

**UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
PATENT TRIAL AND APPEAL BOARD**

Rocket Media, LLC d/b/a Launch Labs,

Petitioner

v.

Fullthrottle Technologies, LLC,

Patent Owner

Case No.: 2025-00148

Patent No. 11,556,947

Declaration of Dr. Oded Gottesman

TABLE OF CONTENTS

Table of Contents	ii
Table of Exhibits	iv
1. Introduction & Qualifications.....	1
1.1. Summary of My Qualifications.....	2
1.1.1. Education, Employment, and Research	2
1.1.2. Publications	5
1.1.3 Prior Testimony.....	5
2. Summary of My Opinions	6
3. Materials Considered	6
4. Legal Standards	7
4.1. Obviousness.....	8
5. Technical Background: User Location Tracking via Browsers	11
5.1. Cookies	12
5.2. Privacy Concerns Lead to Limits on Cookies.....	14
5.3. Tracking Users in Browser Storage Using Cookies.....	16
5.4. Tracking Users in Browser Storage Using Browser Cache	19
5.5. Example Storage Locations Used by Browsers For Cookies and Browser Cache	21
5.6. RFC Standards Documents	24
6. The '947 Patent.....	25
6.1. The Relevant Technical Field, And The Person of Ordinary Skill in the Art	29
6.2. The Prosecution History	31
6.3. Claim Construction	32
7. Overview of the Prior Art.....	34
7.1. Doughty	34
7.2. Van Boucq	41
8. Ground I.....	46
8.1. Claim 1	46
8.1.1. 1[c]: “determining that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device” and 1[d]: “assigning the unique identifier to the user.”.....	46
8.1.1.1 Doughty	47
8.1.1.2 Van Boucq	55
8.1.1.3 Doughty + van Boucq.....	58

8.1.2.	1[e]: “determining whether the user opted-in to or out of location tracking, based on whether a location tracker is installed on the user computing device;”	59
8.1.2.1	Doughty	59
8.1.2.2	Van Boucq	62
8.1.2.3	Doughty + van Boucq.....	64
8.1.3.	1[f]: “sending, upon determining that the user opted-out of location tracking, the unique identifier to the user computing device for storage in a local browser cache;”	66
8.1.3.1	“Cookies” versus “storage in local browser cache”	66
8.1.3.2	“Sending upon determining”	71
8.1.3.3	Same Unique Identifier.....	73
8.1.4.	1[l]: “identifying a second visit to the URL during the second browser session using the unique identifier stored in the local browser cache”	74
8.2.	Claim 11	77
8.3.	Claims 2-10 and 12-20	77
8.4.	Secondary Considerations	77
9.	Ground II	77
10.	Use of Demonstratives.....	78

TABLE OF EXHIBITS

Exhibit	Description
2001	Safari Privacy Overview – Learn how the Safari web browser protects your privacy (Nov. 2019) (available at https://www.apple.com/safari/docs/Safari_White_Paper_Nov_2019.pdf)
2002	The next step toward phasing out third-party cookies in Chrome (Dec. 14, 2023) (available at https://blog.google/products/chrome/privacy-sandbox-tracking-protection/)
2003	Third-party cookies restricted by default for 1% of Chrome users (Jan. 1, 2024) (available at https://debox/blog/cookie-countdown-2024jan)
2004	Thriving in the Post-Third-Party Cookie Era (Feb. 2, 2024) (available at https://www.launchlabs.ai/post/post-third-party-cookie-era)
2005	Tracking and Privacy Changes for Local Business: Capitalizing on the loss of third-party cookies (available at https://www.launchlabs.ai/ebook)
2006	fullthrottle.ai – Audience Generation (available at https://www.fullthrottle.ai/audience-generation/)
2007	Launch Labs – Automotive (available at https://www.fullthrottle.ai/automotive/)
2008	Launch Labs – Geolocation Marketing Demystified (available at https://www.launchlabs.ai/post/geolocation-marketing-demystified)
2009	fullthrottle.ai – Home Page (available at https://www.fullthrottle.ai/)
2010	Fullthrottle Technologies, LLC v. Rocket Media, LLC (d/b/a Launch Labs), No. 1:24-cv-00314 (M.D.N.C.), Dkt. Report as of March 12, 2025
2011	Fullthrottle Technologies, LLC v. Rocket Media, LLC (d/b/a Launch Labs), No. 1:24-cv-00314 (M.D.N.C.), Dkt. 24 (“FAC”)
2012	Declaration of Oded Gottesman, Sep. 9, 2025.
2013	Curriculum Vitae of Oded Gottesman
2014	Internet Engineering Task Force, RFC 6265
2015	Internet Engineering Task Force, RFC 9110
2016	Internet Engineering Task Force, RFC 9111
2017	Gregory Fleischer, Implementing Web Tracking, available at https://media.blackhat.com/bh-us-

Declaration of Dr. Oded Gottesman Regarding U.S. Patent No. 11,556,947

Exhibit	Description
	12/Briefings/Fleischer/BH_US_12_Fleischer_Implementing_Web_Tracking_gfleischer_WP.pdf.
2018	Transcript of Deposition of David Hilliard Williams, Aug. 29, 2025
2019	James F. Kurose & Keith W. Ross, Computer Networking, a Top-Down Approach (7th ed. 2013).
2020	Internet Engineering Task Force, RFC 7234, HTTP/1.1: Caching (June 2014).
2021	Onetrust, The Ultimate Cookie Handbook for Privacy Professionals, Nov. 2020.

1. Introduction & Qualifications

1. My name is Dr. Oded Gottesman. I have been retained as an expert witness by counsel for Fullthrottle Technologies, LLC (“Fullthrottle”) in the above captioned proceeding. I have been asked to provide certain opinions regarding the validity/invalidity of the U.S. Patent No. 11,556,947 (“the ’947 Patent”) in view of Petitioner Rocket Media, LLC’s (“Petitioner”) petition for *inter partes* review (the “Petition”) of Claims 1-20 (“the Challenged Claims”) of the ’947 Patent and the asserted references cited therein. My analysis in this declaration relates to claims 1-20 of the ’947 Patent (collectively, the “Asserted Claims”).

2. This declaration contains a statement of the opinions that I have formed regarding the validity/invalidity of the Challenged Claims to date and provides the bases and reasons for my opinions. In connection with those opinions, I have provided my opinion as to the level of skill of a person of ordinary skill in the art (“POSITA”), certain common general knowledge that would have been understood by a POSITA in 2021, and the appropriate meaning of one of the claim terms to a POSITA. I may offer additional opinions based on further review of materials in this proceeding, including opinions and/or testimony of other experts, including those of Petitioner.

3. I am being compensated for my time in connection with this matter at my standard hourly rate of \$700/hour. My compensation is not affected by my

opinions or the outcome of this proceeding. I do not have any financial interest in the outcome of this proceeding.

4. I reserve the right to amend and/or supplement my opinions to respond to any declarations, reports, or testimony from any of Petitioner's expert(s) or witnesses; any briefs or pleadings that Petitioner may file; and any other matters relating to validity/invalidity of the Asserted Claims, the level of skill of a POSITA, and/or the interpretation of claim terms that are proposed by Petitioner or the Patent Trial and Appeal Board ("the Board"). I also reserve the right to prepare and rely on demonstrative exhibits concerning the opinions and their bases as an aid for trial or to assist the Board in connection with this proceeding.

1.1. Summary of My Qualifications

1.1.1. Education, Employment, and Research

5. A copy of my curriculum vitae (CV) is attached as Exhibit 2013. As set forth more fully in my CV, over the course of my 30-year career in communication system hardware and software development, I have worked in nearly many aspects of communication system and database design.

6. I am currently the President and CEO of Compandent, Inc., a company I founded in February 2001. My work at Compandent includes developing and implementing digital signal processing hardware and software used by various types of communication networks. The hardware and software developed by Compandent

is used in a large variety of communication networks, including cellular networks, satellite networks, telephone networks, packetized networks, and military networks. I have partnered with SignalCom (a Microsoft company), MIT Lincoln Labs, and the Department of Defense (DoD, NSA, DARPA), and NATO to develop and implement a variety of communication system hardware and software solutions, some of which were adopted as standards by US DoD and NATO.

7. I have developed and implemented Android applications and have extensive software development experience in many areas including interfaces, protocols, communications, databases, server, client, different programming languages, and APIs, etc.

8. I have extensive experience in client-server applications, web site development, including Comparent's web site, and development environments such as Wordpress using plugins. I have also used Google Analytics and Google Advertisements, and worked with Google Analytics and Google Search Console, including incorporating Google and other third-party code that uses cookies.

9. In the late 80s I developed a database application for business management using MAGIC application generator. Over the years I have developed and implemented many interfaces and protocols for device communication, voice communication, etc., including IP based device communication for VoIP (Voice Over Internet). I monitored IP based interfaces using tools such as Wireshark. I

have developed and used many software packages that use data structures, objects, and databases. I have also developed software packages that included APIs and used others' packages using their APIs. I have developed web sites and mobile device applications that use server-client services, using different APIs, *e.g.*, Google's Android APIs. I have also served as expert in cases that were related to client-server systems and databases for e-commerce.

10. My post-secondary education began in 1988 when I graduated from Ben-Gurion University in Beer Sheva, Israel, where I obtained a Bachelor of Science in Electrical and Computer Engineering, *cum laude*. In 1992, I received a Masters of Science in Electrical and Computer Engineering from Drexel University in Philadelphia, Pennsylvania. I also received a Ph.D. from the Electrical and Computer Engineering Department of The University of California at Santa Barbara ("UCSB") in 2000. My Ph.D. research included a dissertation entitled "*Analysis-by-Synthesis Waveform Interpolative Coding of Speech at Low Bit Rates*." After receiving my Ph.D., I remained at UCSB for about a year performing post-doctorate research related to Voice-over-Internet Protocol (VoIP) and other issues related to packetized communication networks.

1.1.2. Publications

11. I have authored or co-authored numerous publications, which are set forth fully in my CV. I am an author or co-author of the below exemplary publications relating to communication systems and networking:

12. Oded Gottesman “Redundant compression techniques for transmitting data over degraded communication links and/or storing data on media subject to degradation,” US6614370, Jan 24, 2002.

13. O. Gottesman and A. Gersho, “Enhanced Waveform Interpolative Coding at Low Bit-Rate,” in IEEE Trans. Speech and Audio Processing, vol. 9, November 2001, pp. 786-98.

14. I have already served as an expert in patent cases involving client-server application services using databases. I believe that my education and experience give me expertise, and I consider myself to be an expert in, the area of web-based client-server technologies, such as HTML protocols, web browsers, and client/server storage locations and file types (*e.g.*, browser cache, cookies, *etc.*), and including the technologies described and claimed in the '947 Patent.

1.1.3 Prior Testimony

15. I have previously served as a testifying expert witness in patent cases as set forth more fully in my CV (Ex-2002).

2. Summary of My Opinions

16. For the reasons described in this declaration, it is my opinion that the Petitioner has not shown that Claims 1-20 (the “Challenged Claims”) of the ’947 Patent are obvious.

17. The primary prior art references relied on in support of Petitioner’s petition for *inter partes* review are: U.S. Patent No. 8,898,074 by Doughty *et al.* (“Doughty”) (Ex-1008) and European Patent No. 2938045 by van Boucq (“van Boucq”) (Ex-1009). I have relied on the disclosures of these references in support of my opinions. I have also relied on the additional references identified in this declaration in support of my opinions.

3. Materials Considered

18. I have considered information from various sources in forming my opinions. Besides drawing from more than thirty years of experience in computer hardware/software and data management, particularly for web-based services and applications, I have also reviewed the ’947 Patent, its file history, as well as the prior art and other references cited by Petitioner. In forming my opinions, I have considered those materials as well as the Petition, the declaration of Petitioner’s expert in support of the Petition, all exhibits to the Petition, and all other materials cited and/or identified in this declaration.

4. Legal Standards

19. I am not an attorney and will not offer opinions on the law. I have, however, an understanding of several principles concerning invalidity that I have used in arriving at my stated conclusions in this declaration.

20. First, I understand that for an invention claimed in a patent to be found patentable, it must be, among other things, new and not obvious from what was known before the application leading to the patent was filed.

21. I understand that the information that is used to evaluate whether an invention is new and not obvious is generally referred to as “prior art” and generally includes patents and printed publications (*e.g.*, books, journal publications, articles on websites, product manuals, *etc.*). I understand whether a document constitutes prior art is a legal conclusion.

22. I understand that, in this proceeding, Petitioner has the burden of showing that the Challenged Claims of the '947 Patent are invalid.

23. As I discuss further in the claim construction section below, I understand that the '947 Patent claims must be interpreted in accordance with certain standards of claim construction, and my understanding of these standards is set forth in greater detail below. The claims after being construed are then to be compared to the information in the prior art.

24. I understand that, in this proceeding, the prior art that may be evaluated as a basis for unpatentability are limited to patents and printed publications.

25. I understand that there are two ways in which prior art may render a patent claim unpatentable. First, the prior art can be shown to “anticipate” the claim. Second, the prior art can be shown to have made the claim “obvious” to a POSITA.

26. My understanding is that what is considered the relevant art is the general subject matter of the claimed invention. In determining the appropriate level of ordinary skill, my understanding is that the following factors can be considered: the inventor’s educational background and experience, the types of problems encountered in the art, prior art solutions to those problems, the rapidity with which innovations are made in the art, the sophistication of the technology, the educational background and experience of those working in the art, and the like.

27. Petitioner only asserted obviousness in its Petition. Therefore, I will confine my discussion to obviousness.

4.1. Obviousness

28. I understand that a claimed invention is not patentable if it would have been obvious to a person of ordinary skill in the field of the invention at the time the invention was made.

29. I understand that a patent may not be obtained even though the invention is not identically disclosed or anticipated by the prior art, if the differences

between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. I also understand that patentability shall not be negated by the manner in which the invention was made.

30. I understand that the following standards govern the determination of whether a claim in a patent is obvious. I have applied these standards in my evaluation of whether the asserted claims of the patent-at-issue here would have been considered obvious as of the relevant priority date. I have been asked to assume that the priority date for the claims at issue here is June 8, 2021.

31. I understand that to find a claim in a patent obvious, one must consider certain factual questions regarding the claimed invention and the prior art. Specifically, I understand that the question of whether an alleged invention is obvious requires consideration of four factors:

- 32. The scope and content of the prior art;
- 33. The differences between the prior art and the claims at issue;
- 34. The knowledge of a person of ordinary skill in the pertinent art; and
- 35. Whatever objective factors indicating obviousness or non-obviousness may be present in any particular case.

36. In addition, I understand that the obviousness inquiry should not be done based on hindsight but must be done using the perspective of a person of ordinary skill in the relevant art as of the priority date of the patent claim.

37. I understand the objective factors indicating obviousness or non-obviousness may include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention; praise of the invention by those in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the accepted wisdom of the prior art. I also understand that any of this evidence must be specifically connected to the invention rather than being associated with the prior art or with marketing or other efforts to promote an invention.

38. I understand that the obviousness analysis can consider the predictability or unpredictability of changes to the prior art and the amount of experimentation needed to make variations to the prior art. I also understand that, in order to make an obviousness determination, sometimes it will be necessary to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art. I understand that all these

issues may be considered to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

39. I understand that the obviousness analysis cannot be confined by a formalistic conception of the words “teaching, suggestion, and motivation.” It is my understanding that any motivation that would have been known to a POSITA may be considered, including common sense and the nature of the problem to be solved.

