2011

When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking

Anne Klinefelter

Publication: *Virginia Journal of Law and Technology*

VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2011 UNIVERSITY OF VIRGINIA VOL. 16, NO. 1

WHEN TO RESEARCH IS TO REVEAL: *THE GROWING THREAT TO ATTORNEY AND CLIENT CONFIDENTIALITY FROM ONLINE TRACKING*

Anne Klinefelter †

ABSTRACT

Attorney-client privilege, work-product protection, and the attorney's ethical requirement to protect confidentiality of client information are at risk from commercial surveillance of online activity. Behavioral advertising, data aggregation and sale, and government access to commercially assembled profiles have been denounced as threats to privacy and confidentiality interests, but the harm to attorney and client confidentiality is of particular concern. As the legal research and broader information industries shift from print materials to services on the internet, attorneys cannot simply avoid the online environment to protect confidentiality. This article examines the risk from tracking of online legal research and draws two conclusions: 1) Lawyers must take reasonable precautions to protect confidentiality of internet-based research; and 2) Reasonable precautions are elusive due to the constant evolution of tracking technologies and practices, so attorneys should work collectively to update best practices and

† Anne Klinefelter is Associate Professor of Law and Director of the Law Library at the University of North Carolina. Thanks go to participants in the 2010 Privacy Law Scholars Conference for helpful suggestions, especially Michael Zimmer and Mary Minow. Thanks also to Ann Clifford Green, John P. Tomaszewski, Elizabeth Johnson, and especially Michael Dorman for helpful conversations on the topic and to Maxine Eichner and Robert C. Mosteller for comments that helped improve the article. Research assistants Michelle Humphries and Ann McKay provided excellent support in the early development of this project, and Dave Hansen provided superlative assistance in the final stages. The author is indebted to the library staff at the Kathrine R. Everett Law Library for their support.

to evaluate and influence online industry activities so that the time-honored confidential nature of legal representation can be preserved.

TABLE OF CONTENTS

I. INTRODUCTION

If an attorney and her client meet and review maps or other visual materials in front of a window onto a busy sidewalk, a court may find the material is not confidential. Similarly, if an attorney consults a legal treatise about a client's case, makes notes and photocopies, and then leaves those notes and copies beside a cash register at a clothing store, that research material is not kept confidential. These scenarios have easy solutions: pull shades over the windows, and keep research material locked in a briefcase.

But how do these scenarios translate to the world of the internet? Consider the attorney who explores a variety of online resources in support of developing legal advice, but in the process leaves a trail of search queries that are collected and merged to produce tailored advertising or perhaps to serve other purposes. Whether or not these activities were intended to be confidential, their exposure to third-party advertisers and potentially

to others could indicate that they are not in fact confidential. Solutions are not always as easy as pulling the shades or using a locked briefcase. Like most online researchers, attorneys and their clients are probably unaware of the growth of online tracking and are also not likely to understand how to implement and update a host of tools to reduce exposure of online activity.[1] Some suggest that even sophisticated users of the internet are unable to effectively protect the confidentiality of online activity because both new and relatively older architectural technologies of the internet evade the tools of confidentiality available to consumers.[2]

The online tracking industry is growing,[3] inspired by decreasing costs of technology[4] along with largely unregulated access to a vast amount of information sent online. A variety of theories would use existing law to restrict online tracking, but these

[1] *Prepared Statement of the Federal Trade Commission on Consumer Privacy*, S. COMM. ON COMMERCE, SCI. & TRANS., 17–18 (July 27, 2010), http://commerce.senate.gov/public/?a=Files.Serve&File_id=057baf64-4393-4b42-8fe1-d216f45d3be0 [hereinafter *FTC Statement on Consumer Online Privacy*] (reporting that the Commission's public roundtables on consumer privacy in late 2009 and early 2010 produced a common theme that "consumers do not understand the extent to which companies are collecting, using, aggregating, storing, and sharing their personal information"). The Wall Street Journal published a series of articles on increased online tracking of consumers in the summer of 2010. *See* Julia Angwin & Tom McGinty, *Personal Details Exposed via Biggest U.S. Websites*, WALL ST. J., July 31, 2010, at A1 (reporting that the most-visited fifty U.S. websites installed an average of sixty-four tracking tools on the computers of individuals who visited those sites); *see also infra* Part IV (outlining various "reasonable precautions" for attorneys to implement in limiting their online exposure of clients' confidential information).

