample computing environment and equivalents. Model data comprises two main categories: active model data **220** and passive model data **210**. Active model data comprises data acquired from a computing device user's interactions therewith and within the computing environment where such data

is not normally stored (logged) or transmitted to a remote location. Such model data includes, without limitation, pointing device vector movements and/or cadence, 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. 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.

Also as used herein, the term "available data" its equivalents and verb forms comprises data associated with a computing device's operation and its interaction with a computing environment, such as the Internet, that is generally recorded within the computing device and/or by other devices that have been affected by the computing device's operation—this is also a type of passive data; the term "acquired data", its equivalents and verb forms comprises data associated with a computing device's operation and its interaction with a computing environment, such as the Internet, that is generally not recorded within the computing device and/or by other devices that have been affected by the computing device's operation, but at least some data of which has/have been recorded and/or transmitted to a remote location, such as a server—this is a type of active data.

In addition to the foregoing, the term "issued data", its equivalents and verb forms comprises data generated by a server or other computing device that is not the same as the computing device for which the assessment as to user status is being performed "monitored data", its equivalents and verb forms comprises active or passive data, whether available or acquired, obtained from the computing device, or as a result of its external interactions, after the generation of issued data "interest data", its equivalents and verb forms comprises active or passive data, whether available or acquired, that correlates to any data within model data, whether obtained prior to or after the generation of issued data. Thus, interest data includes time independent available data and acquired data, unless qualified differently.

With the foregoing definitions in mind, operation of the various invention embodiments can be better understood. In a first series of embodiments, a comparison between interest data, acquired prior to delivery of issued data to the client computing device, and model data is performed to ascertain the likely status of the client computing device, i.e., human user or bot **130**, **420**. In a second series of embodiments, a comparison between monitored data, by definition acquired after delivery of issued data to the client computing device, and model data is performed to ascertain the likely status of the client computing device, i.e., human user or bot **130**, **420**. In both series of embodiments, acquired and/or available data may be used for comparison with suitable model data. The recited comparisons can take place locally on the computing device, remotely on the originating server, or on a server dedicated to performing such actions and for which subscriptions may be offered in conjunction with methods for providing services according to the methods, apparatus and systems embodiments described herein.

While available data represents data that is readily harvestable by query, for example, from the computing device or the computing environment in which the device operates, acquired data requires some form of information capture means. In the various embodiments described herein, the computing device is caused to monitor and retain certain data useful as acquired data for comparison purposes. 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**.

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, and/or merely retain the data until requested from, for example, the server, at which time some or all data may be transmitted **120**, **310**. As described above with reference to the comparison actions **130**, **410**, such receiving and/or polling actions can be carried out remotely on the originating server or on a server dedicated to performing such actions, if not performed locally on the computing device.

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. Moreover, the methods, and associated systems and apparatus, described herein are highly transparent to the user, thereby achieving an objective of enhancing the user's experience of a web site employing bot assessment protocols.

## DESCRIPTION OF AN INVENTION EMBODIMENT

A primary objective of bot creation is to autonomously access data and/or functionality of a target server as quickly as possible. By assessing user biometrics having a time domain, the time variable becomes a necessary component to accessing the data and/or functionality of the server. Because such assessment has heretofore been absent as a valid CAPTCHA marker of a human user, and more importantly because proper data input would necessarily slow the process, the likelihood of bot penetration has been significantly reduced.

An embodiment of the invention employs a first layer of testing that simply checks if there were valid mouse movements and/or key strokes inputted by the user of a computing device that is attempting to access a server resource "protected" from bots. This basic "if-then" check is essentially without overhead since there are no computations being carried out. Checking for the existence of the target activity therefore represents a first pass evaluation; if the bot is not programmed to include pseudo biometric data, further

access is denied. In other words, if no activity is recorded there is a very high probability that the user is actually a bot.