40. I understand that an invention that might be considered an obvious variation or modification of the prior art may be considered non-obvious if one or more prior art references discourages or lead away from the line of inquiry disclosed in the reference(s). A reference does not “teach away” from an invention simply because the reference suggests that another embodiment of the invention is better or preferred. My understanding of the doctrine of teaching away requires a clear indication that the combination should not be attempted (*e.g.*, because it would not work or explicit statements saying the combination should not be made).

5. Technical Background: User Location Tracking via Browsers

41. Below is a brief introduction to browser-based user tracking technologies and other terms and concepts related to web services that would have been well understood to a POSITA in 2021.

5.1. Cookies

42. One of the common forms of user location tracking via browser applications includes browser cookies. When a user visits a website with a computing device, the website can request that the user's browser store a cookie on the computing device (Ex-2021, p. 5). A cookie is a small piece of data (text file) comprising data bits generated by a website that remembers information about users and website usage, such as remembering users' custom preferences; to help users complete tasks without having to re-enter information; for authentication; and for user tracking for targeted advertising (*id.*; Ex-2001, p. 4; Ex. 2005, p. 4; Ex-2021, p. 5). Browser cookies can be thousands of characters long.

43. Cookies are browser specific (Ex-2021, p. 5). For example, if a user uses the Edge browser and visits a website, a cookie may be placed on the user's computer, so that when the user visits the website in the future, it will identify the user's return visit and may apply user preferences (*id.*). However, if the next time the user visits the same website using Chrome instead of Edge, the site will not recognize the return visit and will not apply the user preferences (*id.*).

44. Websites can use cookies for a number of purposes (Ex-2021, p. 5). For example, websites may use cookies to identify users; remember users' custom preferences; and help users complete tasks without having to re-enter information when browsing from one page to another or when visiting the site later (*id.*). They

were originally developed for e-commerce purposes, including to remember what items a user had added to their online shopping cart (Ex-2021, p. 6). Cookies are generally classified according to their purpose into one of four categories: strictly necessary cookies, performance cookies, functional cookies, and targeting cookies (advertising) (Ex-2021, p. 7).

45. Cookies may be temporary, such that they are erased when the user closes the browser, or persistent, such that they remain on the user's computer/device for a pre-defined period (Ex-2021, p. 6).

46. Cookies may be further classified according to their source as either first-party cookies or third-party cookies (Ex-2021, p. 6).

47. First-party cookies are set by the web server of the visited page and share the same domain (Ex-2021, p. 6). First-party cookies are generally considered more secure and privacy-friendly, but they still have some drawbacks. For example, while first-party cookies are mainly used for improving user experience (*e.g.*, saving preferences and login information, saving user time and effort), they can still track user behavior across a website, which may raise privacy issues. Additionally, if not properly secured, first-party cookies can be vulnerable to attacks or session hijacking, where attackers steal session cookies to impersonate users.

48. "Third-party cookies" originate from a different website from the website that a user is visiting, and from a different domain (Ex-2021, p. 8). The

most common third-party cookies are enabled by social media platforms, marketers, advertisers and ad tech companies (*id.*).

49. As an example, if you visit a news website and the site has ads on it, the news website itself can store cookies on your device (first party cookies), but your browser is also communicating with another website—which is the website that has the ad that is displayed on the news website (Ex-2021, p. 8). This other website can also store a cookie on your device, which is a third-party cookie (*id.*).

50. Third-party cookies can track users across multiple websites, building detailed profiles on their behavior, interests, and preferences.

5.2. Privacy Concerns Lead to Limits on Cookies

51. Cookies have come under scrutiny due to privacy and security concerns. Further, while some users benefit from targeted ads, many users dislike them, as users often feel overwhelmed by retargeted ads following them across websites. Also, third-party cookies can be exploited by malicious actors to steal personal data or conduct phishing attacks. Some third-party cookies can be used to send unauthorized requests from an authenticated user. Loading third-party cookies from multiple sources can even slow down page performance on the browser.

52. A technical problem was recognized when governments and companies around the world began to restrict the use of cookies due to privacy concerns, including moves to ban third-party cookies entirely (Ex-2011, ¶19; Ex-2003; Ex-

2002). For example, Article 5(3) of the European ePrivacy Directive requires that any storing or retrieving (writing or reading) of information from an end user device be subject to consent unless it is technically necessary to enable the intended communication to take place (Ex-2021, 13). This rule requires consent for all types of cookies, including first-party and third-party cookies (Ex-2021, 14). The European General Data Protection Law (“GDPR”) further regulates the use of cookies, and includes additional requirements regarding consent to cookies (Ex-2021, 20-21). By way of further example, the California Consumer Privacy Act (“CCPA”) seeks to provide users with choice about the personal information that businesses collect, including through use of cookies, and how business use or sell that personal information (Ex-2021, 42-43).

53. Makers of web browser software have responded to the privacy concerns surrounding cookies by restricting them or allowing users to restrict them. For example, Apple’s Safari browser “block[s] third-party cookies by default,” and further limits tracking via first-party cookies (Ex-2001, 4, 6-7). Similarly, Google allows users to block third-party cookies and has considered blocking third party cookies by default (*see* Ex-2002; Ex-2003).

54. These cookie restrictions limit website owners’ ability to identify a user each time the user visits the same web page, the number of times a user visits a web page, or to determine that it was the same user accessing the internet from different

devices (*e.g.*, a laptop and a mobile phone) (Ex-2021, pp. 5-6). The technical problem included how to develop new software that facilitates interaction between users and websites while still meeting certain technical constraints (*e.g.*, being persistent across multiple internet browsing sessions), and while meeting the privacy concerns and restrictions associated with cookies, all without slowing the user's browsing experience.

5.3. Tracking Users in Browser Storage Using Cookies

55. HTTP cookies are well supported in some form by every major web browser (Ex.-2017, p. 9, citing http://en.wikipedia.org/wiki/HTTP_cookie; *See also*, Ex-2019, p. 139-40 (“Most major commercial Web sites use cookies today.”)). A well-known “method to identify a user is by using cookies—small pieces of data (each limited to 4 KB) placed in a browser storage by the web server” (Ex.-2017, p. 5). “A cookie is a small piece of data (text file) comprising data bits generated by a website that remembers information about users and website usage” (Ex-2017, p. 5). “When a user visits a website for the first time, a cookie file with a unique user identifier (could be randomly generated) is stored on the user's computer” (Ex.-2017, p. 5). “Then, the website can retrieve this identifier each time the user visits it, unless the user delete the cookie from his computer” (Ex.-2017, p. 5).

56. “[C]ookie technology has four components: (1) a cookie header line in the HTTP response message; (2) a cookie header line in the HTTP request message;

(3) a cookie file kept on the user's end system and managed by the user's browser; and (4) a back-end database at the Web site" (Ex-2019, p. 139-40). Figure 2.10 below is a system flow diagram illustrating example HTTP request messages and HTTP response messages communicated between client and server devices for communicating cookie-related data.

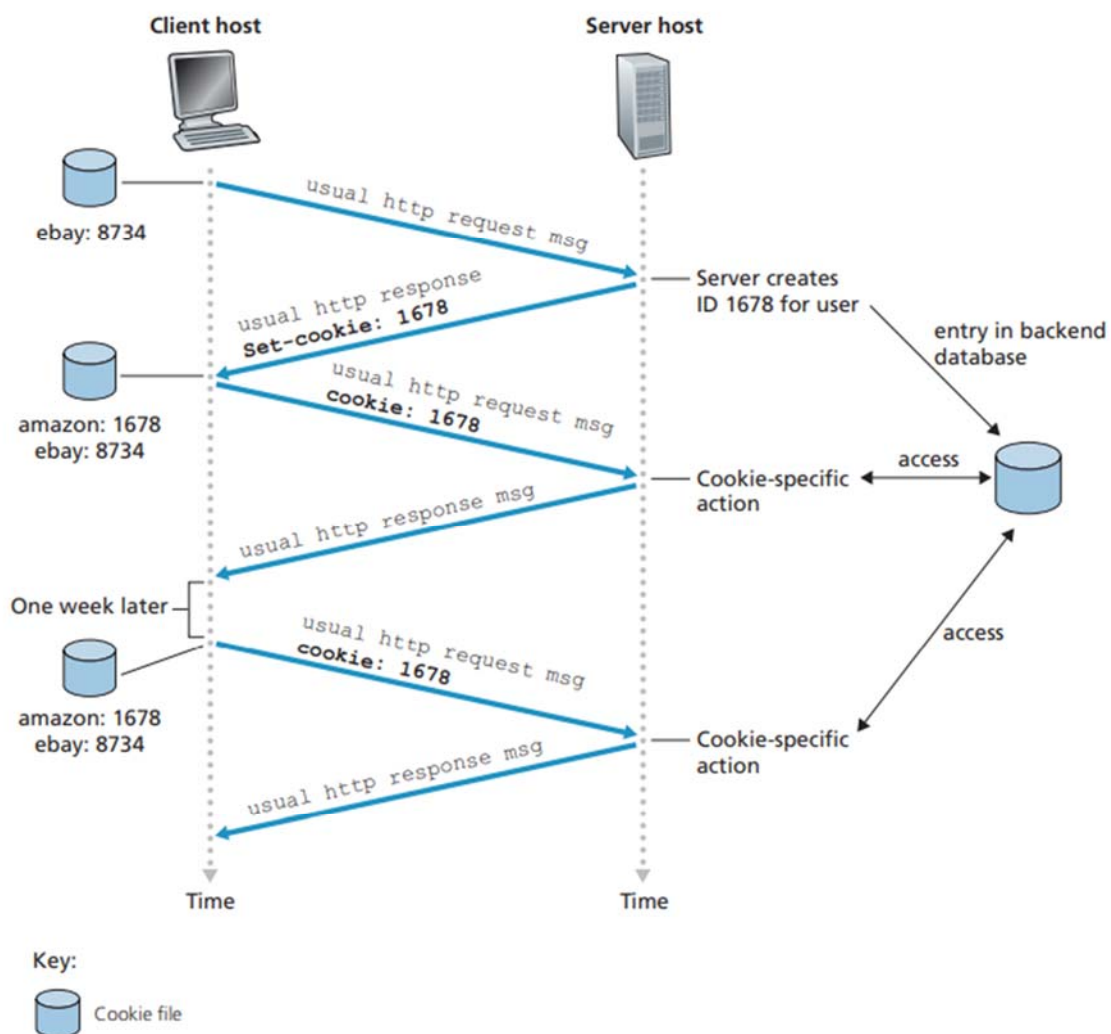


Figure 2.10 ♦ Keeping user state with cookies

(Ex-2019, p. 141).

57. The Internet Engineering Task Force (IETF) published the Request for Comments (RFC) 6265 in April 2011 that “defines the HTTP Cookie and Set-Cookie header fields” in the “HTTP request” and “HTTP response” messages (Ex-2014, Abstract and p. 5). The “HTTP Cookie and Set-Cookie header fields ... can be used by HTTP servers to store state (called cookies) at HTTP user agents, letting the servers maintain a stateful session over the mostly stateless HTTP protocol” (Ex-2014, Abstract).

58. As described in RFC 6265, “[u]sing the Set-Cookie header field, an HTTP server can pass name/value pairs and associated metadata (called cookies) to a user agent” and “[w]hen the user agent makes subsequent requests to the server, the user agent uses the metadata and other information to determine whether to return the name/value pairs in the Cookie header” (Ex-2014, p. 3).

59. The RFC 6265 standards document specifically provides a “Storage Model” for storing cookies (Ex-2014, p. 21). As described in this standard document, “[w]hen the user agent ‘receives a cookie’ ... the user agent MUST process the cookie” by “[c]reat[ing] a new cookie” and “[i]nsert[ing] the newly created cookie into the cookie store” (Ex-2014, p. 21).

60. As further described in the RFC 6265 standards document, “cookies facilitate tracking because they are persistent across user agent sessions and can be

shared between hosts” (Ex-2014, p. 28). Thus, the cookie store described in the RFC 6265 comprises a persistent storage.

61. “[T]he standard web cookie has the benefit that it will be automatically sent on every web request to servers that match the path and domain” (Ex.-2017, p. 9). As required by the RFC 6265 standards document, “[t]he user agent includes stored cookies in the Cookie HTTP request header” (Ex-2014, p. 25). “If the user agent does attach a Cookie header field to an HTTP request, the user agent MUST send the cookie-string (defined below) as the value of the header field” and “compute the ‘cookie-string’ from a cookie store and a request-url” (Ex-2014, p. 25).

5.4. Tracking Users in Browser Storage Using Browser Cache

62. Another form of storage available to browsers includes browser cache (Ex-1012, p. 7). The Internet Engineering Task Force (IETF) published the Request for Comments (RFC) 7234 in June 2014 standardizing the definition of “HTTP caches and associated header fields that control cache behavior” (Ex-2020, Abstract).

63. “When a browser downloads an object (e.g., an image), it is usually stored in the browser cache for faster display when the user visits the website again” (Ex-1012, p. 7). In one practical implementation of how browser cache is generally used, “when a user browses a website, the website can easily determine if this user

visited it before (so that this object is pulled from the cache) or not (so that the object is downloaded from the server)” (Ex-1012, p. 7).

64. As defined in RFC 7234, “[a]n HTTP cache is a local store of response messages and the subsystem that controls storage, retrieval, and deletion of messages in it” (Ex-2020, p. 4). A “goal of HTTP caching ... is significantly improving performance by reusing a prior response message to satisfy a current request” (Ex-2020, p. 4). “A cache stores cacheable responses [to server requests] to reduce the response time and network bandwidth consumption on future, equivalent requests” (Ex-2020, p. 4).

65. RFC 7234 defines both a “shared cache” and a “private cache” (Ex-2020, p. 4). “A shared cache is a cache that stores responses to be reused by more than one user; shared caches are usually (but not always) deployed as a part of an intermediary”, while “[a] private cache, in contrast, is dedicated to a single user; often, they are deployed as a component of a user agent” (Ex-2020, p. 4).

66. Users may be tracked in browser cache by “[e]mbedding identifiers in cached documents” (Ex-1012, p. 7). “Unless the browser’s cache is disabled, the cache history is cleared, or the resource is retrieved using a private browsing mode, any content may be stored indefinitely” in browser cache (Ex-2017, p. 9). One “approach to using the browser cache for tracking purposes is to embed the tracking identifier directly in the content and then force it to be cached by setting the

appropriate headers” (Ex-2017, p. 9). “By embedding the tracking identifier directly in the content, this allows for any active content to gain access to value where it is exposed” (Ex-2017, p. 9).

67. Embedding tracking identifiers in different types of cached content “depends on the type of content” (Ex-2017, p. 9). For example, “[i]n script content [generated using Javascript], storing an identifier could be [implemented by] embedding a variable and then exposing the value as a variable, function or callback” (Ex-2017, p. 9). “In instances where JavaScript is not currently enabled or executing, [the tracking identifier] could be read at a future date by referencing the cached HTML file” (Ex-2017, p. 10). “The identifier can be stored in an invisible div and subsequently read from the browser cache using the div id property” (Ex-1012, p. 7, citing Ex-2017, p. 10). “Embedding desired tracking identifiers into cached CSS [(Cascading Style Sheets)] content can be done in several ways, but browser support varies” (Ex-2017, p. 10).