[2] Leslie Harris, *[Prepared] Testimony before the House Subcommittee on Commerce, Trade, & Consumer Protection*, CTR FOR DEMOCRACY & TECH., 2–3 (July 22, 2010), http://www.cdt.org/files/pdfs/CDT_privacy_bill_testimony.pdf ("[C]ollection, sharing, and use of online consumer data . . . are increasingly outside of consumers' control. Online, even very savvy consumers are being thwarted in their efforts to take technological steps to protect their privacy and are seeing the privacy decisions they make directly overridden."); Nick Wingfield, *Microsoft Quashed Effort to Boost Online Privacy*, WALL ST. J., Aug. 2, 2010, at A1 (describing how advertising interests persuaded Microsoft not to make privacy features in its internet browser software, Internet Explorer, operate by default).

[3] This article uses the terms "online" and "internet" interchangeably. The use of online tracking tools to match advertisements with presumed purchasing preferences has increased dramatically in recent years. Stephanie Clifford, *Ads Follow Web Users and Get More Personal*, N.Y. TIMES, July 31, 2009, at A1 (reporting on the growth in use of tracking tools linked to the web browsing software on individual computers). While the global economy suffered during 2009, online advertising grew 2% to $55.2 billion. Online advertising spending is projected to increase at a rate of 11.9% compounded annually through 2014. Jared Jenks, *Worldwide Ad Spending*, EMARKETER (July 2010), http://www.emarketer.com/Reports/All/Emarketer_2000710.aspx (drawing on reports from twenty-three market research firms worldwide). Companies that collect and compile information on individuals and resell it may be on the rise. The advocacy organization Privacy Rights Clearinghouse lists contact information for over 100 data brokers said to collect information from public records, information publicly available on the internet, and possibly other sources. *See Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/online-information-brokers-list (last visited Feb. 18, 2011). The Federal Trade Commission has reported that commenters and panelists at recent privacy roundtables "raised concerns about the tendency for companies storing data to find new uses for that data." *FTC Statement on Consumer Online Privacy, supra* note 3, at 19.

[4] Paul Rosenzweig, *Privacy and Counter-Terrorism: The Pervasiveness of Data*, 42 CASE W. RES. J. INT'L L. 625, 627–29 (2010) (reviewing the logarithmic rates of increase in computing power and decrease in costs of data storage).

theories are largely untested, unsettled, or without broad application.[5] Proposed federal statutes and regulations would limit the collection and sharing of data about online activity, but they have yet to result in clear protections.[6] Given the lack of transparency in this data collection and reuse, and given the weakness of the law of tracking, any user of the internet seeking to maintain confidentiality of those activities is at a disadvantage. Attorneys and their clients face challenges in creating and maintaining confidentiality for privileged information reflected in online research. In addition, attorneys are poorly positioned to protect their work-product and meet ethical requirements of confidentiality—and even competency—in this heavily monitored environment.

¶ 1 This article brings to light the harm to attorney and client confidentiality from commercial tracking of online research and demonstrates how difficult it is for attorneys and clients to prevent this tracking. The article suggests how attorneys should collectively develop best practices, both to guide individual attorneys and to encourage online industry support for confidentiality. Finally, the article proposes that if these best practices fail to secure confidentiality of online legal research, attorneys and their clients should seek stronger legal protections for online confidentiality.

II. OVERVIEW OF ONLINE TRACKING

A. The Two-Way Mirror of Internet Research

Many internet users consider online activity to be confidential because no person stands looking over their shoulders, but the reality is quite different.[7] For most internet users, the online research process is similar to facing a two-way mirror. The computer screen displays information that reflects the queries and clicks entered but hides from view the monitoring and re-use of data about those queries and clicks.[8] Without transparency, online researchers have little opportunity to evaluate the threat to confidentiality and limited ability to exercise control.

