CONNECTICUT PUBLIC INTEREST LAW JOURNAL

VOLUME 14 FALL-WINTER 2014 NUMBER 1

Privacy Law in the Digital Age: Establishing Privacy Rights in Search Engine Logs

KURT YOUNG, JR. †

I. INTRODUCTION

Over the past decade search engines have become a common part of first-world-society life. It might be impossible for some to remember the last day they have not utilized Bing, Google, Yahoo, Vivisimo, or some other search engine. Yet with the advent of these convenient—and some would assert essential—navigators emerges a new frontier of privacy issues. Chief among these issues is whether the information provided to the search engine by the user is protected under the Fourth Amendment or the Stored Communications Act from unlawful search and seizure.[1] Currently, the state can obtain the information in search engine logs from service providers[2] without a warrant because the implicit agreement of the user to the terms of use agreement renders the information non-private.[3] Some search engine queries contain information the user wishes to maintain private, like medical questions or pornography. While the distinction between this type of information—the content information[4]—

† University of Connecticut School of Law, Juris Doctor Candidate, 2015. Quinnipiac University, B.S. Political Science, minors in Legal Studies and English Literature, 2012. I would like to thank my fellow members of the Connecticut Public Interest Law Journal and Professor Daniel Klau for their invaluable assistance editing this article. I would also like to thank my family for their love and unwavering support throughout my academic career. Lastly, I would like to dedicate this article to Krislyn Boggs, who inspires me every day to be better. I love you.

[1] *U.S. Const. amend* IV; 18 U.S.C. §§ 2701–12 (2012).

[2] In this context service providers refer to search engine hosts like Google, Yahoo, and Bing.

[3] Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 Berkeley Tech. L.J. 447, 451 (2007).

[4] According to the Stored Communications Act content information is meant to convey a subject of thought or discussion. If the search were a letter it would be the information found in the body of the letter in the envelope. Non-content information would normally be used to direct the sending of

and other information collected by service providers will be discussed later, it is the search queries which deserves the protection. While not forthcoming about the methodology by which they obtain and store data, search engines like Google collect user identifying information including the IP address and all search queries.[5] This information is then compiled into a running log of all search queries made from the user's computer.[6] Each log serves three purposes: (1) to document the computer's IP address and identifying information,[7] (2) to document the date and time of the query, and (3) to document the terms of the search query themselves.[8] With this log investigators could tell what search queries came from what computer and when, although the user on the computer may remain anonymous.[9] Search engines have no screening process to prevent collection, or to delete after collection, private or sensitive information collected as part of the search data log. The process is completely automated and collects all inputted entries.[10]

And not only are providers collecting all this data, they are keeping it for extended periods of time. Recent outcries from privacy groups have resulted in changes to the retention policies of the search engine logs.[11] Currently, major search engines like Google and Yahoo are maintaining possession of search logs for eighteen months before disassociating the data from the user and computer.[12] After the information has been disassociated, it can no longer be traced back to the user or computer, even if the government were to request it. However, the length of time the

---

information, (for example: a name, address, or phone number) like the information on the front of a mailing envelope. Omer Tene, *What Google Knows: Privacy and Internet Search Engines,* 2008 Utah L. Rev. 1433 (2008).

[5] Danny Sullivan, *Google Anonymizing Search Records to Maintain Privacy*, SEARCH ENGINE LAND, http://perma.cc/5DVR-LBF5 (last visited Aug. 28, 2014); "When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include: details of how you used our service, such as your search queries..." *Privacy Policy*, GOOGLE.COM, http://perma.cc/YTB6-T27T (last visited Sept. 2, 2014).

[6] Foley, *supra* note 5.

[7] An IP address is a unique identifying number for a computer or website that can be used to trace it. It is similar to a phone number for a cell-phone and is treated like such by the courts. *In re* Application of the United States of America for an Order Authorizing the Use of a Pen Register and trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F.Supp.2d 45, 48–49 (D. Mass. 2008).

[8] Sullivan, *supra* note 7.

[9] Although if the user is logged into an account with the search engine, like a Google Plus or email account, then the search could also be documented down to the individual user.

[10] "This includes information like your usage data and preferences, Gmail messages, G+ profile, photos, videos, **browsing history**, map searches, docs, or other Google-hosted content. Our **automated** systems analyze this information as it is sent and received and when it is stored." *"Collect Information"*,(emphasis added) GOOGLE.COM http://perma.cc/4YCC-MRF3 (last visited Sep. 24, 2014).

[11] Sullivan, *supra* note 7.

[12] *How Long Should Google Remember Searches?*, GOOGLE BLOG, http://perma.cc/8ZCD-E6TR (last visited Aug. 28, 2014); *Yahoo Data Storage and Anonymization FAQ*, YAHOO.COM, https://info.yahoo.com/privacy/us/yahoo/drfaq/ (last visited Aug. 28, 2014).

service provider keeps the information is merely a choice of the service providers, it is not mandated by law to protect privacy.[13]

One of the primary obstacles in researching this topic is the relative novelty of the preeminence of the internet in our lives. As a recent phenomenon there is little case law regarding search engine logs or privacy rights associated with them. As such, most of the information on the topic comes from the Department of Justice Computer and Intellectual Crime Manual[14] and Andrew William Bagley's article "Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, And Digital Papers and Effects," from 2011.[15]

The Department of Justice Computer and Intellectual Crime Manual is meant to unofficially advise individuals as to the government's position concerning their digital rights.[16] Most importantly, it states that the government believes that a person waives his subjective expectation of privacy when he agrees to a terms of use agreement that includes a provision of complying with law enforcement.[17] They believe that under such an agreement the user knowingly waives any expectation of privacy.[18]

Bagley's 2011 paper is the best scholarly overview of the current digital privacy laws.[19] It asserts that currently the courts agree with the government's perspective that the terms of use agreements are binding, even if the users were unaware of them.[20] He recommends that an understanding, similar to the confidentiality agreement proposal, be developed that the information collected can only be used internally unless the user specifically volunteers the information for third party uses.[21]

Part II of this article focuses on the current understanding of the privacy rights of users in their search queries. Part III argues that the 4th Amendment and, alternatively, the Stored Communications Act should provide protection for user search logs as unreasonable searches or as protected content information.