5.5. Example Storage Locations Used by Browsers For Cookies and Browser Cache

68. As cookie and browser cache locations can be treated differently for different browsers, I have reviewed the storage folder locations for each of the following browsers. Provided below are identified file locations for cookies and browser cache by particular browser types.

Google Chrome

Cookies:

Stored in Cookies (SQLite DB).

Path (Windows): %LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies

where the path variable %LOCALAPPDATA% is also referred to as C:\Users\%USERNAME%\AppData\Local\, where %USERNAME% is the login user name.

Path (macOS): ~/Library/Application Support/Google/Chrome/Default/Cookies

Local Browser Cache:

Stored separately in the Cache directory, often using the “Simple Cache” file format.

Path (Windows): %LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache.

For example, in my Windows PC these are the paths used to store the cookies and the cache.

Mozilla Firefox

Cookies:

Stored in cookies.sqlite (SQLite DB).

Path (Windows):

%APPDATA%\Mozilla\Firefox\Profiles\<profile>\cookies.sqlite

For example on my PC it is located under

C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\

Path (macOS/Linux): ~/Library/Application

Support/Firefox/Profiles/<profile>/cookies.sqlite

Local Browser Cache:

Stored separately under the cache2 directory.

Path: <profile>/cache2/

For example in my PC it is stored in caches.sqlight files located under C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\<profile>\storage\default\

Safari

Cookies:

Stored in Cookies.binarycookies (older versions) or in SQLite DB under Safari's data container.

Path (macOS):

~/Library/Containers/com.apple.Safari/Data/Library/Cookies/

Local Browser Cache:

Stored in the Cache folder.

Path (macOS): ~/Library/Caches/com.apple.Safari/

Microsoft Edge

Cookies:

Stored in Cookies SQLite DB.

Path (Windows): %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cookies

On my PC for example it is stored at:

C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies

Local Browser Cache:

Stored in Cache folder.

Path (Windows): %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\

On my PC for example it is stored at:

C:\Users\%USERNAME%\AppData\Local\Microsoft\Edge\User Data\Default\Cache\

69. Further confirming the separate storage of cookies and cache, browsers provide separate facilities for managing and clearing cookies and cache. For example, in the Chrome browser under "Settings," "Privacy and security," "Delete browsing data," there are separate options to remove "Cookies and other site data" and other items, including "Cached images and files." In the Mozilla Firefox browser, under "Settings," "Privacy & Security," "Cookies and Site Data," "Clear

Data,” there are separate options for “Cookies and site data,” and other items, including “Temporary cached files and pages.” In the Microsoft Edge browser, under “Settings,” “Privacy, search, and services,” “Clear browsing data,” “Choose what to clear,” there are separate options for “Cookies and other site data,” and other items, including “Cached images and files.” A POSITA would understand that these separate options for clearing data operate on separate storage for cookies and cache.

5.6. RFC Standards Documents

70. The RFC documents cited in this declaration—RFC 6265, RFC 7234, RFC 9110, and RFC 9111—are or were accepted standards published by the Internet Engineering Task Force (“IETF”). The status of each document can be found at a link to datatracker.ietf.org found on the first page of each (see, e.g., Ex-2014, 1 (“Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6265>.”)). The table below shows the current status of each of these standards documents, according to their respective pages on datatracker.ietf.org as of today.

Document	Date	Current Status
RFC 6265	April, 2011	Proposed Standard
RFC 7234	June, 2014	Proposed Standard, Obsoleted by RFC 9111
RFC 9110	June 2022	Internet Standard
RFC 9111	June 2022	Internet Standard

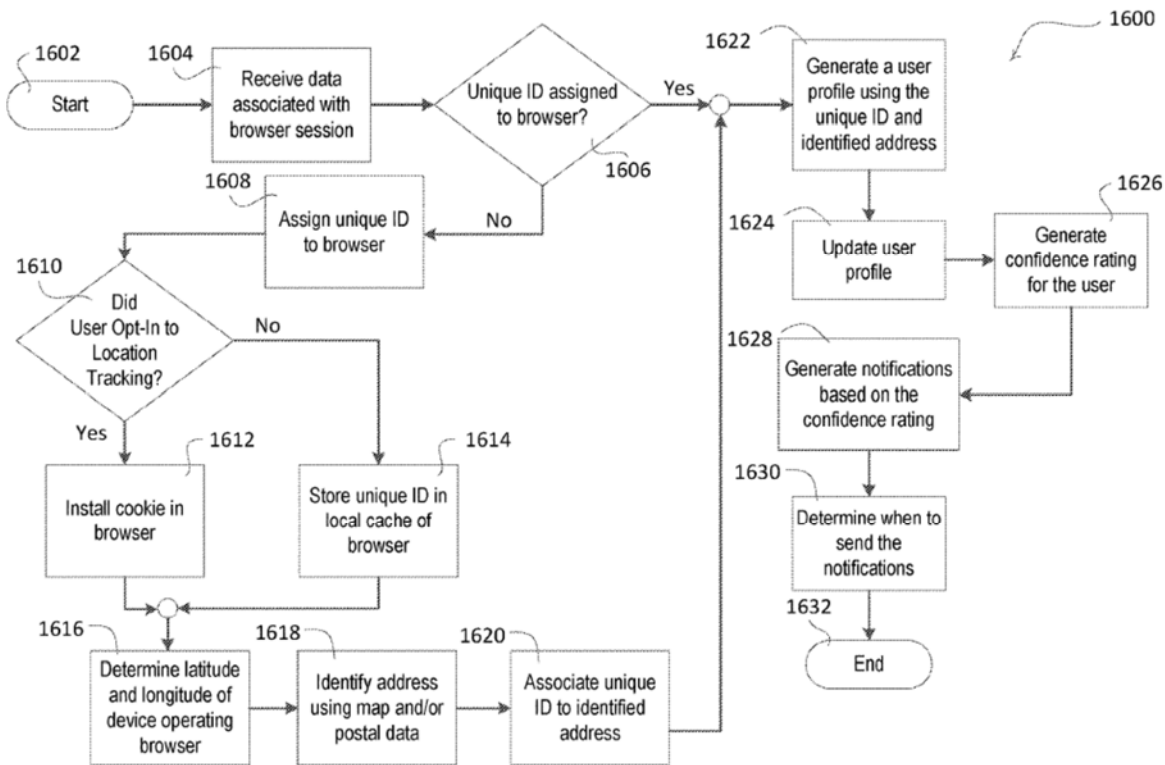
71. The term “Proposed Standard” can be confusing. Even in the status “Proposed Standard,” RFCs are final publications. Generally, RFCs provide

technical standards and documentation for how the Internet works. The cited RFC documents each states on its cover that it “represents the consensus of the IETF community” (*e.g.*, Ex-6265, 1).

72. Pre-RFC documents that are Internet Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. Preliminary documents will say “draft” and have an expiration date. They will further caution the reader that it is inappropriate to use Internet-Drafts as reference material or to cite them other than as work in progress. None of the RFC documents cited in this declaration are drafts.

6. The '947 Patent

73. The '947 Patent discloses and claims a novel technique to solve the challenge presented by restrictions on cookies. For example, '947 Patent Figure 16, reproduced below, describes an embodiment of the invention:

'947 Patent, Fig. 16

(Ex-1001 Fig. 16).

74. At 1604, a computing device receives browsing session data from a user such as “anonymous data (*e.g.*, data that includes no personally identifiable information associated with the user)” (Ex-1001, 43:15-26). Examples of such anonymous data are time, date, webpage URL, browser type, language, IP address, and location (Ex-1001, 43:26-29).

75. Because the received data is anonymous, the '947 Patent describes multiple techniques for determining whether the user was previously identified with a unique identifier (Ex-1001, 9:47-59, 43:49-44:4). In one example technique, the '947 Patent describes that the “computing device may determine that there is no

unique identifier associated with the user computing device when there is no location data stored for the user computing device” (Ex-1001, 9:47-52, 43:52-55). According to this technique, “the computing device may access a database or other storage location that maintains a mapping of unique identifier to a browser session, a user computing device, and/or location data” (Ex-1001, 9:52-55, 43:56-59). “Additionally or alternatively, the computing device may determine whether there is a unique identifier for associated with the user based on presence of a location tracker (e.g., cookie) installed in the browser application on the user computing device” (Ex-1001, 9:55-59, 43:59-63). “The tracker may include the unique identifier associated with the user” (Ex-1001, 9:59-61, 43:63-64). “The tracker may have been installed in the user's browser application (e.g., by the computing device) during a previous visit to the URL via the user's browser application, for example, if the user opted-in to location tracking, as described herein” (Ex-1001, 9:61-65, 43:64-44:1). In this “Unique Identifier/Tracker” embodiment, the anonymous user is identified not with saved location data, but rather, with a previously assigned location tracker associated with a unique identifier.

76. The '947 Patent's claimed technique considers whether the system previously stored location data for the user that is associated with an assigned unique identifier (Ex-1001, 43:55-58). As the '947 Patent describes, the system “may access a database or other storage location that maintains a mapping of unique

identifier” to saved location data (Ex-1001, 43:55-58). At 1608, if the computing device determines that no unique identifier has been assigned based on a lack of stored location data, the computing device generates a unique identifier for that user (Ex-1001, 44:5-8). When the computing device determines (1606) that a unique ID was previously assigned to the browser, the user is no longer anonymous and the system updates the user profile (1622-1632) (Ex-1001, 44:1-4). If, however, the computing device determines that there is no unique identifier assigned to the user based on the lack of stored location data for the anonymous user, the computing device generates (1608), a unique identifier for the anonymous user (Ex-1001, 44:5-8).

77. In order to track the user and update a user profile, the computing device determines at 1610 whether the user opted-in to location tracking (Ex-1001, 44:17-18). If the user opted-in to location tracking, there is a “tracker (*e.g.*, cookie)” in the browser application” (Ex-1001, 44:25-27; Fig. 16, 1612).

78. If there is no “tracker (*e.g.*, cookie)” in the browser application, the computing device stores the generated unique identifier in the user’s local browser cache at 1614 (Ex-1001, 44:59-62). Because the assigned unique identifier is stored in the local browser cache, the computing device can recognize return visits by the user when there is no “tracker (*e.g.*, cookie)” and when using the same browsing application (Ex-1001, 44:59-61, 44:65-67). The unique ID may enable persistence

across browser sessions and maybe recognizable across browsing sessions, but not browser applications (Ex-1001, 45:12-20). Further, the unique ID “may remain in the local browser cache, for example, until the local browser cache is explicitly cleared” (Ex-1001, 45:14-16).

79. At 1616, the computing device determines the user’s latitude and longitude from the browsing session data (Ex-1001, 45:21-25). At 1618, the computing device determines a physical address (*e.g.*, postal address) for the browsing session by correlating the browsing session location data with information (*e.g.*, map information) using an application programming interface (“API”) (Ex-1001, 45:31-41). At 1620, the computing device associates the unique identifier with the physical address (Ex-1001, 45:61-65). Having assigned a unique identifier to the anonymous user, determined how to track the anonymous user, and determined the location of the anonymous user, the system generates a profile for the user (1622-1632) (Ex-1001, 46:9-47:29). In summary, the ’947 Patent discloses a new technique that uses unique identifiers, the lack of saved location data, and tracking techniques to solve the problem of increasing limits on browser cookies.

6.1. The Relevant Technical Field, And The Person of Ordinary Skill in the Art

80. I was asked to use the definition of a POSITA provided by Petitioner for purposes of this analysis (Petition, p. 14).

81. I believe such a person also would have been familiar with technologies known at the time, such as such as online web services, hypertext transfer protocol (HTTP), cookies (*e.g.*, first-party and third-party cookies) and other browser-based location tracking techniques, browser storage (*e.g.*, including browser cache), web servers, HyperText Markup Language (“HTML”) and HTML communications, as well as other technologies implemented in accessing web services.

82. As explained above, I understand that the relevant timeframe runs up to June 8, 2021.

83. As shown in my CV, I have extensive experience in the relevant technical field (“online web services and browser-based location tracking techniques”). Based on my experience, I have an understanding of the relevant field in the relevant timeframe.

84. I consider myself to be a person of at least ordinary skill in the art for the '947 Patent. As of 2021, I had a Bachelors, Masters, and Ph.D degrees in electrical and computer engineering and at least 30 years of experience with online web services, web servers, browser-based location tracking techniques (*e.g.*, via cookies and other technologies), and/or internet browsers and related software applications, as well as about 25 years of web development experience.

6.2. The Prosecution History

85. In preparing my declaration, I have reviewed the file history of the '947 Patent ("File History") (Ex-1002). I discuss only portions of the file history herein but reserve the right to rely on any other portion of the file history for my opinions.

86. The '947 Patent was filed as U.S. App. No. 17/687,992 on March 7, 2022 ("the '992 application"). The '992 application claimed priority to U.S. Provisional Patent Application No. 63/208,275, filed on June 8, 2021. The as-filed '992 application contained 20 claims, of which claims 1-10 were method claims (with claim 1 being independent) and claims 11-20 were machine-readable storage device claims (claim 11 being independent) (Ex-1002, pp. 223-37).

87. In a first, and only, office action, the examiner rejected claims 1-20 under 35 U.S.C. § 101 as not being directed to patentable subject matter (Ex-1002, pp. 73-77). Claims 1, 2, 4, 5, 6, 9-12, 14, 15, 16, 19, and 20 were rejected as being obvious in view of U.S. Patent Pub. No. 2014/0143655 by Alon et al ("Alon"), in further view of U.S. Patent Pub. No. 2019/0199774 by Demsey et al ("Demsey"), in further view of U.S. Patent Pub. No. 2010/0323716 by Jaffri ("Jaffri") in further view of U.S. Patent Pub. No. 2013/0151645 by Siliski (Ex-1002, pp. 78-96). Claims 3 and 13 were rejected as being obvious in view of Alon, Demsey, Jafri, and Siliski, in further view of U.S. Patent No. 8,935,797 by Silver et al ("Silver") (Ex-1002, pp. 97-98). Claims 7, 8, 17, and 18 were rejected as being obvious in view of Alon,

Demsey, Jafri, and Siliski, in further view of U.S. Patent Pub. No. 2020/0233911 by Siroker et al. (“Siroker”) (Ex-1002, pp. 98-101).

88. In a response to the rejection, the Patent Owner amended the claims to recite “identifying a second visit to the URL during the second browser session using the unique identifier stored in the local browser cache” and argued that the asserted references are completely silent with respect to this subject matter (Ex-1002, pp. 56, 59, 64-66). The Patent Owner also argued that the asserted references fail to teach or suggest “sending, upon determining that the user opted-out of location tracking, the unique identifier to the user computing device for storage in a local browser cache” (Ex-1002, pp. 65-66). The Patent Owner further traversed the rejection of claims 1-20 for lack of patentable subject matter due to the analysis in the office action being insufficient to establish a proper rejection under the two-prong test under Alice/Mayo (Ex-1002, pp. 62-64). The examiner agreed and allowed the ’992 application (Ex-1002, pp. 24-33).

6.3. Claim Construction

89. I understand that, in this proceeding, the claims are construed according to their ordinary and customary meaning, in view of the specification and prosecution history, to POSITA as of the effective filing date of the underlying patent application.