¶ 2 The lack of transparency in online tracking practices is a function of several factors. A familiarity with information technology is required to understand the tools and practices of tracking.[9] Tracking tools continue to evolve in order to elude consumer

[5] *See infra* Part II.C.

[6] *Id.*

[7] *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets—A Journal Investigation Finds That One of the Fastest-Growing Businesses on the Internet is the Business of Spying on Consumers*, WALL ST. J., July 31, 2010, at W1 ("[T]he tracking of consumers has grown both far more pervasive and far more intrusive than is realized by all but a handful of people in the vanguard of the [internet] industry."); Joshua Gomez et al., *KnowPrivacy Report*, KNOWPRIVACY 15, 18 (June 1, 2009), http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (comparing the privacy policies and practices of the most visited websites with surveys and polls of consumer expectations and finding a "large level of ignorance on the part of users about how data is collected").

[8] The very architecture of the internet is intended to "hide all the details of the physical layout of the internet from the applications." 1 W. RICHARD STEVENS , TCP/IP ILLUSTRATED: THE PROTOCOLS 5 (1994).

[9] As the recommendations for "reasonable steps" to protect confidentiality in this article demonstrate, even less-than-perfect protection from online tracking requires a fairly complex set of precautions to address the layered vulnerabilities. The Federal Trade Commission reported that feedback collected

efforts to limit monitoring of their online behavior.[10] Furthermore, online service providers and related industries have had limited motivation to explain their processes in any great detail.[11] Some tracking of internet use is employed in secret because it is clearly malign,[12] but this article highlights tracking conducted for cost recovery for business and for government purposes that are at least arguably benign. This overview draws on recent investigative reports, online industry publications, privacy advocacy initiatives, legal scholarship, and testimony relating to potential regulation of online tracking to provide a picture of current tracking activities.

B. Why They Track and How to Limit Their Tracking

1. Websites

A website needs to know some information about its visitors, such as their unique location on the internet, to be able to deliver the website's content to each site visitor's

---

through its public roundtable discussions on privacy in late 2009 and early 2010 included concerns that the current environment "places too high a burden on consumers to read and understand lengthy privacy policies and then ostensibly to exercise meaningful choices based on them." *FTC Statement on Consumer Online Privacy*, *supra* note 3, at 19.

[10] Rosenzweig, *supra* note 6, at 625, 627–32 (suggesting that practical limitations in "dataveillance," the electronic "collection and analysis of personal data," lie only in the capacity of search algorithms available to take advantage of exponential "increases in computing power and decreases in data storage costs"). As consumers gain technological tools to prevent the display of advertisements, developers create new tools, and the process repeats. *See* Ashkan Soltani et al., Flash Cookies and Privacy 3 (August 10, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1446862 (describing the adaptation of an internet tool in order to evade consumers' attempts to prevent tracking); Press Release, comScore, Flash and Rich Media Ads Represent 40 Percent of U.S. Online Display Ad Impressions (June 29, 2010), *available at* http://www.comscore.com/Press_Events/Press_Releases/2010/6/Flash_and_Rich_Media_Ads_Represent_40_Percent_of_U.S._Online_Display_Ad_Impressions ("[P]op-ups and pop-unders now represent less than 1 percent of all display ad impressions, most likely a function of the pop-up blockers now standard in most browsers.").

[11] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 610–13 (2007) (noting that website owners had little motivation to provide accurate descriptions of their tracking practices, but instead benefited from writing overbroad notices of potential collection and re-use of visitor data because consumers did not read the policies); Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, at D1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html (reporting that NebuAd, Phorm, and Front Porch data collection companies were working with several internet service providers ("ISPs") to track subscribers' internet activities but that the ISPs would not respond to journalists' inquiries about tracking practices).