---

[13] Yahoo is a good example. For a period of time its retention of search logs was only ninety days. YAHOO, *supra* note 14.

[14] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, DEPARTMENT OF JUSTICE: COMPUTER CRIME AND INTELLECTUAL PROPERTY DIVISION, http://perma.cc/HL67-JZ27 (last visited Jan. 11, 2015).

[15] Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, And Digital Papers and Effects*, 21.1 ALB. L. J. SCI. & TECH. 153 (2011).

[16] *Id.* at 25–26.

[17] *Id.* at 26.

[18] *Id.*

[19] Bagley, *supra* note 17.

[20] *Id.* at 178–79.

[21] *Id.* at 179.

II. THE CURRENT INTERPRETATION OF THE USER'S PRIVACY RIGHTS IN THEIR SEARCH ENGINE QUERIES

Currently, there are no protections afforded user search engine logs under the 4th Amendment or Stored Communications Act.

In 1967 Justice Harlan outlined what would become the test for determining whether information should be afforded the protection of the 4th Amendment in his concurrence in *United States v. Katz*.[22] In *Katz*, the government had used evidence obtained by wiretapping a telephone booth without a warrant against the petitioner to convict him.[23] The court was asked to decide whether the conversation that the petitioner had over the phone, whilst in the telephone booth, was protected despite the fact that it was made in public.[24] The court developed a two prong test to determine if the telephone conversation should be protected under the Fourth Amendment.[25] First, was there a subjective expectation of privacy, and, second, was there an objective expectation of privacy.[26] Prior to this case the Court had reasoned that privacy rights were only implicated when the government trespassed upon an individual's property.[27] Justice Harlan's test was later adopted in *Smith* when the court held that the standard for Fourth Amendment protections was independent of the location of the conduct and, instead, hinged on the two prongs previously mentioned.[28]

The first prong of the adopted *Katz* privacy test, asks whether the person has an expectation that what he is saying, doing, or writing, is private.[29] It is a subjective standard, from the prospective of the individual, or in the case of search engine logs, the user.[30] To determine if the individual had a subjective expectation of privacy the court needs to look at the individual facts in each case that suggest that the individual had such an expectation of privacy and then use those facts to make an objective determination whether the showing is sufficient.[31]

However, the courts have asserted that search engine users automatically fail to meet this standard because the user knows his information is being shared. [32] If a user knowingly gives information,

---

[22] United States v. Katz, 389 U.S. 347, 361 (1967). (Concurring Opinion Adopted by: Smith v. Maryland, 442 U.S. 735, 740 (1979).

[23] *Id.* at 348–50.

[24] *Id.* at 349.

[25] *Id.* at 361.

[26] *Id.*

[27] *Id.* at 350.

[28] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[29] *Katz*, 389 U.S. at 361. (Concurring Opinion Adopted by: Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[30] Bagley, *supra* note 17, at 171.

[31] State v. Brown, 198 Conn. 348, 356, 364 (1986).

[32] Schuyler Sorosky, *United States v. Forrester: An Unwarranted Narrowing Of The Fourth Amendment*, 41 LOY. L. A. L. REV. 1121, 1137 (2007–2008) (citing United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002)).

content or non-content, or knows that his activity is being monitored—like when at work—then he cannot have a subjective expectation of privacy in the information.[33] The court in *Forrester* held there is a presumption the user knowingly gives the service provider non-content information, like phone numbers dialed and IP addresses visited, because otherwise they could not expect the service provider to direct them to the telephone line or website.[34] The Supreme Court explained in *Smith*, in reference to telephone numbers recorded by the government, that while the user may expect his telephone conversation to be private, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[35] However, this presumption does not extend to content information, therefore, whether the user has knowledge that what he is doing is being shared or monitored remains an undecided and significant fact in determining the existence of a subjective expectation of privacy. Towards this end, other facts which speak to the user's state of mind regarding the information, like any efforts to keep it private and if he is at home, can be considered.[36]

Courts have reasoned that the existence of a terms of use agreement, which contains a privacy rights agreement, provide notice to the user that the content information provided the service provider is being recorded.[37] The current consensus among the courts is that the user agrees to the privacy rights agreements contained within "terms of use" agreements by utilizing the service provider, whether they know the terms of the agreement or not.[38] The court presumes that the user has read and understands the content of the agreement prior to use of the service provider.[39] In effect, this means that the user has waived his right to privacy in the information because an individual does not have a subjective right to privacy in information that he has knowingly consented to disclose.[40]

Service providers like Google specifically state in their agreements that you either must agree to all of the terms of the agreement or not use the service at all.[41] The terms outline the responsibilities of the user and serve as an expansive waiver of liability for Google.[42] Furthermore, the terms of use includes the privacy policy of all the Google services.[43] The privacy

---

[33] *Id.*

[34] United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).

[35] Smith v. Maryland, 442 US 735, 743 (1979).

[36] *See* Sorosky, *supra* note 34, at 1137.

[37] Bagley, *supra* note 17, at 178–79.

[38] *Id.*

[39] *Id.*

[40] United States v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007).

[41] *Google Terms of Service*, GOOGLE.COM, http://perma.cc/QHC5-F7Z5 (last visited Sept. 2, 2014).