90. I have been instructed that the claims of the '947 Patent are to be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention in light of the specification and the prosecution history pertaining to the patent. I have followed these principles in my analysis.

91. I understand that the Petitioner agreed with the following proposed construction for certain claim terms (Petition, pp. 15-16):

Term	Construction
"location tracker"	"the third-party tracking cookie described in the patent specification ('tracker (e.g., cookie)')"
"upon determining that the user opted-out of location tracking"	"upon determining that the user opted out of location tracking by the lack of a ('tracker (e.g., cookie)')"
"unique identifier"	"unique to the user and whose correlation to the user is known by the assignor"
"determining that the user has not been assigned a unique identifier"	"a 'unique identifier' that was not previously assigned when it was previously determined that the user had opted out of location tracking"

92. I have used these constructions in my analysis.

93. I am not aware of any other terms that require a construction for purposes of my analysis and have applied the plain and ordinary meaning of the claims to a POSITA.

7. Overview of the Prior Art

7.1. Doughty

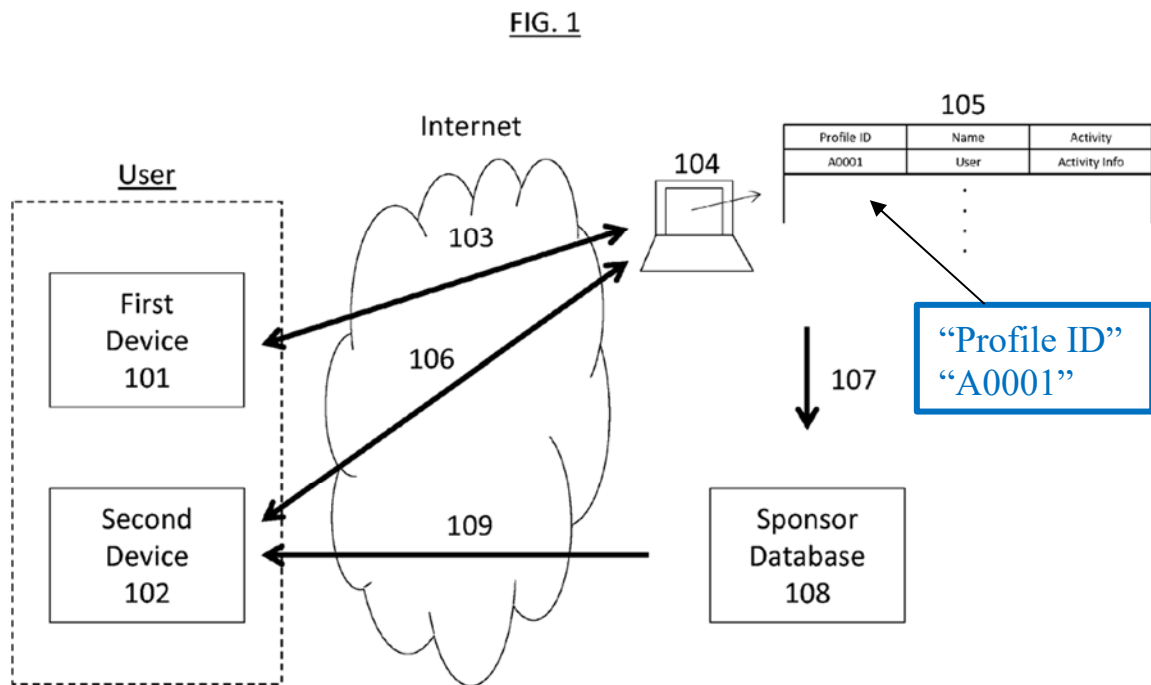
94. Doughty identifies that an internet user of a stationary device can be sent advertising on the stationary device (Ex-1008, 5:33-58, 9:32-63). According to Doughty, there was “no efficient way to optimally target the same user across all the devices he may use” including for example, cellular phones, smart phones, televisions, and gaming devices (Ex-1008, 5:35-53, 9:64-10:11). Petitioner relies on at least two embodiments of Doughty, a “Profile-ID Embodiment” and a “MKP Embodiment.”

95. **Profile ID Embodiment:** Doughty’s Profile ID Embodiment focuses on assigning a unique identifier to each device, determining whether the devices are associated with the same user based on user activity, and then linking the assigned identifiers, so that an advertiser can send advertisements to both devices based on knowing that both devices belong to the same user (Ex-1008, 10:34-67).

96. As shown with reference to Figures 1 and 2, Doughty’s “server 104 communicates with first device 101 to receive information relating to the user’s activity on first device 101” (Ex-1008, 10:34-36, 12:10-13; Fig. 2, 201). Upon receiving the “user’s activity information, server 104 assigns a unique identifier” (202) and “stores the assigned unique identifier, user information, and activity information in table 105” at the server (Ex-1008, 10:45-50; 12:13-15, Fig. 2, 202).

The “user’s activity may be [sic] behavioral pattern, viewing habits, usage information, duration on each application, geographic location, proximity to other locations, etc.” (Ex-1008, 10:36-39). Doughty shows the assignment of Doughty’s unique identifier as “Profile ID” “A0001” at server 104 in table 105 (Figure 1 below) (Ex-1008, Fig. 1).

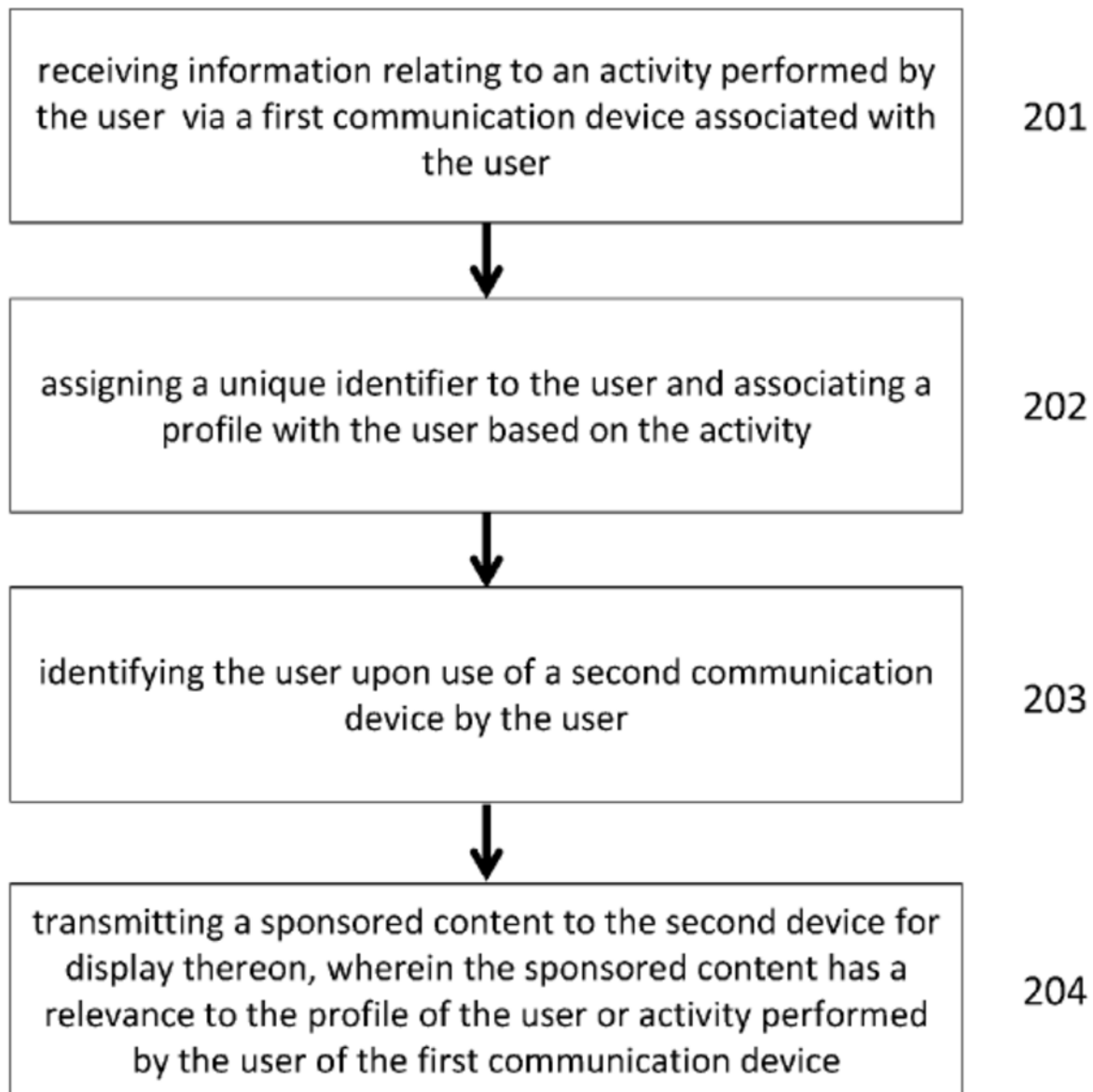
Doughty Fig. 1 (Ex-1008) (Annotated)



97. At 203, Doughty also teaches that server 104 may “identify the second device 102” as being used by the same user (Ex-1008, 10:54-56, 12:15-16, Fig. 2). Sponsored content is transmitted (204) to the second user device that is relevant to the profile of the first user device (Ex-1008, 12:16-20).

Doughty Fig. 2 (Ex-1008)

FIG. 2



98. Doughty teaches with reference to Figures 3-8 different embodiments within the Profile ID Embodiment for determining that two devices have been used by the same user (*e.g.*, user profiles, user managed assets, & use patterns) and creating a “universal profile” to correlate those two devices so that advertisers can

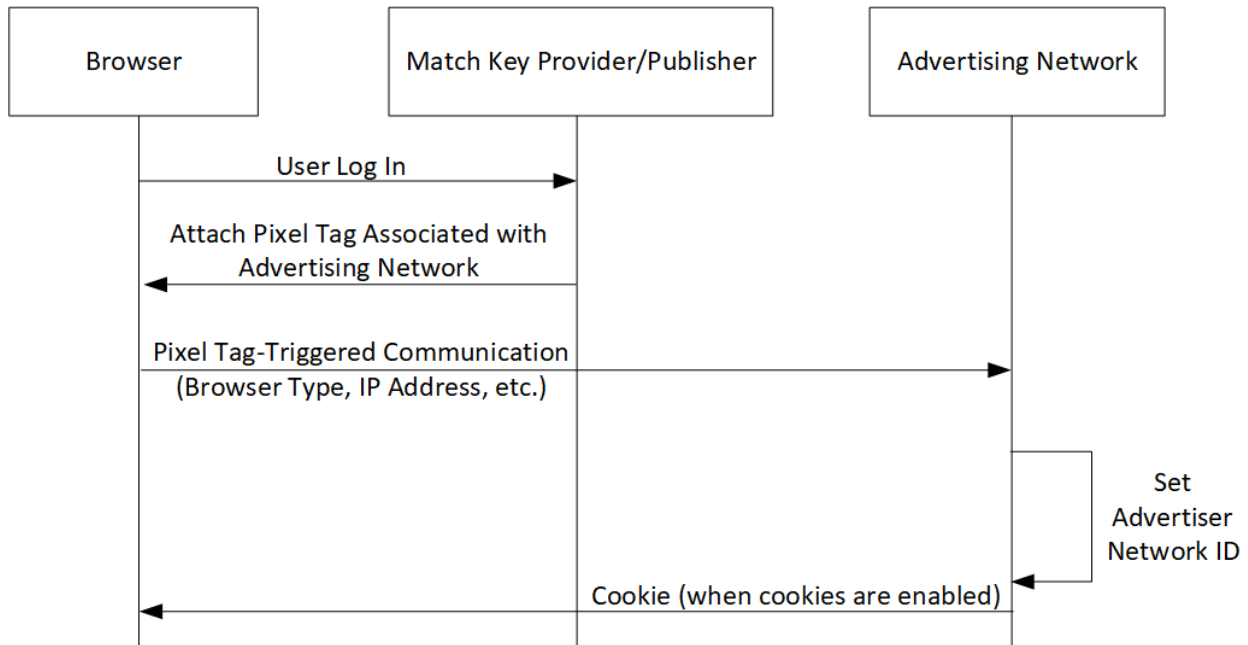
use data from the two devices to select advertisements to send to the user (Ex-1008, see generally 12:35-15:17; Figs. 3-8). Doughty, however, does not disclose sending Doughty's server Profile ID to the user devices, as Doughty's Profile ID is used to correlate devices and for sending advertisements (Ex-1008, Figs 3-8). Nor does Doughty discuss determining whether a unique identifier was previously assigned based on "a lack of stored location data." Doughty also does not discuss cookies in reference to the Profile-ID Embodiment.

99. **MKP Embodiment:** Doughty discloses "another embodiment" (i.e., "MKP Embodiment") in which "an advertising network" identifies "match keys for the same user across wired web, mobile web, and mobile application traffic," to enable the "advertising network to collapse a profile for a user and create [sic] universal profile" (Ex-1008, 16:38-42). Doughty discloses a two-step process. First, the advertising network establishes communication with a user device based on a matchkey provider's communication with a user device. Second, the advertising network creates a user device profile with a matchkey provided by the matchkey provider, user device information transmitted by the user device to the advertising network, and information the advertising network can obtain from a data supplier using the matchkey.

100. **AD Network Establishes Communication:** Doughty discloses that an advertising network can use pixel tags to establish communication with a user

device that is in communication with a MKP. After a user logs into a publisher or application (*e.g.*, MKP), Doughty discloses that the publisher (MKP) sends a pixel tag to the user that enables the advertising network to serve a cookie to the user's browser (Ex-1008, 16:63-65). Doughty describes the pixel tag as a "usually a transparent graphic image...placed on a webpage or in an email" (Ex-1008, 17:11-14). HTML code for a pixel tag can point to the ad network's site (Ex-1008, 17:16-20). When the user's browser loads the HTML code from the publisher (MKP) that includes a pixel tag pointing to the advertising network, the HTML code associated with the pixel tag directs the user device to pass information such as the type of browser, user IP address, and previously set cookie values to the advertising network (Ex-1008, 17:16-20). As Doughty provides no figure for the MKP embodiment, I have included a diagram to illustrate and explain Doughty's disclosure.