[12] Sometimes the line between malign and benign tracking is difficult to draw because both can offend by happening without the knowledge or understanding of the consumer and because an apparently benign collection of data could later be re-used for an unforeseen and unwelcome purpose. *See, e.g.*, Daniel B. Garrie et al., *Regulating Spyware: Challenges and Solutions*, 13 No. 8 J. INTERNET L. 3, 4 (Feb. 2010) (stating that "[s]pyware blurs the existing line between a malicious virus and an aggressive Internet marketing tool," but ultimately distinguishing spyware from programs that collect internet browsing data for advertising purposes). *See generally* Heather Osborn Ng, *Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware*, 31 HASTINGS COMM. & ENT. L.J. 369, 374–75 (2009) (comparing relative harms from spyware and tracking devices used for behavioral marketing).

computer.[13] Websites may track use in some detail to support billing[14] and system security,[15] improve or personalize their systems,[16] create new products,[17] and target marketing of their own products or services.[18] For example, when an attorney signs on to Westlaw and enters a username and password, the system will match that sign-on information to saved preferences which personalize the service for the attorney, such as the selection of "tabs" to display frequently used categories of Westlaw content.[19]

Some fee-free website services may never know a visitor's name or physical address and instead track each visitor by his access point to the internet (his "IP address")[20] and by assigning a unique identifier to the software he uses to browse the internet.[21] Many websites also track each visitor's activity on a site through invisible programs called "web bugs" that are embedded in the display of the web page.[22]

---

[13] 1 STEVENS, *supra* note 10, at 33–34 (providing a detailed description of how information travels across the internet, including how a visit to a website requires the delivery of information from an internet information provider to the visitor's particular internet address).

[14] For example, the PACER database of federal court filings has a rather elaborate billing structure, which must require detailed tracking. PACER, http://www.pacer.gov (last visited Feb. 18, 2011) (charging $0.08 per page for court documents, but only for the first thirty pages (with some exceptions), and waiving fees for users whose quarterly bills would otherwise be $10 or less).

[15] *See, e.g.*, Frederick Lah, Note, *Are IP Addresses "Personally Identifiable Information"?*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 681, 693 & nn.68–69 (2008) (explaining that search engines track IP addresses to account for or prevent "click fraud," a false accrual of clicks on advertisements). Google defends its retention of search queries and their associated IP addresses as "tremendously helpful" for "protecting our networks from hackers, spammers, and fraudsters. For example, bad actors continually seek to manipulate our search ranking, launch denial-of-service attacks, and scam our users via email spam or malware. We use our log files to track, block, and keep ahead of the bad guys." *[Prepared] Testimony of Dr. Alma Whitten, Privacy Engineering Lead, Google Inc.*, S. COMM. ON COMMERCE, SCI. & TRANS., 9–10 (July 27, 2010), http://commerce.senate.gov/public/?a=Files.Serve&File_id=f67ebd69-a109-433b-ae34-abbcce06aa33 [hereinafter *Testimony of Dr. Alma Whitten*]. Fee-based online legal research system Westlaw tracks use to identify unusual or excessive uses that might suggest impermissible uses in violation of terms of service by law students limited to academic use. Telephone Interview with Jeff Rohlmeier, Director of Privacy and Compliance, Thomson Reuters (May 27, 2010) (notes on file with author).

[16] *See, e.g.*, *Simplifying Legal Research: Thomson Reuters Rolls Out WestlawNext at LegalTech*, 27 No. 10 LAW. PC 1 (Feb. 15, 2010) (describing how Westlaw product developers used "log analysis" of legal professionals doing legal research on Westlaw to identify and improve their system to support habits of researchers); *Testimony of Dr. Alma Whitten*, *supra* note 17, at 9 (defending Google's retention of search queries and their associated IP addresses, stating that "this data is actually tremendously helpful to us in improving our products").

[17] For example, Google publishes a Flu Trends report based on the geographical locations associated with IP addresses of individuals entering queries that Google assumes reflect a local case of the flu. *See Testimony of Dr. Alma Whitten*, *supra* note 17, at 10; *Flu Trends*, GOOGLE.ORG, www.google.com/flutrends (last visited Feb. 18, 2011).