A fundamental premise of robust biometrics is that a given dataset for each person is unique. Therefore, if the dataset is sufficiently robust, it is impossible to have duplicative input data unless the input data was derived from a machine. Exploiting this premise allows a second level knockout assessment to deny user access if the input data exactly (or statistically sufficiently) matches previously recorded data. Of course, the skilled practitioner employing this method can select (either explicitly or via programming) sample points of a dataset for comparison as opposed to all data, thereby reducing computational overhead and storage issues. Alternatively, if samples are used, an exact match could then invoke a more intensive comparison with the same stored datasets, where again access can be denied when an exact or statistically sufficient match is found.

In the foregoing two assessments, an object has been to ferret out bots in an efficient and low overhead manner by exploiting intrinsic design limitations. However, it is possible that a bot designer could spoof these assessment means by, for example, running many bots in parallel wherein intrinsic delays in CPU processing and bandwidth would introduce inherent time delays associated with the very inputs being assessed. Therefore, more robust assessment means may be employed to ascertain the presence of a bot.

In robust embodiments of the invention, a third layer of testing may be employed that compares recorded pointer movements and key strokes to previously recorded activity for a given input page that was knowingly created by humans. Thus, as input data is collected for a given page, patterns will emerge that are unique to human activity. Subsequently recorded activity that is inconsistent with these patterns would indicate the potential that the user is a bot. Access could then be denied, or further CAPTCHA tests presented. Alternatively, access could be granted since no lock is pick proof and an object of the invention embodiments is to minimize user exposure to CAPTCHA tests.

What is claimed:

**1**. A method comprising:

testing for a presence of biometric data associated with an operator of a computing device attempting to access a server;

controlling access to the server by at least one of:

denying access of the computing device attempting to access the server when the biometric data is not present; or

not denying access of the computing device attempting to access the server when some biometric data is present.

**2**. A method as claim **1** recites, wherein the biometric data includes at least one of mouse movement or keystrokes associated with the computing device.

**3**. A method as claim **1** recites, further comprising identifying whether the biometric data matches previously recorded biometric data.

**4**. A method as claim **3** 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 when the biometric data matches previously recorded biometric data.

**5**. A method as claim **3** recites, further comprising denying access of the computing device attempting to access the server when the biometric data matches previously recorded biometric data.

**6**. A method as claim **3** recites, further comprising:

identifying a pattern in input data corresponding to human interaction with the web page;

identifying that at least some of the biometric data is inconsistent with the pattern in the input data corresponding to the human interaction with the web page.

**7**. A method as claim **6** 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 when the at least some biometric data is inconsistent with the pattern of human interaction with the web page.

**8**. A method as claim **6** recites, further comprising denying access of the computing device attempting to access the server when the at least some biometric data is inconsistent with the pattern of human interaction with the web page.

**9**. A method as claim **1** recites, further comprising:

identifying that at least some of the biometric data matches previously recorded biometric data;

comparing a portion of the biometric data in addition to the at least some of the biometric data to the previously recorded biometric data; and

denying access to the computing device attempting to access the server when the at least some biometric data and the portion of the biometric data match previously recorded biometric data.

**10**. A method as claim **1** recites, further comprising:

identifying a pattern in input data corresponding to human interaction with the web page; and

identifying that at least some of the biometric data is inconsistent with the pattern in the input data corresponding to the human interaction with the web page.

**11**. A method as claim **10** 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 when the at least some biometric data is inconsistent with the pattern of human interaction with the web page.

**12**. A method as claim **10** recites, further comprising denying access of the computing device attempting to access the server when the at least some biometric data is inconsistent with the pattern of human interaction with the web page.

**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.

**14**. A method as claim **13** recites, wherein the model data comprises at least one of passive model data or active model data.

**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.

**16**. A method as claim **13** recites, further comprising granting access for delivery of issued data if the probability value indicates a greater likelihood that the operator of the computing device is a human.

**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.

**18**. A method as claim **13** recites, further comprising denying access to issued data from the server if the probability value indicates a greater likelihood that the operator of the computing device is an autonomic computer application.

**19**. A method as claim **13** recites, wherein the model data relating to human interaction with the computing device is recorded prior to a time in which the interest data is acquired.

**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.

* * * * *