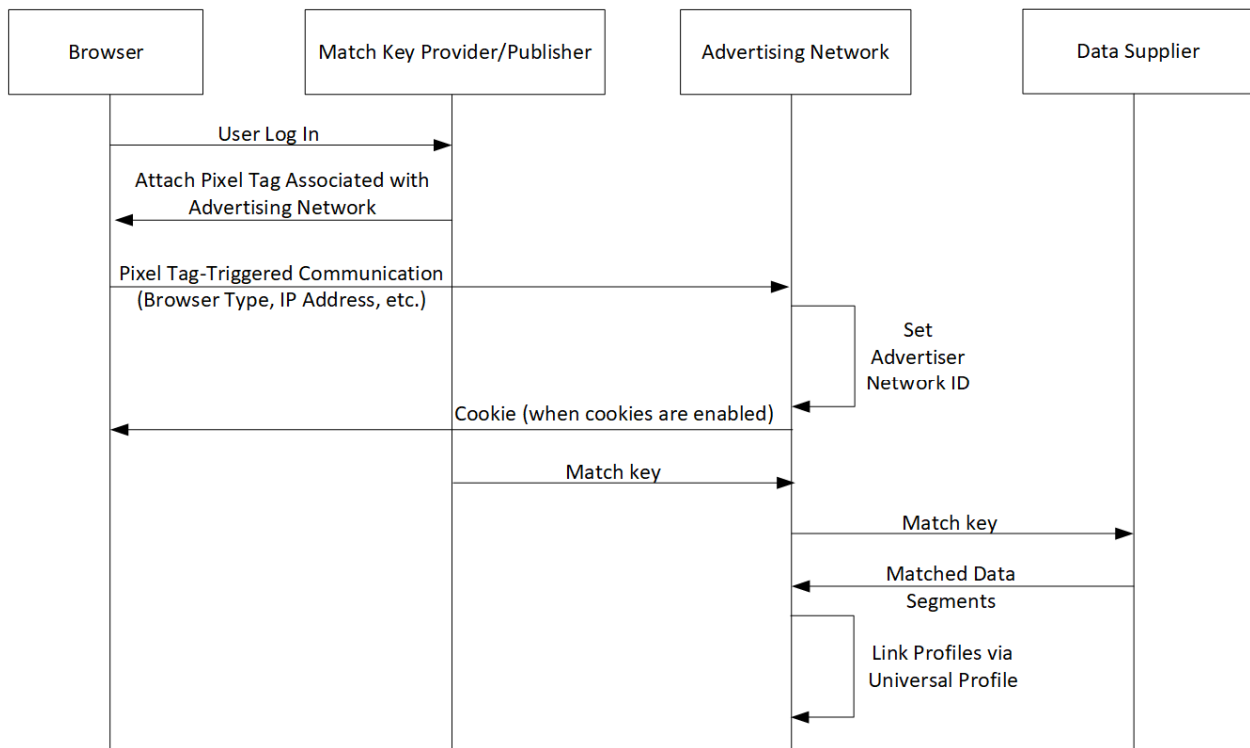
Doughty's MKP Embodiment:
Establishing Ad Network – User Device Communications



101. **Profile Creation:** Once the advertising network has received information from the user device, the advertising network builds a user device profile as follows. The MKP provides the advertising network with a matchkey that is associated with the information provided by the user browser to the advertising network (*e.g.*, IP address). Examples of information sent by the MKP to the advertising network include: 1) an obfuscated or encrypted personal identifiable information (oPII), such as a name, address, email, and zip code; 2) a consistent cross-channel user identifier, such as a login ID or internal user ID; or 3) an MKP ID, which is user ID that is pre-processed to match with the data sources (Ex-1008, 16:65-17:3). The advertising network sends the received matchkey to a data supplier

(Ex-1008, 17:8-10). In response to receiving the matchkey, the data supplier sends the advertising network matching segments that are associated with the user (e.g., “student,” “male,” “25 years old,” and “luxury shopper.”) (Ex-1008, 17:8-10). The advertising network uses the information received from the browser and the data supplier information to build a profile for the user device (*see* Ex-1008, 17:34-41). The advertising network can determine that two user devices are associated with the same user if the user profile devices are correlated (*see* Ex-1008, 16:38-50).

Doughty’s MKP Embodiment: Profile Creation



102. **Cookies Off:** Doughty recognizes that “[t]urning off browser cookies will prevent pixel tags from tracking the user’s activity,” in which case a pixel tag can only account for an anonymous visit (*e.g.*, a profile cannot be created) (Ex-1008,

17:24-27). Doughty teaches that if the user is anonymous, “the advertising network will not be able to recognize him by the previously assigned ID” (Ex-1008, 17:46-49). This is because the ad network will not be able to set a cookie in the browser, and the browser will not return the cookie and user information to the ad network. With cookies off, the advertising network cannot build the user device profile because the advertising network is not receiving user device information that can be correlated with the MKP information to identify the user.

103. Doughty’s solution to an advertising network seeing an anonymous user, due to cookies being turned off, is that the “advertising network may uniquely identify a user by creating a hashed (e.g., anonymous) email address” (Ex-1008, 17:28-30).

104. **New User Devices:** Doughty teaches to identify new user devices “by user behavior and location” (Ex-1008, 17:57-59) and correlating this new user device information with other saved device information to correlate two devices to the same user (*see, e.g.*, Ex-1008, 15:41-45, 16:9-27).

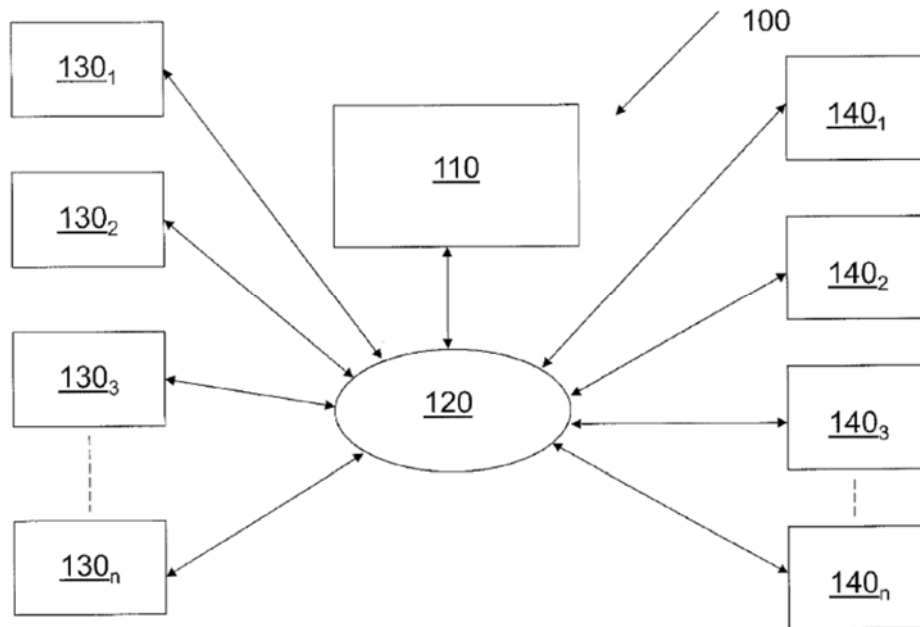
7.2. Van Boucq

105. Van Boucq proposes a cookie-based solution to the alleged problems with using IP addresses to locate internet users for targeted advertising. Using an IP address is problematic, according to van Boucq, because IP addresses may be temporarily assigned, are imprecise in identifying exact location, may not be

associated with the device's geographic location, and can change (Ex-1009, ¶¶[0005], [0010]). Also, many users may refuse to be “geolocated by their browsers,” their browser's geolocation services, and to specify their location (Ex-1009, ¶[0009]). Thus, a “purpose of the present invention” of van Boucq was “to provide a geolocation method enabling a precise geolocation to be assigned to an Internet user whose IP address is known, but who is not geolocated by any geolocation method other than geolocation via the user's IP address (Ex-1009, ¶[0013]).

106. Van Boucq discloses a “communication system 100” (Fig. 1) comprising “an internet service provider 100” that is the interface with the internet 120 for Internet users 140_{1-n} and services providers / advertisers 130_{1-n}. (Ex-1009, ¶[0056]). The Internet providers 130_{1-n} preferably provide the internet users local information relating to a specific geographic area defined by geographic coordinates “longitude and latitude” predetermined by each Internet user 140_{1-n} (Ex-1009, ¶[0056]).

Van Boucq Fig. 1

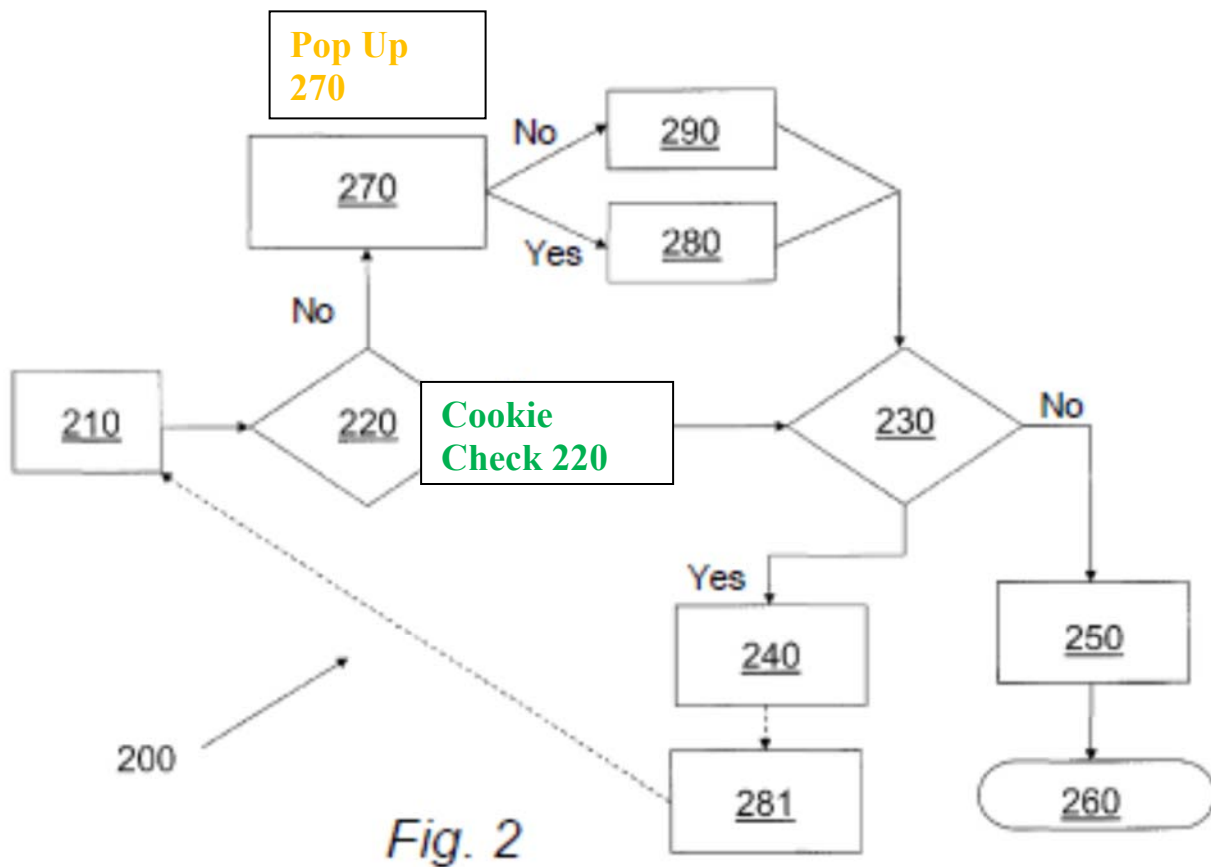


(Ex-1009 Fig. 1).

107. With reference to Figure 2, van Boucq describes a cookie check and a pop up for determining whether to send a location to a user device. Van Boucq's cookie check determines whether the Internet user already has a connection cookie, which makes it possible to determine whether the geolocation of said Internet user has already been stored in a browsing device (Ex-1009, ¶¶[0060], [0063]). If van Boucq's cookie check is positive and "the user's geolocation has already been stored in the communication system," the communication system will display an advertisement associated with the user's saved location (Ex-1009, ¶[0060]). However, if the cookie check negative, van Boucq teaches that "the Web browser will send a pop-up (message) 270 asking the user if he/she wishes to be geolocated"

(Ex-1009, ¶¶ [0063], [0068]). Regardless of whether the user answers the pop-up yes or no (Fig. 2, 270, 290), van Boucq creates a connection cookie (Ex-1009, ¶¶ [0063], [0068]). Van Boucq uses this determined location for selecting advertisements for the user (Ex-1009, ¶ [0069]).

van Boucq Fig. 2 (Annotated)



108. While van Boucq determines a user location and saving that location, van Boucq does not disclose tracking the user and routinely updating the user location. In contrast, van Boucq's saved location data is static. Van Boucq's static location supports van Boucq's desire to send advertisements based on the user's determined location (e.g., residence). Van Boucq does not teach updating that saved location if, for example, the user drives 30 miles.

8. Ground I

109. In my opinion, the combination of Doughty and van Boucq, in view of the common knowledge in the art, does not render obvious the claims of the '947 Patent.

8.1. Claim 1

8.1.1. 1[c]: “determining that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device” and 1[d]: “assigning the unique identifier to the user.”

110. It is my opinion that Doughty and van Boucq fail to teach, either alone or in combination, these limitations.

111. In considering the above claim limitation I have considered the agreed-upon claim construction for each of the terms provided herein. Specifically, the agreed upon constructions provide that the term “determining that the user has not been assigned a unique identifier,” as recited in step 1[c], has been construed to mean that “a ‘unique identifier’ that was not previously assigned when it was previously determined that the user had opted out of location tracking.”

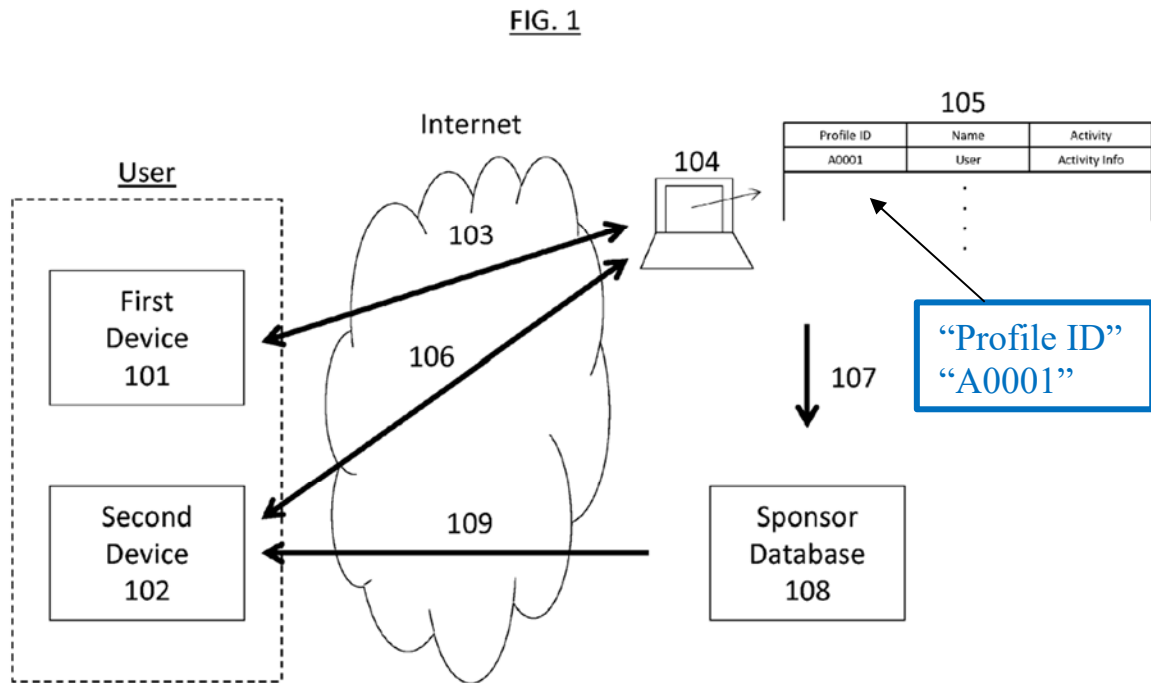
112. Claim 1 recites a particular way of assigning a unique identifier—making a determination that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device—and assigning that same unique identifier based on the lack of stored location data. In my opinion, these limitations are not taught by or rendered obvious by either Doughty and/or van

Boucq because neither teaches or suggests making the claimed determination “based on a lack of stored location data for the user computing device” and assigning the unique identifier that was determined not to be assigned.