[18] *See* Ron A. Dolin, *Search Query Privacy: The Problem of Anonymization*, 2 HASTINGS SCI. & TECH. L.J. 137, 142–44 (2010) (describing the utility of non-anonymized search data to search engines, to the individual user, to governments, and to society).

[19] Customizations are available to subscribers. *See, e.g.*, *Westlaw Advantage: My Westlaw*, WEST, http://west.thomson.com/westlaw/advantage/tools/my-westlaw/default.aspx (last visited Feb. 18, 2011).

[20] This IP or Internet Protocol address is represented by a series of numbers punctuated by periods. *See infra* note 25 and accompanying text.

[21] Microsoft Explorer and Mozilla Firefox are two commonly used browsers. *See* Nick Eaton, *IE Use Back Up, Firefox Use Down in June*, SEATTLE POST-INTELLIGENCER, (July 6, 2010), http://blog.seattlepi.com/microsoft/archives/213689.asp (reporting that Internet Explorer's market share for June 2010 was sixty percent and Mozilla Firefox's was twenty-four percent). Websites usually

These tracking practices are said to protect the anonymity of the researcher, but the integrity of IP address anonymity in particular has been challenged.[23] "Anonymization" and "personally identifying information" are terms of contested application in the context of online tracking, largely due to the risk of re-identifying individuals if anonymous data is merged with identifying data.[24] Even query information alone has been used to identify the individual researcher.[25] This problem can be exacerbated when an attorney conducts a "vanity search" of his own name in a search

automatically transfer "cookies" or short programs to the researcher's computer to report back information about the researcher's use of the website. "Session cookies" are erased when the browser is closed. "Persistent cookies" remain active whenever the browser is opened and for varying periods of time. Laura McCarthy & Dave Yates, *The Use of Cookies in Federal Agency Web Sites: Privacy and Recordkeeping Issues*, 27 GOV. INFO. Q. 231, 233 (2010). Flash cookies are a persistent variety of cookies not dependent on or controlled by most browsers that can be used to reinstall regular cookies researchers deleted through their browsers. Soltani et al., *supra* note 12, at 3–4 (reporting that more than 50% of 100 most visited websites used flash cookies and identifying a limited number of tools consumers can use to restrict deposit or to remove flash cookies).

[22] "Web bugs," also known as "beacons" or "clear GIFs," are programs that track activity on a website, including what the visitor types and where the mouse cursor moves on the webpage. Angwin, *supra* note 9 (examining the fifty most popular U.S. websites' use of cookies, flash cookies, and web bugs). "Web bugs" occupy a one-by-one pixel on the display of a webpage and so are effectively invisible to the website visitor. Gomez et al., *supra* note 9, at 8.

[23] Whether IP addresses are "personally identifying" is debated. Some cable and broadband internet subscribers now have static, assigned IP addresses, so those addresses can identify a subscriber's location, if not a particular user of the connection. Some researchers gain internet access via dynamic IP addresses that are assigned at each online session, so they might have a variety of IP addresses connected to their online activity and any identifying information. On the other hand, a single IP address may be used by different persons in the same household or by different persons who use wireless internet access at a retail site, such as a coffee shop. Dolin, *supra* note 20, at 149–50 (explaining how multiple users and multiple locations can obscure the ability to connect a particular researcher with an IP address, but demonstrating how IP addresses can be mapped to a location using public information); Lah, *supra* note 17, at 688–95, 699–704 (explaining how IP addresses work and noting disagreement about the ease or reliability of inferring identity from IP addresses); *see also* Joshua J. McIntyre, *The Number is Me: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. (forthcoming 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621102; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA. L. REV. 1701 (2010) (exploring more generally the problem of privacy law's reliance on anonymization in light of ease of re-identification); Dan Jerker B. Svantesson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet*, 23 J. MARSHALL J. COMPUTER & INFO. L. 101, 109–10 (2004) (describing how geo-locational services can build databases to identify the location associated with IP addresses). Examples of services that determine the location of an IP address—including that of visitors to their websites—include: WEBHOSTING.INFO, http://ip-to-country.webhosting.info (last visited Feb. 20, 2011); IP2LOCATION, http://www.ip2location.com (last visited Feb. 20, 2011); WHATISMYIPADDRESS.COM, http://whatismyipaddress.com (last visited Feb. 20, 2011); IP ADDRESS LOCATION, http://ipaddresslocation.org (last visited Feb. 20, 2011).