[42] *Id.*

[43] *Id.*

policy states that Google collects all of the data submitted to it, that Google will share the gathered information, and for what purposes they will disclose it.[44] The terms of use states:

> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
>
> - meet any applicable law, regulation, legal process or enforceable governmental request.
> - enforce applicable Terms of Service, including investigation of potential violations.
> - detect, prevent, or otherwise address fraud, security or technical issues.
> - protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.[45]

This language is not unique to Google, it is similar to the language of other search engine providers as well.[46] Courts have found these terms of use and privacy agreements binding; even though the users did not participate in negotiating them and/or were aware of their existence.[47] Using the service is considered to be an agreement to the contract despite the possible lack of knowledge and lack of explicit consent and a waiver of the user's subjective expectation of privacy in the date.[48]

The second prong of the *Katz* privacy test is objective and independent of the user's thought processes.[49] The question asked is whether the information being held as private is something that the public is willing to accept as private.[50] In other words, is the public willing to accept information of that type, under those circumstances, as something which can reasonably be considered private? To reach this conclusion courts consider established principles in the appropriate areas of law, like in property law the right to exclude others from your property, as well as the current understandings of society and common sense.[51] It is not a bright-

---

[44] GOOGLE.COM, *supra* note 7 (stating that Google has the ability to collect everything the user inputs into its site); Bagley, *supra* note 17, at 174.

[45] GOOGLE.COM, *supra* note 7.

[46] See generally Bing Privacy Statement, Bing.com, http://perma.cc/8E7B-5W2F (last visited Sept. 2, 2014); Yahoo Privacy Center, Yahoo.com, http://info.yahoo.com/privacy/us/yahoo/details.html (last visited Sept. 2, 2014) (Yahoo is by-far the most forthcoming service provider. It provides a document detailing exactly why and when they must disclose user-information to the government.).

[47] Bagley, *supra* note 17, at 178–79. (Terms can still be found unconscionable if there are no reasonable market alternatives.)

[48] Tene, *supra* note 6, at 1469–70.

[49] Bagley, *supra* note 17, at 171.

[50] *Id.*

[51] Rakas v. Illinois, 439 U.S. 128, 143, n. 12, (1978).

line test, flexibility and discretion are available to the judge, but even so, this prong is rarely debated. It is meant to be a fail-safe to the first-prong and to maintain consistency with other areas of established law.[52] For example, even though a burglar might have a subjective expectation that his doings are being kept secret, that is not an interest the public is willing to accept as legitimate.[53] The flexibility also allows the *Katz* test to evolve as the public's expectations of privacy change.

The primary issue with respect to this objective expectation of privacy prong is the developed principle of the Third Party Disclosure Doctrine.[54] The Third Party Disclosure Doctrine states that a party has no subjective expectation of privacy in records information he discloses to a third party.[55] The public is not willing to accept that such records information disclosed to another can legitimately be held as private. In many ways the Third Party Disclosure Doctrine is similar to the analysis performed during the first prong analysis.

However, even if search engine logs do not qualify for 4th Amendment protection they may still be protected by the Stored Communications Act. In 1986, in response to wiretapping allegations, the Stored Communications Act was passed as part of the Electronic Communications Privacy Act.[56] It provides a baseline of protection for electronic data stored by electronic communications services (ECS) or remote computing services (RCS).[57] Search engine service providers are considered RCS providers because they provide a service separate from the sending and storing of communications. As such, this article will mostly focus on how the Stored Communications Act governs RCS providers instead of ECS providers.

The Stored Communications Act distinguishes between "content" and "non-content" information when discussing certain types of information. It is a classification based on what the common purpose of the information is. If the information would normally be used to direct the sending of information, (for example: a name, address, or phone number) like the information on the front of a mailing envelope, then it is non-content information.[58] If however, the information is meant to convey a subject of thought or discussion or, to continue the metaphor, is something that would be found in the body of the letter in the envelope, then it would be content

---

[52] *Id.*

[53] *Id.*

[54] Smith v. Maryland, 442 U.S.735 at 744 (1979).

[55] *Id.*

[56] Bagley, *supra* note 17, at 167.

[57] Electronic Communications Services (ECS) provide users with the ability to send and store communications like emails. Remote Computing Services (RCS) provide free processing services to the public, like search engines, and stores records.

[58] Tene, *supra* note 6, at 1478.

information.[59] Under the Stored Communications Act non-content information is afforded less protection under privacy laws then content information.[60]

For RCS the Stored Communication Act sets restrictions and requirements for when the service provider can voluntarily release user information.[61] Section 2702 restricts RCS providers from voluntarily releasing any content information collected from the user to anybody.[62] The statute also prohibits the service provider from voluntarily sharing non-content information with governmental entities.[63] There is one exception to this prohibition; if the remote service provider feels that there is an emergency that would result in death or serious harm if the information is not immediately disclosed it may share the information with the government.[64] Otherwise section 2702 offers protection from voluntary disclosure to the government of content and non-content information.

The SCA also restricts when a RCS must disclose the search logs, arguably content information, to the government upon request.[65] The government could compel disclosure through service of a search warrant to the service provider.[66] A warrant is obtained through the standard criminal procedures, thus requiring a finding of probable cause by a magistrate,[67] and is the one disclosure method under the SCA that does not require notice to the user.[68]

Alternatively, the government can use an administrative, trial, or grand jury subpoena to require the service provider to turn-over the content information.[69] Normally, this method requires that the government provide prior notice to the consumer of the request, however, this notice can be delayed up to ninety days if the notice would endanger someone or likely result in the destruction of evidence.[70] This subpoena method has no prior judicial branch supervision and is only required to meet a relevancy finding standard before being issued.[71] Due to the lower standard of proof required, the courts have allowed service providers to fight the subpoenas

---

[59] *Id.*

[60] *See* 18 U.S.C. § 2702–03 (2008).

[61] *Id.*

[62] 18 U.S.C. § 2702(a)(2)(A) (2008).

[63] 18 U.S.C. § 2702(a)(3) (2008).

[64] *Id.*

[65] 18 U.S.C. § 2703(b) (2008).

[66] 18 U.S.C. § 2703(b)(1)(A) (2008).

[67] The SCA also restricts how the government can compel a RCS to provide the search logs. One way is for the government to serve a search warrant to the RCS. 18 U.S.C. § 2703(b)(1)(A) (2008).

[68] *Id.*

[69] 18 U.S.C. § 2703(b)(1)(B)(i) (2008).