8.1.1.1 Doughty

113. In my opinion, Doughty does not disclose limitations 1[c] and 1[d]. In its Profile ID Embodiment, Doughty explains with reference to Figures 1 and 2 that “[u]pon receiving the user’s activity information, server 104 assigns a unique identifier” (Ex. 1008, 10:45-47; *see supra* §7.1). Doughty shows the assignment of a unique identifier as “Profile ID” “A0001” in Figure 1, reproduced below (Ex-1008, Fig. 1).

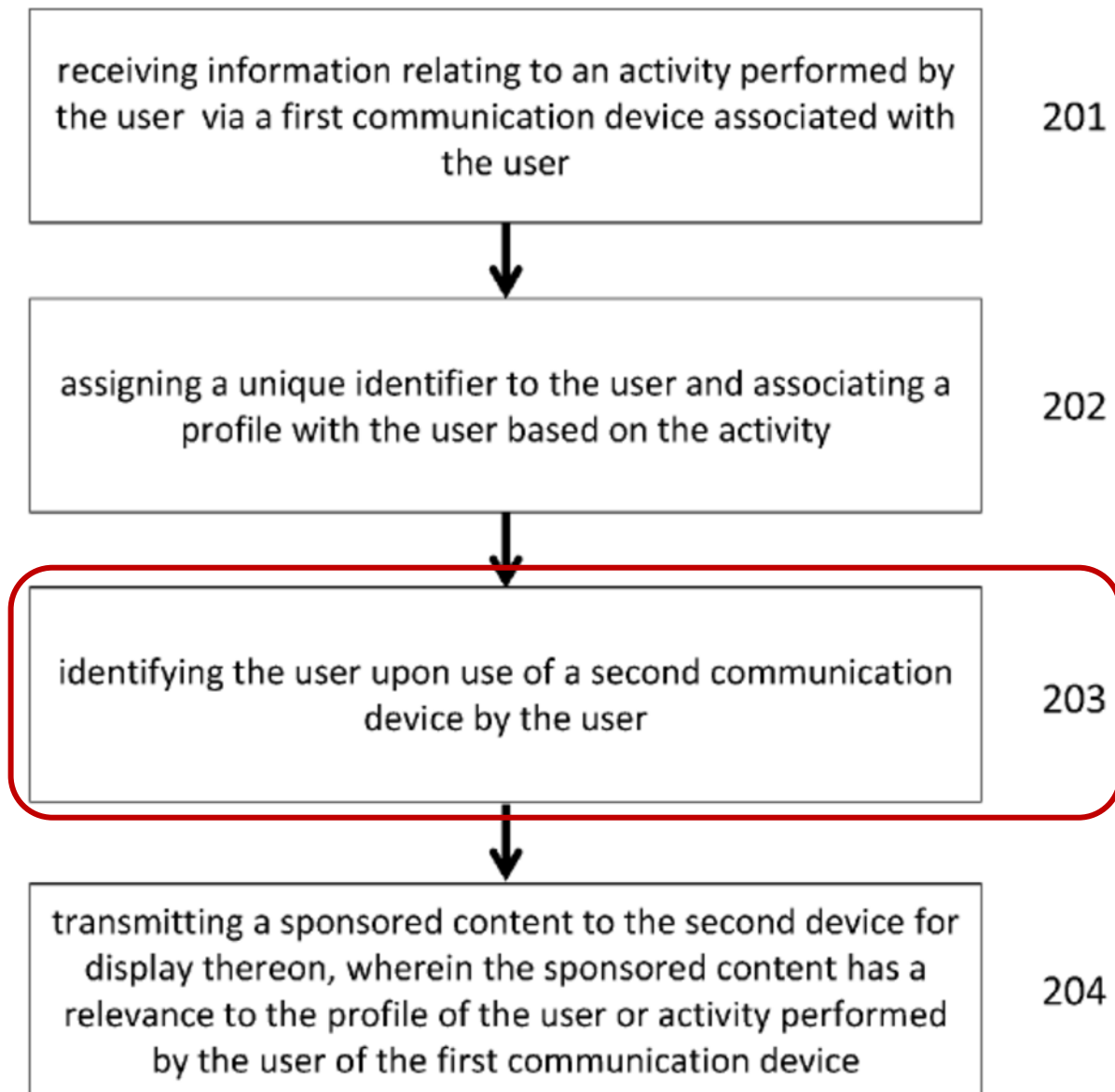
Doughty Fig. 1 (Ex-1008) (Annotated)



114. Doughty also teaches that server 104 may “identify the second device 102” as being used by the same user (Ex-1008, 10:54-56, Fig. 2).

Doughty Fig. 2 (Ex-1008) (Annotated)

FIG. 2



115. With reference to Figures 3-8, Doughty teaches different embodiments for determining that two devices are used by the same user (*e.g.*, profiles, user managed assets, & use patterns) and creating a “universal profile” to correlate those two devices so that advertisers can use data from the two devices to select

advertisements to send to the user (Ex-1008, Figs. 3-8). Doughty does not disclose making the claimed “determination that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device” and assigning the unique identifier when this determination is made.

116. In Doughty’s MKP Embodiment, the advertising network assigns an advertising network ID based on receiving communications from a user device (*see supra* §7.1; Ex-1008, 16:39-17:24). Likewise for this embodiment, Doughty does not disclose making the claimed “determination that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device” and assigning the unique identifier when this determination is made.

117. Petitioner states “Doughty discloses this limitation,” citing to Doughty’s disclosure that “[u]pon receiving the user’s activity information, server 104 assigns a unique identifier” (in the Profile ID Embodiment) and creating of a unique identifier by creating a hashed email address (in the MKP Embodiment) (Petition 27, citing Ex-1008, 10:45-47; 17:28-32). I disagree. Doughty’s assigning a unique identifier upon receiving user activity information and creating a hashed email address are not “assigning the unique identifier to the user” as claimed because the claim does not merely claim assigning any unique identifier. Rather, the antecedent for “the unique identifier” in limitation 1[c] requires that the assigned unique identifier was determined not to be assigned “based on a lack of stored

location data for the user computing device” (Ex-1001, 47:54-57). There is no teaching or suggestion that Doughty’s Profile ID and hashed email are related to any determination based on a lack of stored location data for the user computing device, as the identifiers in Doughty that Petitioner has mapped to the “unique identifier” are based upon receipt of user activity information or creating a hashed email address. Thus, Doughty does not disclose limitation 1[c] or 1[d].

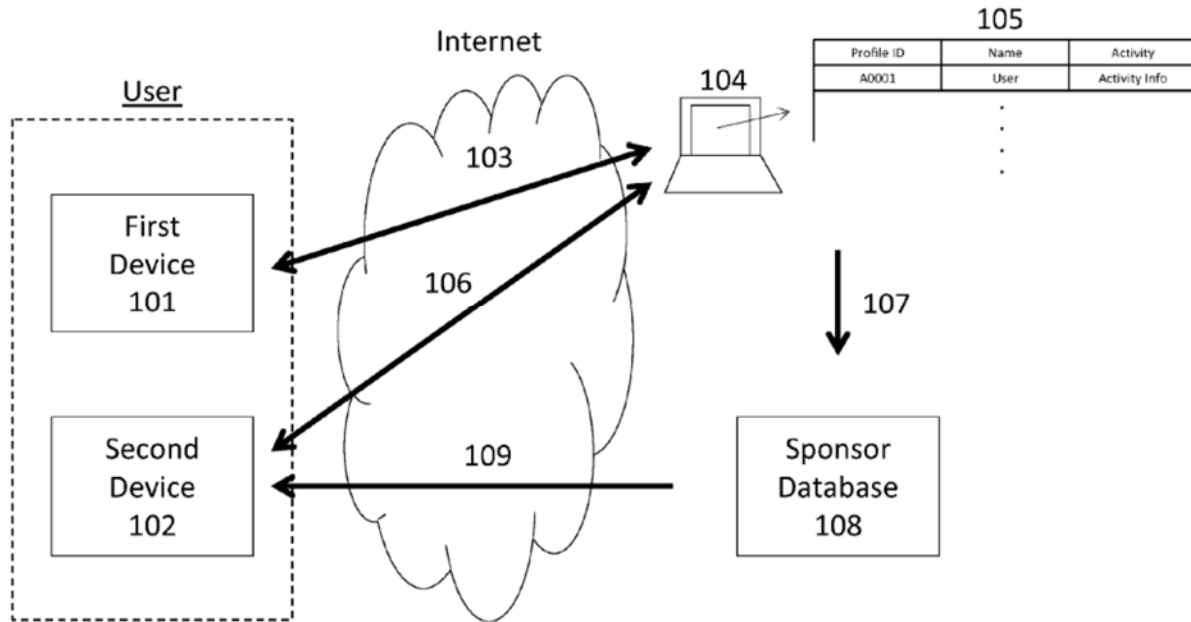
118. Mr. Williams includes two alternative obviousness theories for limitation 1[c] (Ex-1007, ¶¶146-151).

119. Mr. Williams first asserts that it “would have been obvious to a POSA that, to check if the user has been assigned a unique identifier, the system would check the user’s computing device for a cookie or other tracking mechanism” and “[i]f the user already had a unique identifier, there would already be a cookie or other tracking mechanism on the user’s computer in the local browser cache” (Ex-1007, ¶148). Mr. Williams then asserts that cookies “typically contained location data” (Ex-1007, ¶¶148-149). Petitioner contends that a “POSA would have been motivated to check for a previously determined location because one of the purposes of the system of Doughty is to consolidate all information about the user in a user profile” (Petition, pp. 24-25; Ex-1007, ¶¶ 149-151). Petitioner concludes that “when Doughty’s system determines a profile does not exist,” it is “based on a lack of stored location data for the user computing device” (Petition, p. 25).

120. The reliance on checking for a cookie or other tracking mechanisms in the browser to allegedly teach limitation 1[c] is incorrect because it rests on an unclaimed embodiment of the recited determination. The '947 Patent specification describes a technique of checking for a cookie or other location tracker for determining that the user has not been assigned a unique identifier (*See, e.g.*, Ex-1001, 9:55-59, 39:30-41, 43:59-44:4). For example, the '947 Patent describes that “the computing device may determine whether there is a unique identifier for associated with the user based on presence of a location tracker (e.g., cookie) installed in the browser application on the user computing device” (Ex-1001, 9:55-59, 39:30-34, 43:59-63). This is only one of the embodiments the '947 Patent discloses for making the recited determination, however, and it is explicitly described as an “additional[]” or “alternative[]” technique (Ex-1001, 9:55, 39:30, 43:59). In another embodiment, the '947 Patent explains that the “computing device may determine that there is no unique identifier associated with the user computing device when there is no location data stored for the user computing device” (Ex-1001, 9:49-52, 39:23-26, 43:52-55). For this embodiment, “the computing device may access a database or other storage location that maintains a mapping of unique identifier to a browser session, a user computing device, and/or location data” (Ex-1001, 9:52-55, 39:26-30, 43:55-59). Limitation 1[c] is directed to the second

technique described above, and not to the alternative technique of looking for a cookie or other location tracker.

121. Mr. Williams' and Petitioner's theories do not follow from Doughty's teachings. Doughty teaches assigning a unique identifier in the form of a "Profile ID" (e.g., A001) based on receipt of user activity information that is saved in "table 105" at the remote server (as shown in Doughty's Fig. 1, reproduced below; *see also* Ex-1008, Figs. 3, 5, 7, 9). I am unaware of any teaching or suggestion in the record that Doughty's Profile ID or advertising network ID is stored at the user computing device, much less in a cookie at the user computing device. Doughty's Profile ID is saved at the remote server, and is used to link together all of a user's devices. I disagree with the theory that it would be obvious in view of Doughty to check for a cookie on a user computing device because Doughty's Profile ID is not saved on any user computing device. That is, determining whether a Profile ID has been assigned requires checking Doughty's table 105 at the server. I am unaware of any teaching or suggestion in the record of determining that a server-based Profile ID has not been assigned based on information stored at an individual user device. Accordingly, in my opinion, a POSITA would not consider it obvious to look for stored location data in a cookie that does not have Doughty's saved Profile ID. In my opinion, A POSITA would not be motivated to look for Doughty's identifier in a place where Doughty's identifier is not saved.

Doughty Fig. 1 (Ex-1008)

122. Mr. Williams opines that Doughty’s system determines that a profile does not exist “based on the ‘lack of stored location data for the user computing device’” (Ex-1007, ¶151). It is not entirely clear what disclosures Mr. Williams is relying on. To the extent that Mr. Williams is opining that it would have been obvious to check table 105 on Doughty’s server 104 for a lack of stored location data, and to conclude from the lack of stored location data in table 105 that a unique identifier has not been assigned, I disagree. There is no teaching of the recited determination in Doughty, and this purported modification of Doughty is contrary to Doughty’s teachings. Doughty’s profiles do not necessarily include location data, and can in some cases store only other types of data such as a “behavioral pattern, viewing habits, usage information, duration on each application, geographic location

information, proximity to other locations,” etc. (Ex-1008, 10:36-39). In my opinion, A POSITA thus would not be motivated to modify Doughty to make the recited determination because it would not work—for a profile with no location data, it would result in an incorrect determination that no unique identifier exists.

8.1.1.2 Van Boucq

123. In my opinion, van Boucq does not teach, suggest, or render obvious limitations 1[c] and 1[d].

124. Petitioner alternatively asserts that limitation 1[c] is obvious over van Boucq (Petition 25-26; Ex-1007, ¶¶152-53) while still relying on Doughty for teaching limitation 1[d]. Mr. Williams opines that “Van Boucq discloses that the system can determine whether the user has a profile and unique ID by checking if the internet user already has a geolocation cookie on the computing device (Ex-1007, ¶ 152, citing Ex-1009, ¶ [0060]). I disagree.

125. **van Boucq’s Cookie Check:** The theory advanced by Petitioner and Mr. Williams again relies on an unclaimed embodiment of the determination recited in limitation 1[c]. As explained above, the ’947 Patent describes two embodiments of the recited determination: one based on the lack of “location data stored for the user computing device” (Ex-1001, 9:49-52, 39:23-26, 43:52-55), and another based on “presence of a location tracker (e.g., cookie) installed in the browser application on the user computing device” (Ex-1001, 9:55-59, 39:30-41, 43:59-44:4).

126. As limitation 1[c] is directed to the first disclosed technique of “determining that the user has not been assigned a unique identifier based on a lack of stored location data for the user computing device,” and not the alternatively disclosed technique of looking for a cookie installed in a browser application on the user computing device, limitation 1[c] cannot be rendered obvious in view of a teaching of the unclaimed alternative embodiment. and not the alternatively disclosed technique of looking for a cookie installed in a browser application on the user computing device, limitation 1[c] cannot be rendered obvious in view of a teaching of the unclaimed alternative embodiment.