[24] Ohm, *supra* note 25, at 1704. *See infra* Part II.B.4.

[25] Consider the release by internet service provider AOL of the queries entered over a three month period and presumably rendered anonymous by the assignment of numbers in place of any other personal identifier. Searches for "landscapers in Lilburn, Ga," "dog that urinates on everything," "60 single men," and "numb fingers" were used to identify sixty-two year old Thelma Arnold. Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

engine because that name becomes part of the profile.[26] Similarly, if an attorney uses a search engine to see what information is retrieved in a search on the client's name, or if the attorney enters the client's name as part of the sign-on procedure for a fee-based service, all of the search data can be associated with the client's name.[27]

Most websites also regularly collect the "URL" or web address of a page that linked to them.[28] This information is called the "referring URL." Sometimes the referring URL contains information such as the name of a displayed document or the search query used on a search engine such as Bing or Google.[29] Sites also regularly collect the date and time that a researcher from a particular IP address visits their site.[30]

Some websites may retain user information indefinitely. Others may delete it or remove personally identifying elements after making use of the full records for billing, system improvement, or marketing purposes.[31] Data retention increases the chances of a security breach or other access, so short periods of retention help maintain confidentiality. Anonymization of user data is the next best approach.[32]

When tracking is done by the website a researcher visits, that data collection is considered "first party" tracking. In contrast, a "third party" would be a different entity

---

[26] Christopher Soghoian, *The Problem of Anonymous Vanity Searches*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 299 (explaining how anonymizing tools for internet use fail when researchers perform searches on their own names).

[27] For example, Westlaw sign-on includes a field for "Client ID." *Westlaw Sign-On*, Westlaw, https://web2.westlaw.com/signon/default.wl?newdoor=true (last visited Feb. 20, 2011). Of course, an attorney can use a code for the client so that identifying information is not shared with the research system.

[28] The very architecture of the World Wide Web incorporated an early interest of website owners in knowing how others linked to their sites, allowing information providers to discover "documents" that referred to them. *See* Tim Berners-Lee, *Information Management: A Proposal*, 4 (1989–1990), http://www.w3.org/History/1989/proposal.html (proposing a non-hierarchical hypertext linking system for information sharing with goals including answers to the question "What documents refer to this one?"). The referring URL is just one data element commonly collected from all visitors to websites using basic "web log" software or more sophisticated services such as Google Analytics. "[M]ost Internet service providers (ISPs) supply a freeware log analyzer with their web-hosting accounts." BRIAN CLIFTON, ADVANCED WEB METRICS WITH GOOGLE ANALYTICS 20–23 (2d ed. 2010) (explaining that page tags (a.k.a. web bugs) that work with cookies to collect information from website visitor's browsers have become a popular method for collecting website user data); *see also Google Analytics*, GOOGLE, http://www.google.com/analytics/ (last visited Aug. 26, 2010). Google may be able to confirm the author's visit on that date.

[29] For example, the results of a Google search for "companies manufacturing wind turbines" produced the URL "http://www.google.com/#hl=en&source=hp&q=companies+manufacturing+wind+turbines&aq=0&aqi=g10&aql=&oq=companies+manu&gs_rfai=Ct8kiFSN0TJXlJoGOzQSe7vEMAAAAqgQFT9CjvFs&fp=ad526d12389e3c08," and a Bing search for "hit and run laws" generated "http://www.bing.com/search?q=hit+and+run+laws&form=QBRE&qs=AS&sk=AS3&pq=hit+and+run+&sp=4&sc=8-12." If a researching attorney were to click on the advertisements displayed in the margin next to these searches' results, those advertisers could read within the linking URL the attorney's research topic, connecting that search query with the attorney's IP address and the time he or she clicked on the ad.