[70] 18 U.S.C. § 2703(b)(1)(B)(i) (2008); Foley, *supra* note 9, at 474; 18 U.S.C. § 2705(a)(4) (2008); 18 U.S.C. § 2705(a)(1)(B) (2008).

[71] Foley, *supra* note 5, at 453.

on undue hardship and difficulty grounds.[72] Notably absent from the list of subpoenas allowed is the pre-trial subpoena. As such, since the government must use a normal, instead of a pre-trial, subpoena to request content information protected under the Stored Communications Act from

a RCS provider there must already have been court action—so other threshold standards have likely already been met.

Lastly, the government may use a court order to compel disclosure of content or non-content information held by a RCS.[73] A court order does not require probable cause instead, the government need only show specific and articulable facts which indicate that the content is relevant to an ongoing criminal investigation.[74] The court order procedure follows the same notice rules as the subpoenas, and likewise, can also be delayed up to ninety days.[75]

III. SEARCH ENGINE LOGS SHOULD BE GIVEN PROTECTION EITHER UNDER THE 4TH AMENDMENT OR THE STORED COMMUNICATIONS ACT

A. Katz Analysis

As previously noted, *Katz* provides a two part analysis in determining whether a type of information should be given protection under the 4th Amendment as private information. The two prongs consist of (1) whether the user has a subjective expectation of privacy, and (2) whether the expectation of privacy is objectively reasonable.

1. The Subjective Expectation of the User

As mentioned above, to determine whether an individual has a subjective expectation of privacy the court looks to any actions or facts which illustrate whether the individual believes the information in question is being kept private.[76] Important in this examination is whether the user has any knowledge that the information is being monitored or shared.[77] If so, then the user is assumed to know that the information is not being kept private and he has no expectation of privacy in the information.[78]

---

[72] Gonzales v. Google, Inc., 234 F.R.D. 674, 680 (N.D. Cal. 2006).

[73] 18 U.S.C. § 2703(b)(1)(B)(ii) (2008).

[74] 18 U.S.C. § 2703(d) (2008).

[75] 18 U.S.C. § 2703(b)(1)(B)(ii) (2008); Foley, *supra* note 5, at 474; 18 U.S.C. §2705(a)(4) (2008); 18 U.S.C. § 2705(a)(1)(B) (2008).

[76] United States v. Katz, 389 U.S. 347, 361 (1967). (Concurring Opinion Adopted by: Smith v. Maryland, 442 U.S. 735, 740 (1979)).

[77] Sorosky, *supra* note 34, at 1137 (citing United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002)).

[78] *Id.*

Otherwise, if the user believes the information is being kept private, then he has a subjective expectation of privacy in the information.[79]

Search query logs should often meet this subjective expectation of privacy standard. Often user search terms are of a content that is highly sensitive and extremely private in nature.[80] The large percentage of searches that encompass pornographic queries demonstrates how prevalent these sensitive searches are.[81] It is common-sense that users are intending searches of this nature, and those of equally private subject-matters, to be private.[82] Some other types of searches that could meet this threshold include: user's financial info, disease or illness research, street addresses, and possibly even doctor information. The user believes (mistakenly) that he is typing these search terms into an anonymous service to be directed to websites to serve his needs. Would a user still type such sensitive information into the search engine if he knew it was being recorded and could be traced back to him? The answer varies from user to user, but it is likely the user would at least be more cautious about his use of the search engine. The high percentage of sensitive searches supports the findings that not only are the searches content information, but that the user had an expectation that they were being kept private.

a. The Search Engine's Terms of Use Agreement Should Not Result in the Waiver of the User's Subjective Expectation of Privacy

Everyone knows the saying that what you post on the internet becomes public knowledge. And while most would assume that this mantra encompasses social sites like Facebook and job site like Linked In; it is unlikely that they knew that their Google searches were being recorded.[83] While terms of use and privacy policies are publicly available on Google, Yahoo, and other search engines, they are hidden in the background making it difficult for users to find. The user is not put on notice that by using the service he is waiving his privacy interests, that the government can obtain these search engine logs without probable cause, or that anyone is even recording the searches. For the reader to read the terms of use agreements he must know of its existence and then find it on the site. And while the cautious user might search for it, search engines have become so

---

[79] United States v. Katz, 389 U.S. 347, 361 (1967).

[80] Tene, *supra* note 6, at 1442; James Grimmelman, *The Structure of Search Engine Law*, 93 IOWA L. REV., 1, 18 (2007).

[81] Based on a Google Trends analysis there are an estimated 500,000 teen-related pornographic searches, just 1/3 of the total pornographic searches, each day. *Pornographic Statistics*, INTERNETSAFETY101.ORG http://perma.cc/2BCH-C9WF (last visited Sep. 24, 2014).

[82] Matthew Tokson, *The Content/Envelope Distinction in Internet Law*,50 Wm. & Mary L. Rev. 2105, 2163 (2008–2009).

[83] *Forrester*, 495 F.3d at 1049; Sorosky, *supra* note 34, at 1128; Tene, *supra* note 6, at 1469.

mainstream and entrenched in the public conscious that this is not the social expectation.

Furthermore, even if the user knew the search engine was recording their search queries, it does not necessarily follow that they knew that this information would be disseminated. As Justice Marshall observed in his dissenting opinion in *Smith v. Maryland*,

> "But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[84]

The same can be said of search engine service providers today as of phone companies then. Users should maintain their expectation of privacy if they did not have the knowledge that what they were inputting would and could be shared. Admittedly there are circumstances where the user has knowledge that their actions are being monitored by another, for instance if they were logged onto a work or school network with highly publicized privacy policies. Under these circumstances privacy should be deemed waived because the user had knowledge that the information was not private. In most cases however, this is not the case and it is likely that the user had no knowledge of the possibility or the intention that any of his search term queries would be shared with the public or government.