127. Van Boucq’s cookie check determines whether the Internet user already has a connection cookie, which makes it possible to determine whether the geolocation of said Internet user has already been stored in a browsing device (Ex-1009, [0060], [0063]). A positive determination that a cookie was assigned (assuming van Boucq’s cookie has a unique identifier) is not determining that a unique identifier was not assigned, much less making the not-assigned determination as claimed. A positive determination is not a negative determination. Claim 1 recites determining an identifier was not assigned, not was assigned.

128. Even assuming van Boucq’s cookie has a unique identifier, van Boucq’s determining that the connection cookie is not present does not teach or suggest limitation 1[c]. Van Boucq’s cookie check determines that the cookie is not

present and concludes from the lack of a cookie that no identifier was assigned (Ex-1009, [0060], [0063]). Limitation 1[c], however, does not recite looking for a unique identifier and concluding from the lack of a unique identifier that no unique identifier was assigned. Claim 1 goes a step further because the claims are directed to the issue of receiving “anonymous data” (Ex-1001, 47:45). Because the data is anonymous, limitation 1[c] makes the claimed determination by using the “lack of stored location data for the user computing device” (Ex-1001, 47:54-56). As the claim recites, if there is a lack of stored location data for the user, the location data cannot be used to determine the user’s assigned unique identifier. Thus, the claim considers whether stored location data can be used to determine the user’s unique identifier.

129. Van Boucq’s cookie check does not teach or suggest limitation 1[c]. For example, if the van Boucq user cleared cookies, van Boucq’s cookie check would conclude that no unique identifier had been assigned, which may be incorrect. Given Petitioner’s reliance on various server-side identifiers as the recited “unique identifier, including Doughty’s Profile ID and hashed email address, the presence or absence of a device-side cookie will not allow the system to determine whether the server-side unique ID has been assigned (*see supra* ¶121). Van Boucq does not teach or suggest what is claimed—looking to see if there is stored location data in van Boucq’s system for the user that is mapped to a previously assigned unique identifier

and assigning a unique identifier if there is no stored location data (*see, e.g.*, Ex-1001, 9:52-55, 39:26-30, 43:55-59).

130. **Van Boucq’s Pop-Up:** Van Boucq teaches that if van Boucq’s cookie check is negative, “the Web browser will send a pop-up (message) 270 asking the user if he/she wishes to be geolocated” (Ex-1009, ¶¶[0063], [0068]). Regardless of whether the user answers the pop-up yes or no, van Boucq creates a connection cookie (Ex-1009, [0068]). Van Boucq’s pop-up process is determining an answer to a question and assigning a cookie, not making the claimed determination based on the lack of location data and assignment based on that determination.

8.1.1.3 Doughty + van Boucq

131. I disagree with Petitioner’s combination of van Boucq for limitation 1[c] with Doughty for limitation 1[d]. Petitioner asserts that limitation 1[d] is satisfied by Doughty assigning a Profile ID in table 105 at the remote server or by creating a hashed email address. (Petition 27; Ex-1007, ¶156). Van Boucq’s “connection cookie” has neither Doughty’s unique identifier from table 105 nor Doughty’s hashed email address. Nothing in the record suggests that van Boucq’s connection cookie could contain any information about either Doughty’s table 105 Profile ID or Doughty’s hashed email address. Accordingly, there is no motivation for a POSITA to combine the teachings of Doughty and van Boucq in such a way as to arrive at limitations 1[c] and 1[d].

8.1.2. 1[e]: “determining whether the user opted-in to or out of location tracking, based on whether a location tracker is installed on the user computing device;”

132. It is my opinion that Doughty and van Boucq fail to teach, either alone or in combination, this limitation.

133. Petitioner asserts that limitation 1[e] is obvious over Doughty alone or Doughty in view of van Boucq (Petition, p. 28, Ex-1007, ¶158). I disagree because neither reference discloses making the claimed determination based on “whether a location tracker is installed on the user computing device.”

8.1.2.1 Doughty

134. In my opinion, Doughty does not teach, suggest, or render obvious limitation 1[e]. I note that Mr. Williams states “I have not seen explicit disclosure in Doughty that explains how to determine if the user opted-out of location tracking” (Ex-1007, ¶159; see Petition, pp. 28-29). Instead, Petitioner argues that limitation 1[e] is obvious over Doughty because Doughty supposedly recognizes that “users can turn off browser cookies” and a POSITA would understand that: (i) Doughty “contemplates location tracking without cookies,” (ii) “location tracking is important to profile consolidation,” and (iii) the importance of determining location if a user opted out of sharing location data (Petition, pp. 28-29 (citing Ex-1007, ¶¶159-161 and Ex-1008, 17:24-27)). According to Mr. Williams, a POSITA would have found it obvious to “query the user’s browser to determine whether the user has allowed

location sharing” / “to see if third-party cookies have already been stored in the cache” (Petition, p. 29; Ex.-1007, ¶161). I disagree.

135. I disagree that “Doughty contemplates location tracking without cookies” (Ex-1007, ¶ 160). Mr. Willams cites Doughty’s recognition that a user can turn off browser’s cookies (Ex-1007, ¶ 160, citing Ex-1008, 17:23-26). But Doughty’s cited statement does not “contemplate location tracking without cookies.” Rather, Doughty’s cited statement recognizes that “turning off browser cookies, will prevent pixel tags from tracking the user’s activity” (Ex-1008, 17:23-26).

136. Recognizing that pixel tags cannot be used for tracking user activity is not “contemplating location tracking without cookies.” I am unaware of any teaching in Doughty of how to perform location tracking with cookies being turned off. Doughty simply does not address this issue. Rather than teach how to track the user’s activity without cookies, Doughty teaches essentially the opposite: that “turning off browser cookies, will prevent pixel tags from tracking the user’s activity” (Ex-1008, 17:23-26).

137. It is further my opinion that it would not be obvious over Doughty alone to query the browser “to determine whether the user opted in or out of location tracking, based on whether a location tracker is installed on the user computing device.” I am unaware of any teaching in Doughty of how to locate a user that opted out of location tracking. As Doughty fails to teach any such technique for locating

a user that opted out of location tracking, there is no reason to query the user to make the claimed determination based on Doughty.

138. It is further my opinion that limitation 1[e] is not obvious over Doughty's recognition that a user can turn off browser's cookies because Doughty's statement regarding turning off browser cookies is made in the context of Doughty's MKP Embodiment, and the user device processing pixel tags to be able to send previously set cookie values to the advertising network (Ex-1008, 16:62-65, 17:16-26). The pixel tag can be used by a third-party—the advertising network—to monitor user activity (Ex-1008, 17:20-22). Doughty recognizes that “turning off browser cookies, will prevent pixel tags from tracking the user's activity” (Ex-1008, 17:23-25). With cookies off, the HTML code for the pixel tag will be unable to cause the user device to return previously set cookie values. Rather than suggesting to query the user's browser to make the claimed determination when cookies are disabled, Doughty teaches that to identify the anonymous user with a hashed email to facilitate communication between the advertising network and the user device (Ex-1008, 17:50-51). In fact, Doughty's pixel tag embodiment is not concerned with tracking user location at all. Thus, in my opinion, a POSITA would not jump from Doughty's disclosure to the claimed invention.

8.1.2.2 Van Boucq

139. In my opinion, van Boucq does not teach, suggest, or render obvious limitation 1[e] because van Boucq does not disclose making the claimed determination “based on whether a location tracker is installed on the user computing device.”

140. Petitioner has identified the same disclosure in van Boucq, of checking for a cookie on a computing device, as teaching both limitations 1[c] and 1[e]. Petitioner argues, “Van Boucq explains that the determination of whether or not the user has a profile and unique ID may be done by checking if the Internet user already has a geolocation cookie on the computing device” (Petition, pp. 25-26). Petitioner then argues, with regard to limitation 1[e], that “it would have been obvious to a POSITA that checking for this cookie would have been an efficient means of determining whether the user opted-out of location tracking” (Petition, p. 31). Petitioner has thus identified checking for the same cookie as teaching both limitations 1[c] and 1[e].

141. It is further my opinion that van Boucq does not disclose the claimed “location tracker.” Van Boucq is silent regarding location tracking, and therefore does not disclose a “location tracker.” What van Boucq discloses is determining a single location on an initial connection of a computing device with the system and saving that location in a user “browsing device” via a connection cookie (Ex-1009,

¶¶[0060], [0063]). Because van Boucq's location is sent to the user when geolocation is performed on the initial connection with the system (*e.g.*, Ex-1009, ¶¶[0067]-[0068]), the location is static, the user location is not tracked, and van Boucq's "cookie" is not a "location tacker." Van Boucq later looks for the connection cookie, which "makes it possible to determine whether the geolocation of said Internet user has already been stored in a browsing device" (Ex.1009, ¶ [0063]). Thus, if the geolocation has already been performed upon the initial connection of the computing device with the system and is stored in a connection cookie, van Boucq uses that geolocation for advertisements (Ex-1009, ¶ [0060]). Thus, van Boucq uses a static predetermined location that the servers do not change. If the user moves, the stored geolocation remains the same because van Boucq wants to provide the user advertisements associated with that location (*e.g.*, the presumed user's home).

142. Even assuming van Boucq's "connection cookie," could be considered the claimed "location tracker," it is further my opinion that van Boucq does not teach or suggest the claimed "determination" because van Boucq installs a connection cookie after seeking consent using a pop up regardless of whether the user responds to or ignores the pop-up (Ex-10009, ¶¶[0063], [0068], [0069]). Accordingly, van Boucq's determination of whether the "connection cookie" is present indicates that the user either agreed to the pop up, declined the pop-up, or ignored the pop-up and

provides no determination of opting in or out. The presence of the connection cookie could be based on any of the three conditions. Accordingly, the presence of van Boucq's connection cookie is not a determination of whether the user opted in or out of location tracking.

143. The only thing that can be inferred from the absence of van Boucq's "connection cookie" is that the user was not provided a connection cookie. As van Boucq provides a connection cookie regardless of opting in or opting out, the absence of a cookie means that the user was never connected to the service, the user cleared cookies, or the user disabled cookies. But the absence of a cookie as taught by van Boucq cannot be used to make a determination of opting in or out.

8.1.2.3 Doughty + van Boucq

144. Petitioner argues that Doughty's teaching that users can "turn off browser cookies" and of "location tracking without cookies" would motivate a POSITA to "find an alternative means of locating the user" (Petition 28-29). The Petitioner then cites portions of van Boucq that teach the "creation of a cookie" to store location (Petition 29-31 (citing Ex-1009, ¶[0063])).

145. The proposed combination and modification is thus inconsistent with and contradicted by the purported motivation. If the motivation is to look for a solution where cookies are not available, a POSITA would not have been motivated to combine Doughty with a reference that relies on cookies. Those cookies would

not be usable because the motivation states that cookies are disabled. Each of the three “approach[es]” taught by van Boucq requires checking for a “cookie (connection cookie)” (Ex-1009, ¶¶[0060], [0063], [0067]) and/or the “creation of a cookie” (Ex-1009, ¶¶[0063], [0068]) in the user’s browser. There is no teaching in van Boucq of any technique that does not require cookies, or that would work when the user has turned off cookies. A POSITA looking for a non-cookie solution would not look to a cookie reference like van Boucq. Van Boucq’s cookies could not be used because cookies were turned off by the user.

146. It is further my opinion that a POSITA would not have been motivated to modify Doughty, with or without van Boucq, to arrive at limitation 1[e] because Doughty fails to discuss geolocating a user that opted out of location tracking. Doughty merely states the possibility that cookies may be disabled, and explains that this would “prevent pixel tags from tracking the user’s activity” (Ex-1008, 17:24-26). Doughty makes no mention of users opting in or out, who might turn off cookies, how, or why. It is thus my opinion that Doughty does not teach or suggest the concept of user opting in to or out of location tracking, or of tracking the user in the event of an opt out. Nor does Doughty disclose any way of doing so. Doughty thus fails to include any teaching or suggestion that might lead a POSITA to modify Doughty, with or without van Boucq, to arrive at limitation 1[e].

8.1.3. 1[f]: “sending, upon determining that the user opted-out of location tracking, the unique identifier to the user computing device for storage in a local browser cache;”

147. It is my opinion that Doughty and van Boucq fail to teach, either alone or in combination, this limitation.

148. Petitioner’s only theory for limitation 1[f] is that the limitation is obvious over Doughty and van Boucq in combination (Petition 31; Ex-1007, ¶165). Petitioner and Mr. Williams posit three obviousness theories, one based on sending a cookie with a unique identifier, one based on sending a pixel tag with a unique identifier, and one based on sending an unidentified “other tracking mechanism” with a unique identifier. I disagree with each of these theories, as explained below.

8.1.3.1 “Cookies” versus “storage in local browser cache”

149. In my opinion, Petitioner’s obviousness theory based on sending a cookie with a unique identifier does not establish obviousness of limitation 1[f] because neither Doughty nor van Boucq teaches or suggests sending a cookie “for storage in a local browser cache.” According to Petitioner and Mr. Williams, a POSITA “would know that cookies...are stored in the user’s ‘local browser cache’” (Petition 31; Ex-1007, ¶166). I disagree.

150. A POSITA would have understood that cookies, as taught by Doughty and van Boucq, are sent for storage in a dedicated storage area of the web browser referred to in the relevant standard as the “cookie store.” For example, RFC 6265,

which has been the standard for browser cookies since 2011, provides that after receiving a cookie from a web server and performing required processing, the browser must “[i]nset the newly created cookie into the cookie store” (Ex-2014, 21-24). When later sending stored cookies to web servers, the browser must use a specified algorithm based on “the set of cookies from the cookie store” (*see, e.g.*, Ex-2014, 25). The standard further encourages web browser developers to support certain minimum size and volumes of cookies in the cookie store (Ex-2014, 27), and to include “mechanism for managing the cookies stored in the cookie store” (Ex-2014, 28-29). In some older implementations, such as Netscape Navigator, cookies were stored in a text file, “COOKIE.TXT” as referenced by Mr. Williams. (See EX-1007, ¶ 60 (citing Ex-1045, 2)). Many browsers have since moved to more sophisticated storage mechanisms, such as databases (*see* Ex-1013, 17 (noting browsers “should probably be cautious about using files to store cookies long-term”))). Modern browsers thus keep their cookies in a dedicated cookie store.

151. A POSITA would not have understood that cookies, as disclosed by van Boucq and Doughty, are sent for storage in local browser cache. A POSITA would have understood that the local browser cache is a separate mechanism from the cookie store that has a different purpose, different function, and different standard. According to the relevant standard, RFC 9111, an “HTTP ‘cache’ is a local store of response messages and the subsystem that controls storage, retrieval, and deletion of

messages in it” (Ex-2016, 4; Ex-2020, 4). The purpose of the cache is to “reduce the response time and network bandwidth consumption on future equivalent requests” (Ex-2016, 4; Ex-2020, 4). Put another way, the “goal of HTTP caching is significantly improving performance by reusing a prior response message to satisfy a current request” (Ex-2016, 5; Ex-2020, 4). The core function of cache is to allow the web browser to load a web page faster by “reusing a prior response” from the web server (Ex-2016, 5; Ex-2020, 4). The purpose of cookies, by contrast, is to allow web servers to “store state (called cookies) at HTTP user agents [e.g. browsers], letting the servers maintain a stateful session over the mostly stateless HTTP protocol” (Ex-2014, 1.) The cache standard does not include any provision for sending cached content back to the server. The core function of cookies, by contrast, is that the cookies may be sent back to the server on a subsequent visit to the same website (*see, e.g.*, Ex-2014, 6 (describing “a way for an origin server to send state information to a user agent [e.g. browser] and for the user agent to return the state information to the origin server”))).