Currently, courts have held that a user is bound by the terms of use agreement, including its privacy agreement provisions, even if he has not read it, is unaware of its existence, and/or has not had input in crafting it.[85] In doing this the courts have adopted a user beware standard when it comes to use of internet service provider services. The executive branch of the government supports this current position.[86] The Department of Justice, in their computer security and intellectual property search guide, states that a privacy agreement that includes a clause stating that the service provider will cooperate with enforceable law enforcement automatically means that the user of such a service has knowingly waived any expectation of privacy

---

[84] Smith v. Maryland, 442 U.S.735 at 749 (1979) (Marshall, J., dissenting). *See also*, Bagley, *supra* note 17, at 171.

[85] Bagley, *supra* note 17, at 178–79.

[86] *See* DEPARTMENT OF JUSTICE: COMPUTER CRIME AND INTELLECTUAL PROPERTY DIVISION, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 26 (2009).

he might have possessed if the government requests the information.[87] They do not state that notice or knowledge of such a policy is necessary.[88] In fact, they maintain that to acquire information from remote service providers like Google, who has such a clause,[89] that they do not even have to use a search warrant or other officially recognized method if consent is given implicitly through the terms of use agreement.[90] The only remaining barriers would thus be statutory in nature, since the user is viewed to have waived his constitutional right to privacy. While such a law is useful for law enforcement purposes, it is not a fair application of contract law and should be viewed as invalid to the extent that it might waive user's privacy rights or be viewed as blanket consent to government searches.

As standardized, one-party drafted agreements become more common in modern transactions, a specific area of law has developed to pertain to that particular type of contract. The law states that an individual can be held to his agreement to a contract he had no part in formulating if he feels at the time that it is a contract that is standardly given to all in a similar situation.[91] The contract is binding to all equally despite their knowledge or understanding of its contents.[92] However, any questionable terms should be construed against the drafter of the contract.[93] And further, the contracts may be reviewed for fairness. First, if the drafting party has a reason to believe that the agreeing party would object to a term if he understood the term and its implications, then the term is void.[94] Second, the term may be found unconscionable by the court[95] if the term fails to meet the standards of good faith.[96]

An unconscionable contract is a contract which "no man in his senses and not under delusion would make on the one hand, and as no honest and fair man would accept on the other."[97] When making this determination a judge looks at the setting, purpose, and effect of the contract along with any other weaknesses.[98] By looking at these factors the judge must determine whether the individual agreeing to that specific contract, with its specific purpose, would have the intention to agree to the term in question, if he would not, then it is an unconscionable term.

---

[87] *Id. See* Bagley, *supra* note 17, at 166.

[88] *Id.*

[89] *Privacy Policy*, GOOGLE, *supra* note 15.

[90] DEPARTMENT OF JUSTICE: COMPUTER CRIME AND INTELLECTUAL PROPERTY DIVISION, *supra* note 16.

[91] RESTATEMENT (SECOND) OF CONTRACTS § 211(1), (2) (1981).

[92] RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. b (1981).

[93] *See* RESTATEMENT (SECOND) OF CONTRACTS § 206 (1981).

[94] *See* RESTATEMENT (SECOND) OF CONTRACTS § 211(3) (1981).

[95] RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. c (1981), introductory cmt. *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 (1981).

[96] *See* RESTATEMENT (SECOND) OF CONTRACTS § 205 (1981).

[97] Hume v. United States, 132 U.S. 406, 411 (1889).

[98] RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. a (1981).

Good faith is defined as keeping faithful to the purpose of the agreement and the other party's justified expectations.[99] Conversely, bad faith is defined by a series of examples such as: "evasion of the spirit of the bargain, lack of diligence and slacking off, willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance."[100]

The terms of use and privacy agreements drafted by the search engine service providers are standardized agreements. They are made to be agreed to by all search engine users and are made without the input and often knowledge of the users. As such, they are subject to all the laws and review applicable to such standardized agreements.

Even if the court's premise, that users have knowledge of the provisions of the terms of use agreements, is presumed true the agreements fail to suggest that—or is at least ambiguous whether—all information is subject to disclosure.[101] The privacy policies generally notify the user that their information is collected and stored with his IP address for a specified time and that information can be shared with the government if the service provider receives an *enforceable* government request or other law, regulation, or statute.[102] This suggests that the service provider will only share a user's information with the government to the extent that it is required to by the law and no more so than that. The privacy agreement does not state that the service provider can or will turn over all data requested by the government merely because the government wishes it. Nor does it say that the user, in providing the service provider with the information, relinquishes any privacy right to the information that is afforded to him by any law, statute, or regulation. It merely confirms that the service provider is obligated to share information with the government to the extent needed to comply with the laws, just like any other private information would be; it provides no additional latitude.

Contrary to this position the Department of Justice interprets the privacy policies to mean that the user waives all privacy rights to *any* information, including content information, shared with the service provider.[103] In making this conclusion the Department of Justice relies on *United States v. Beckett*.[104] In that case however, the service provider, MySpace, sent the information in response to exigent emergency circumstances detailed by the investigating detective who felt that there

---

[99] Entergy Arkansas, Inc., v. Nebraska, 358 F.3d 528, 547 (8th Cir. 2004).

[100] *Id.*

[101] Bagley, *supra* note 17, at 178–79.

[102] *Google Terms of Service*, GOOGLE, http://perma.cc/QHC5-F7Z5. (Jan. 23, 2014); *Privacy Policy*, GOOGLE, *supra* note 7 (stating that Google has the ability to collect everything the user inputs into its site).

[103] *See* DEPARTMENT OF JUSTICE: COMPUTER CRIME AND INTELLECTUAL PROPERTY DIVISION, *supra* note 16, at 26.

[104] United States v. Beckett, 544 F. Supp. 2d 1346 (S.D. Fla. 2008).

were victims in danger of imminent sexual assault if the information was not obtained immediately.[105] The comment about legitimate subjective interest was made in regards to the disclosure of information to prevent harm to others as detailed by the express term of the privacy agreement related to that circumstance, not the general complying with enforceable law enforcement requests term.[106] That is why in its statement concerning the subjective privacy interest of the user the court specifically included the language "circumstances similar to those in our case," which was also included in the excerpt in the Department of Justice Manual.[107] While it is conceded that disclosures of information for emergency purposes to protect public safety are valid, this language does not apply to non-exigent circumstances situations such as a mere government request for information.[108] Furthermore, because this is a standardized contract any ambiguous terms should be resolved in favor of the user.[109]

While it is uncontested that the user does not need to be aware of the privacy agreement, understand the agreement, nor have a part in the creation of the agreement, there are still common law fairness protections that need to be considered.[110] To determine if the contract term is fair the court first asks whether the drafter believes that if the user knew the terms and implications of the contract he would still agree to it. If the court finds that the drafter should expect that the user would not agree to such a term then that term would be void.[111] There is an argument to be made that users would not utilize service providers if they knew the service provider was collecting and could turn sensitive information over to the government. However, most users are likely to feel that they would never be the targets of a government inquiry and since there are no alternatives short of not using any search engine, that users would have no choice but to use the search engine or not participate in the digital world. So while the average user might be outraged and consider the term unfair, it is unlikely that they would refuse to agree to the term in order to use the service.

Second the court looks at whether the term was made in good faith. Every party has the duty of entering a contract in good faith and to deal fairly with the other party.[112] Creating an unnecessary, complete, waiver of Fourth Amendment privacy rights is a breach of good faith and fair dealing

---

[105] *Id.* at 1348.

[106] *Id.* at 1350.

[107] *Id.*

[108] What threshold should be necessary to count as exigent circumstances to warrant immediate disclosure of information without other legal force goes beyond the scope of this paper.

[109] *See* RESTATEMENT (SECOND) OF CONTRACTS § 206 (1981).

[110] RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. b (1981) (updated 2013).

[111] *See* RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. c (1981) (updated 2013).

[112] RESTATEMENT (SECOND) OF CONTRACTS § 205 (1981) (updated 2013).

by the service providers.[113] It could be viewed as evasion of the spirit of the bargain and expectations of the other party—to provide the best service for the user as possible while seeming to maintain privacy rights—and an abuse of power to specify the terms by not protecting the user's privacy rights when it has no reason not to do so but to appease the government. While most jurisdictions openly embrace the concept of good faith in fair dealing in contracts, the exact means of analysis and enforcement of the provision in non-obvious cases is far from certain.[114] Therefore it is unclear whether the waiver of privacy rights term is enough for a court to take action on breach of good faith grounds.

Finally, the court could consider voiding the term as unconscionable. If the courts insist on interpreting the terms of use as a waiver of all privacy rights this term should be considered unconscionable. While part of the analysis is similar to the drafter question of whether he felt that the user would agree to the contract, the court is also allowed to consider the setting, purpose, and effect of the contract along with an extremely lax standard of reasonableness in both parties' actions.[115] While some contract terms will always be unconscionable, others might be depending on the circumstances.[116] In such cases factors like an overall imbalance in consideration or weaknesses in the bargaining process like unequal bargaining power become important factors when determining if a contract is unconscionable.[117] For search engine users there is an imbalance in the bargaining power because there are no alternatives to agreeing with the terms of use besides not participating in the digital world due to the pervasiveness of the search engines. And secondly, the process of hiding the terms elsewhere on the website instead of making them known to users before they are bound by them through the utilization of services is akin to the comment's example of using large amounts of fine print; its purpose is to obscure and hide the information.[118] And lastly, there is no reasonable alternative to the utilization of the service, as such there is a gross imbalance in consideration. An individual should not be required or essentially coerced, into giving up his Fourth Amendment privacy rights in

---

[113] *See* RESTATEMENT (SECOND) OF CONTRACTS § 205, cmt. a (1981) (updated 2013). While there is no exact definition of "Good Faith," the comment emphasizes "faithfulness to an agreed common purpose and consistency with the justified expectations of the other party." It is the opposite of bad faith actions which violate "decency, fairness, or reasonableness." So while the definition itself is flexible, it is mostly determined not by the action but by the intent of the actor and expectations of the other party in the deal.

[114] *See* GNC Franchising Inc. v. O'Brien, 443 F. Supp. 2d 737, 750 (W.D. Penn. 2006).

[115] Hume v. United States, 132 U.S. 406 (1889); RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. a (1981) (updated 2013).

[116] RESTATEMENT (SECOND) OF CONTRACTS § 208 cmt. e (1981) (updated 2013).

[117] *Id.* Examples of unconscionable terms included in the comments include: when sellers sell items that have latent defects, when a seller takes advantage of a unknowledgeable client with tricks such as large amounts of fine print, and when clauses impose difficulties on a party for no purpose other than to cause a difficulty (like stating jurisdiction for disputes is in a state 200 miles away).

[118] *See Id.*

order to participate in the digital community. If a court were to consider these factors together, they should determine that the contract waiving privacy rights is unconscionable.

2. The Expectation that Search Engine Queries are Private is Objectively Reasonable

The second prong, the objective expectation of privacy, is the fail-safe to the first factor. The court determines whether the expectation of privacy in the information is something that the public is willing to accept as "legitimate".[119] This standard evolves as the public consensus changes but will consistently rule out criminal acts and other acts which should be excluded for policy reasons.[120] This principle also insures that privacy law adheres to other legally developed principles.[121]

Search engine logs meet the general requirements for this prong. They are not criminal in nature and could contain information that most of the public would expect to be considered private. There is nothing innate about search logs that renders them public information nor is there a policy reason for making such information public. However, one area of law has developed that impacts this analysis, the Third Party Disclosure Doctrine. To properly apply this doctrine, search engine logs must be classified as either content or non-content information.

a. The Third Party Disclosure Doctrine

In *Smith* the court established the Third Party Disclosure Doctrine which states that a person does not have a legitimate privacy interest in records information, or non-content information, turned over voluntarily to another.[122] In *Smith* a government agent recorded the petitioner with a pen register, and the issue for the court was how much information of that conversation was protected by the 4th Amendment The court ruled that the defendant had no objective expectation of privacy in any records information about the call shared with another party, like the phone number to the telephone operator.[123] From this ruling the Third Party Disclosure Doctrine, also known as the Assumption of Risk Doctrine was created for any individual who provides non-content information to another party.[124] Falling outside the scope of this rule, content communication information is still governed by the rest of the *Katz* privacy

---

[119] Rakas v. Illinois, 439 U.S. 128, 143, n. 12, (1978).