152. A POSITA would have understood that yet another distinction between cookies, as taught by Doughty and van Boucq, and browser cache is in the facilities that a web browser provides for user management of cache and cookies. For example, most web browsers offer the ability to clear the cache of the browser. Clearing the cache of the browser, however, will not clear the cookie store. Similarly,

most browsers offer the option to clear some or all cookies. Doing so, however, will not also clear the browser cache (*see supra* ¶69). This further reinforces that cookies and cache have separate storage and separate management.

153. Further evidence shows that a POSITA would have understood that cookies, as taught by Doughty and van Boucq, and browser cache are distinct and separate mechanisms in the context of online advertising and user tracking. For example, a 2015 paper provides a survey of “the existing literature on the methods currently used by web services to track the user online” (Ex-1012, 1). “HTTP cookies” is but one of the many tracking mechanisms discussed in this paper, while several others relate to cache (Ex-1012, 3 (Table I summarizing mechanisms)). This paper places HTTP cookies under the broader category of “storage-based tracking mechanisms” (Ex-1012, 5) while also including a separate category of “cache-based tracking mechanisms” (Ex-1012, 7). This paper thus further confirms that a POSITA would not have understood that cookies are sent for storage in local browser cache.

154. Consistent with a POSITA’s understanding, the ’947 Patent recognizes and relies upon the distinction between cookie storage and the local browser cache, as illustrated in Figures 5, 15, and 16 of the ’947 Patent. For example, ’947 Patent Figure 16 depicts separate operations for “[i]nstall cookie in browser” 512 and “[s]tore unique ID in local cache of browser” 514, as shown in the figure reproduced below.

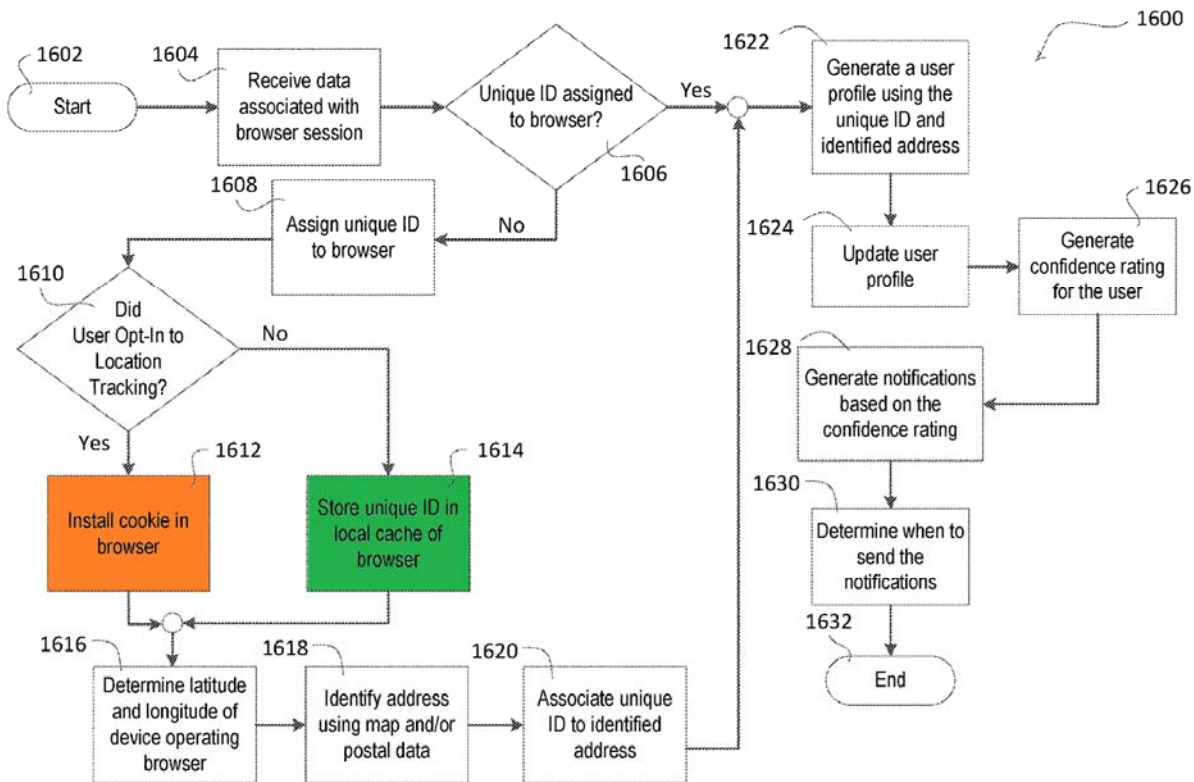
'947 Patent, Fig. 16 (Annotated)

FIG. 16

155. The '947 Patent describes the “cookie” of step 1612 as a “tracking cookie, browser cookie, HTTP cookie, etc.” ('947 Patent 44:31-35). A POSITA would have understood that the reference to “install cookie in browser” could include, for example, setting a cookie according to RFC 6265, discussed above. The '947 Patent explains that the “unique ID may be stored in the local browser cache, for example, even if the user computing device does not allow cookies (e.g., full cookies)” (Ex-1001, 44:62-64). A POSITA would have understood that the reference to the “local cache of browser” in step 1614 could include for example a cache such as that described in RFC 9111, discussed above.

156. As both van Boucq and Doughty are cited for cookies but do not state where the cookies are stored, a POSITA reading both references would have understood that van Boucq's and Doughty's cookies are sent for storage in the cookie store, not in local browser cache, because the cookie store is the accepted place for storing cookies and the place where the cookie standard, RFC 6265, requires them to be stored. Neither van Boucq nor Doughty teach or suggest sending anything for storage in local browser cache, much less storage of a unique identifier.

8.1.3.2 “Sending upon determining”

157. Limitation 1[f] requires sending the unique identifier “upon determining that the user opted-out of location tracking.” Neither reference renders obvious this “sending upon determining” requirement because neither reference renders obvious the antecedent “determining whether the user opted-in to or out of location tracking” as recited in limitation 1[e] and as discussed above (*see supra* §8.1.2).

158. Mr. Williams opines that this limitation is obvious because van Boucq discloses sending a “connection cookie,” which he opines renders limitation 1[f] obvious (Ex. 1007, ¶165; *see* Petition 31-32). As described above, however, van Boucq's connection cookie is not sent based on the recited determination (*See supra* §8.1.2.2). Therefore, limitation 1[f] is not obvious over van Boucq.

159. To the extent Petitioner claims that limitation 1[f] is satisfied by Doughty teaching sending a pixel tag or “other tracking mechanism” / “similar files” with a unique identifier (Petition 32; Ex-1007, ¶166), I disagree. It is not clear what “unique identifier” Petitioner and Mr. Williams are mapping to this limitation. For example, Mr. Williams states that a “POSA would know that cookies and similar files (e.g., pixel tags)...would include the user’s unique identifier” (Ex-1007, ¶ 166). I am unaware of any teaching or suggestion in Doughty of any relevant unique identifier associated with Mr. Williams’ identification of “other tracking mechanism[s],” “pixel tags,” or “cookies and similar files.”

160. Regarding the pixel tag allegations, I am unaware of any teaching in Doughty of including any identifier in a pixel tag. Doughty’s pixel tags are described as “a transparent graphic image, usually no larger than one pixel by one pixel, placed on a webpage or in an email” (Ex-1008, 17:11-14). Doughty’s pixel tags rely on cookies (*see supra* §7.1). For example, Doughty teaches that a “publisher attaches a pixel associated with the advertising network that enables a cookie to be served” (Ex-1008, 16:63-65). Doughty further teaches that “Turning off the browser’s cookies will prevent pixel tags from tracking the user’s activity” (Ex-1008, 17:24-26). In that case, the “pixel tag will still account for an anonymous visit, but the user’s unique information will not be recorded” (Ex-1008, 17:26-27). Doughty’s pixel tag is thus a mechanism that may enable a server to send a cookie. Doughty

teaches that HTML code associated with the pixel tag can direct the user device to pass information such as the type of browser, user IP address, and previously set cookie values to the advertising network (Ex-1008, 17:16-20), but makes no mention of a unique identifier stored in the browser cache. Furthermore, Doughty does not teach or suggest using pixel tags to send a unique identifier to the user computing device based on the claimed determination of the user opting out of location tracking. Rather, Doughty teaches that the advertising network sends the pixel tag in response to a MKP communication with a user device, not based on the claimed determination (*see supra* §§7.1, 8.1.2, 8.1.2.1).

8.1.3.3 Same Unique Identifier

161. Limitation 1[f] requires “sending...the unique identifier to the user computing device.” The antecedent bases for “the unique identifier” are in limitations 1[c] and 1[d]. I am unaware of any teaching or suggestion in the record that the user identifiers that Petitioner identifies regarding limitations 1[c] and 1[d] would be the same identifiers that would be sent to the user device for limitation 1[f].

162. For limitation 1[c], Mr. Williams relies on Doughty’s Profile ID (Ex-1007, ¶147), and refers to unspecified identifiers associated with a pixel tag and unidentified “tacking mechanisms” (Ex-1007, ¶¶147-149). For limitation 1[d], Mr. Williams relies on the identifier for Doughty’s Profile ID as well as a hashed email

address (Ex-1007, ¶156). For limitation 1[f], Mr. Williams refers to unidentified unique identifiers associated with cookies, pixel tags, and unspecified “other tacking mechanisms” (Ex-1007, ¶156-166 (citing Ex-1008, 16:59-17:5)). I am unaware of any evidence to suggest that a POSITA would be motivated to modify the combined teachings of Doughty and van Boucq to instead use the same identifier for limitations 1[c], 1[d], and 1[f].

163. To the extent Mr. Williams relies on an unidentified and undefined identifier included in “cookies and similar files (e.g., pixel tags)” (Ex-1007, ¶166), I am unaware of any teaching or suggestion in the record of how or why a POSITA would have been motivated to configure this unidentified unique identifier to be the same “unique identifier” as that assigned per limitations 1[c] and [d] (See Ex-1007, ¶¶165-67), particularly given Doughty’s disclosure of different systems (*i.e.*, a publisher and advertising network) for sending the different types of identifiers (e.g., “cookies and similar files (e.g., pixel tags)”) for different purposes (Ex-1008, 16:59-65).

8.1.4. 1[l]: “identifying a second visit to the URL during the second browser session using the unique identifier stored in the local browser cache”

164. It is my opinion that Doughty and van Boucq fail to teach, either alone or in combination, this limitation.

165. Petitioner relies on Doughty for this limitation (Petition, pp. 39-40).

166. As explained above regarding limitation 1[f], neither Doughty nor van Boucq teaches, suggests, or renders obvious “sending . . . the unique identifier to the user computing device for storage in a local browser cache.” Without sending the unique identifier for storage in the local browser cache, Doughty’s system cannot then later rely on that unique identifier having been stored in the local browser cache to identify a second visit to the URL. Doughty does not teach or suggest using a unique identifier as recited in the claim.

167. Most of the distinctions discussed above regarding limitation 1[f] apply equally to limitation 1[l]. To summarize the relevant distinctions that are set forth more fully above regarding limitation 1[f]: (a) the cited cookies are not stored in local browser cache; (b) the cited “unique identifiers” are not sent to the user computing device upon the determination recited in limitation 1[e]; (b) Petitioner does not consistently identify the same universal identifier for each limitation that recites one; (c) Doughty’s pixel tags and “other mechanisms” do not send a unique identifier. For these same reasons, Doughty does not teach or suggest limitation 1[l].

168. Petitioner’s citation to Doughty concerns a back-end server linking saved universal profiles for two devices by comparing location information to the user behavior data (Petition 39-40). The portion of Doughty that either Petitioner or its expert cite for limitation 1[l] (Ex-1008, 6:19-25) does not teach or suggest any identification or tracking “using the unique identifier stored in the local browser

cache” as recited in limitation 1[l]. Rather, this citation to Doughty discusses the information that the system receives and saves from the user to evaluate user activity. (Ex-1008, 6:19-25.) This passage of Doughty does not teach or suggest any use of a unique identifier, much less during a second browsing session.

169. The only identifiers on which Petitioner relies—the profile identifiers stored in table 105 and those associated with “hashed email addresses” (Petition 27 (citing Ex-1008, 10:45-50, 17:28-32))—cannot satisfy limitation 1[l]. This limitation recites “the unique identifier,” and thus requires the same “unique identifier” that was previously sent to the user computing device, as recited in limitation 1[f]. Doughty’s system, however, focuses on linking multiple devices to the same user upon each device’s initial visit to a URL (Ex-1008, 11:37-39). Each user device would have a separate device identifier.

170. Finally, Petitioner contends in a single conclusory sentence that it would have been obvious “that the unique identifier of the user stored in the local browser cache would have been the mechanism for how two separate browsing sessions would be attributed to the same user” (Petition 40). The only support for this obviousness theory is a single, nearly-identical, conclusory sentence from Petitioner’s expert that provides no explanation or citation to the record (Ex-1007 ¶187). This testimony, however, is not supported by Doughty’s teachings, none of which involve storing a user unique identifier on the user device.

8.2. Claim 11

171. Claim 11 recites a “machine-readable storage device” with substantially similar limitations to the above-referenced method steps of claim 1. For at least the reasons stated in the above-referenced analysis of claim 1, the applied prior art references for Ground I fail to teach at least limitations 11[c], 11[d], 1[e], 11[f], and 11[l].

8.3. Claims 2-10 and 12-20

172. Claims 2-10 and 12-20 depend, directly or indirectly, from claim 1 or 11 respectively, and therefore are not obvious for the same reasons as set forth above at least due to their dependency from claim 1 or 11.

8.4. Secondary Considerations

173. I have not been asked to consider any secondary conditions of non-obviousness in rendering this opinion.

9. Ground II

174. Petitioner’s Ground II is a three-way obviousness combination based on Doughty, van Boucq, and Maginnis. The only difference between Ground I and Ground II is that Petitioner argues for Ground II that Maginnis discloses limitation 1[h] (Petition 57-58). Thus, adding Maginnis to the mix does not cure the deficiencies of the teachings of Doughty and van Boucq as explained in detail above regarding Ground I. Ground II fails to establish obviousness because neither

Doughty nor van Boucq teaches, suggests, or renders obvious at least limitations 1[c], 1[d], 1[e], 1[f] and 1[l], and because there is no motivation to combine the references in such a way as to form the claimed invention (*see supra* §8).

10. Use of Demonstratives

175. I reserve the right to make demonstratives (including product demonstrations, product usage, and videos thereof), charts, graphs, or other similar visual aids for trial based upon the opinions expressed in this declaration, the data contained in this declaration, the exhibits or other things cited in this declaration and/or attached as exhibits to this declaration.

Date: September 9, 2025



Dr. Oded Gottesman

Declaration of Dr. Oded Gottesman Regarding U.S. Patent No. 11,556,947

I, Oded Gottesman, do hereby declare and state, that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and may jeopardize the validity of the subject patent.

Executed on: September 9, 2025



Oded Gottesman