[120] *Id.*

[121] *Id.*

[122] Smith v. Maryland, 442 U.S. 740–41 (1979); Tene, *supra* note 6, at 1471.

[123] Smith v. Maryland, 442 U.S. 747, 745–46 (1979); Sorosky, *supra* 34, at 1126.

[124] Orin Kerr and Greg Nojeim, "The Data Question: Should the Third-Party Records Doctrine Be Revisited?" ABA JOURNAL (Aug. 1, 2012), *available at* http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

analysis.[125] There has been no hint that the government or courts plans on removing this distinction.

In *Smith* the court distinguished "content" from "non-content" information, and held that there is no "legitimate" expectation of privacy in non-content information.[126] Currently the status of search engine logs is undecided amongst the courts,[127] however they should be considered content because the information contained in search logs contains the substance of the communication similar to a URL address and unlike an IP address.

As previously mentioned, content is defined in the Stored Communications Act as "information concerning the substance, purport or meaning of [a] communication."[128]

Recently this classification has been applied to internet and computer law. The court in *Forrester* said that IP addresses, the unique number identifying each computer that is linked to the internet, were like telephone numbers and, along with email addresses, they should be considered non-content information.[129] But this holding begs the question, what about the classification of URLs, the web address that tells the internet service provider what webpage to go to?

Whether URLs contain search terms in them or not, scholars are unanimous that URLs should be considered content information.[130] Whether directly stating in the URL the content, like when containing search terms, or after following the URL directly, it is possible to learn with specificity the content of the page a user was on. For example, if a customer were to search for George Orwell's 1984 at Barnes and Noble, the URL, when followed, would reveal the book being searched for; the IP address would only reveal that the user was on the Barnes and Noble website. In this way, the URL is more analogous to the phone conversation protected in *Katz* than the phone number log collected in *Smith* and *Miller*.[131] Because of the possible specificity of information that can be gained from URLs, the Court in *Forrester* took care to distinguish URLs from IP addresses in a footnote, stating that URLs could possibly require greater privacy protection.[132] Furthermore, URLs can be used to reveal the content of the information, and despite its function of guiding the user to the website—like an address—it is the end result of knowing

---

[125] *Id.*

[126] Smith v. Maryland, 442 U.S.735 at 745–46 (1979).

[127] Foley, *supra* note 5, at 458; Tokson, *supra* note 84 at 2147.

[128] 18 U.S.C. § 2510(8) (2013).

[129] U.S. v. Forrester, 495 F.3d 1041, 1048–49 (9th Cir. 2007); Tokson, *supra* note 84, at 2135–36; Sokorsky, *supra* note 24, at 1127. *But see* Tokson, *supra* note 84, at 2147; Sorosky, *supra* note 34, at 1139 n.112 (IP information that can reveal content should be afforded the same content protection).

[130] Tokson, *supra* note 84, at 2143, 2147; Tene, *supra* note 6, at 1479.

[131] Foley, *supra* note 5, at 470. *See* Katz v. United States, 389 U.S. 347 (1967); Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

[132] *Forrester*, 495 F.3d at 1049 n. 6.

the content of the user's communication with the website that should be viewed as the key factor. It is for these reasons that that URLs should receive the content classification.

Even more so than URLs, search engine logs should also be classified as content communications. While not currently debated to the same extent, it is possible to utilize the same considerations the court has used for URL in making the determination for search logs.[133] Since the search engine logs gather the exact search queries used, the search engine logs are even more revealing of content than URLs themselves.[134] By looking at them, the government could see each and every exact term, despite how private or sensitive they might be. It is these terms that the user sent to the service provider, in confidence, as a request to receive possible website destinations. It is a communication between the user and the service provider; even more so than just typing in the URL to a browser as a destination. As such, the courts should maintain that search engine logs should be considered content information.[135]

Therefore the Third Party Disclosure Doctrine, that plagues other non-content information like personal user information records and contact information lists, should not apply to search logs.[136] The basic *Katz* objective legitimacy test still applies but as previously mentioned search logs pose no innate threat to the public. It is a privacy expectation that is not only based in common sense, but matches the common belief and expectation of the public that search engines are private.[137] Furthermore, unless the user takes additional actions to make his search queries public, they are assumed protected as content information. While the nature of search engine use is not the same as an object in a yard that can be covered by a tarp to illustrate the owner's intent, it should be reasonable to assume a default intention of privacy by the user. As such, in instances without extraordinary circumstances, search engine logs should pass the *Katz* publicly legitimate prong.

If however, search engine logs are considered non-content information then the Third Party Disclosure Doctrine would apply.[138] Then, this paper acknowledges the second prong of the *Katz* analysis would not be met and search engine logs would not be afforded 4th Amendment Protection.

---

[133] This is necessary because currently there is only one district court case that addresses the content or non-content status of search queries. Though it does not specifically address the accumulated log of search queries created by the remote service provider, the case states that the information a user types into a search box is content. *In re* Application of the United States for the Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

[134] Sullivan, *supra* note 7.

[135] *In re* Application of the United States for the Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 45 (D. Mass. 2005).

[136] *But see* Foley, *supra* note 5, at 463. (Foley assumed that search terms would be determined to be non-content information. This analysis was before U.S. v. Forrester).

[137] Tene, *supra* note 6, at 1489.

[138] Smith v. Maryland, 442 U.S. 747, 745–46 (1979).

While some might consider search engine logs merely an identifying record, like a phone-numbers dialed registry kept by a phone company, and thus non-content info, the content specific information contained within the logs, namely the search queries, are an expression of the user's thoughts and interests, which are beyond the scope of non-content information.

In summary, users have a subjective and objective expectation of privacy in search and thus are protected by the Fourth Amendment. For the government to obtain access to search logs they should be required to get a warrant supported by probable cause of wrongdoing and relevancy of the information.[139] No other government request, subpoena, or court order should be sufficient.[140]

B. The Stored Communications Act

If search engine logs fail to receive *Katz* protection, the Stored Communications Act may still afford some protection.[141] Currently there is no case law stating whether search engine logs receive Stored Communications Act protection or not.[142] However, the lack of discussion on the topic is due to a lack of opportunity not because of an inherent deficiency in the claim.

As previously noted the SCA places restrictions on what RCS can disclose to the government and to the public. These restrictions depend in part on whether the information is content or non-content information along with why this information is being released. Release of search logs to the government may be the result of voluntary disclosure, a response to a government request, or to prevent substantial harm.[143] As this article has already concluded search engine log data fits the definitions of content information and therefore voluntary and required disclosure should be restricted.

To begin, remote service providers are prevented from voluntarily disclosing any content information maintained on its service to anybody.[144] They are also prevented from disclosing any non-content "records or other information pertaining to a subscriber to or customer," with the government.[145] This should prevent Google and any search engine provider from volunteering information, outside of the emergency exception situations, to a governmental entity because search engine

---

[139] G.M. Leasing Corp. v. United States, 429 U.S. 338, 352–53 (1977). (If protected by the Fourth Amendment then a warrant should be required for the government to obtain the information).

[140] *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 679 (N.D. Cal. 2006). (Google can comply with government requests without a warrant, as such there is no 4th Amendment privacy interest).

[141] 18 U.S.C. §§ 2701–2712 (2012).

[142] Foley, *supra* note 5, at 473.

[143] 18 U.S.C. §§ 2701–2712 (2012).

[144] 18 U.S.C. § 2702(a)(2) (2012).

[145] 18 U.S.C. § 2702(a)(3) (2012).

queries should be viewed as content and is at least a record pertaining to a customer.[146]

Continuing on to the required disclosure section, the statute says the section applies to "any wire or electronic communication that is held or maintained on that service...on behalf of, and received by means of electronic transmission from...a subscriber or customer of such remote computing service."[147] A user's search term log should be considered an electronic communication (i.e. content); it is received through the internet; and it was sent by the user who was a customer of the remote computing service. As such, the search logs should meet this definition and get this section's protections. Alternatively, if viewed as non-content information, it also meets the definition of a "record or other information pertaining to a subscriber to or customer of such service."[148] And even under the non-content listing, search queries do not fall under the list of mandatory disclosure information items that can be given without an official request.[149] Therfore, immaterial of its classification of content or non-content; search engine logs should meet the definitions of what is protected under the Stored Communications Act.

As discussed in the background section above, the protections of the Stored Communications Act are significant. It inhibits voluntary disclosure as well as prevents pre-trial subpoenas from being sufficient.[150] Thus, the government must already have a case or have presented one to a grand jury for consideration before requesting the information. It cannot be the first of its building blocks in the case. While this protection is less significant than the Fourth Amendment affords it is still a protection that if *Katz* fails, should protect search engine query logs.

However, even this analysis is not certain in regards to content stored by an online provider. Some have stated that it is possible to read the terms of service agreement to be equal to the voluntary consent of the user to allow the search.[151] Under such an analysis the government would not need to wait or meet any standard of proof, or obtain any order before receiving the information because the user would have consented to the search. However, the terms of service agreement should not be read in this way. Similar to the argument above, the terms of service agreement simply puts the user on notice that the service will comply with, "any applicable law, regulation, legal process or enforceable governmental request," not that the user is waiving his right to the privacy of the information to *any* government request; only the legally enforceable ones

---

[146] *See Google*, 234 F.R.D. at 687. (Google can comply with government requests without a warrant, as such there is no 4th Amendment privacy interest).

[147] 18 U.S.C. § 2703(b)(2)(A) (2012).

[148] 18 U.S.C. § 2703(c)(1) (2012).

[149] 18 U.S.C. § 2703(c)(2) (2012).

[150] 18 U.S.C. §§ 2702(a)(2)–(3) (2012); 18 U.S.C. §2703(b)(1)(B)(i) (2012).

[151] Bagley, *supra* note 21, at 169.

that meet the standards outlined by law.[152] The Stored Communications Act makes it clear which standards need to be met for each type of disclosure to the government, and this provision, and all similar ones of other agreements, does nothing to reduce or change that. Still, because some individuals are confused by the implications of such terms, the language of the Stored Communications Act should be updated to reflect the modern digital age and encompass all of its types of data and communications.[153] However, despite its current state, nothing exists that should detract from the protections that should be afforded through it to users for their search engine query logs.

III. CONCLUSION

Search engines are a necessity in the current digital world, and privacy law should recognize this and adopt accordingly. Users should be able to participate in this digital world without their entire intimate and private searches being made public or turned over to the government without their knowledge or consent. The courts should recognize search queries as content information in which the user has both a subjective and objective expectation of privacy. The terms of use and privacy agreement contracts—to any extent that they are found to a waiver of the user's Fourth Amendment rights—should be found void as an unconscionable term under standardized contract laws because of the lack of public awareness, fairness principles of contract law, as well as the current necessity of search engines in the digital age. Finally, regardless of whether the logs qualify for Fourth Amendment protection, they should at least qualify under the protections that the Stored Communications Act provide. To this generation the anonymity, expediency, and necessity of search engines have become as second nature as the writing of letters and the use of telephone boxes were in past generations. Yet searches have not received the same level of privacy protection that is warranted their sensitive nature and public perception. It is time for the law to catch-up with the generation and recognize all logs of such searches with the statutory and constitutional privacy protections that they deserve.

---

[152] *See Google Terms of Service*, GOOGLE, http://perma.cc/QHC5-F7Z5 (last visited Jan. 23, 2014).

[153] Bagley, *supra* note 21, at 169–70 (Hearings have been held by Congress seeking to remove the ambiguities of the Stored Communications Act).