[30] Gomez et al., *supra* note 9, at 8.

[31] For example, Google has stated that it anonymizes IP addresses after nine months. *Testimony of Dr. Alma Whitten*, *supra* note 17, at 9.

[32] *But see* Dolin, *supra* note 20, at 142, 148, 152–54 (arguing that anonymization of search engine query records that link queries to IP addresses and potentially to individuals is both insufficient and unnecessary for privacy protection and an unwise tradeoff, as "it is difficult to overstate the vast number of potential uses for search query information, which are limited only by one's imagination").

with whom the website may share tracking information or whom the website may allow to collect information directly from its website visitors.[33] Researchers have some options for reducing tracking or the confidentiality-threatening effects of tracking by first party websites, but each precaution is insufficient in some way and must be updated in response to evolving tracker and tracker-blocking technologies.

¶3 As a first step, attorneys using subscription services can negotiate for contract terms that limit collection and reuse of data or that limit data retention or provide some level of anonymization of retained data. For fee-free websites, attorneys can look for similar reassurances in posted privacy policies and can avoid supplying personally-identifying information to the website. Another precaution would be to avoid linking to a website from search query results or a displayed document to prevent potential exposure to the new website of identifying confidential information in a referring URL. The attorney would have to cut and paste the address of the new website into the browser instead of linking to the site. A related strategy is to link only from web pages that provide encryption, since most browsers are configured to prevent transmission of the referring URL from encrypted web pages.[34] These precautions address collection and use of data by first party websites, but as the sections that follow show, additional precautions are necessary to address a variety of third parties who may track online research.

2. Third Party Advertisers

Attorneys' online legal research may be tracked by advertising companies placing ads through a network of websites on behalf of entities that wish to promote their products or services.[35] Online advertising is on the rise and provides the funding for many website services.[36] Some advertisements for third party products or services are

[33] In the context of attorney and client confidentiality, any person other than the attorney or client is generally referred to as a "third party." *See infra* Part III. Further confusion arises in the internet context in categorizing affiliates of the website visited. *See infra* Part II.B.3. For a humorous example of how these terms may be applied, see the contract scene from A NIGHT AT THE OPERA (MGM Studios 1925), *transcript available at* http://www.nightattheopera.net/contract.html.

[34] Google promises that use of its encrypted Search option usually triggers browser software to prevent the display of the referring URL from Google Search to a website linked from Google Search results. *SSL Search: Features*, GOOGLE, https://www.google.com/support/websearch/bin/answer.py?answer=173733&hl= en (last visited Feb. 20, 2011). Most search engines, however, including Bing and Google Scholar, did not offer an encrypted search option at the time of this writing.

[35] The Federal Trade Commission has focused attention on privacy and confidentiality issues relating to online behavioral advertising, and recommended guidelines for industry self-regulation in February of 2009. FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009) [hereinafter FTC STAFF REPORT ON BEHAVIORAL ADVERTISING], *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. In July of 2010, the FTC reported that industry self-regulation efforts were "still in their developmental stages" yet "encouraging." *FTC Statement on Consumer Online Privacy*, *supra* note 3, at 14.

[36] Increases in online advertising have been touted as a sign of a recovering economy. *WebVisible; Q2 Search Trends Signal Recovery – SMB Ad Spend Up 160 Percent Over a Year Ago, Job Recruitment Services and Luxury Categories Spending More, According to WebVisible Report*, MARKETING WEEKLY NEWS, Aug. 7, 2010. Google reports that their "products are free to individuals for personal use, supported by revenue from online advertising." *Testimony of Dr. Alma Whitten*, *supra* note 17, at 1.

delivered to any visitor to a particular website.[37] Increasingly, though, tracking is performed by network advertisers who collect information about a researcher's activity across multiple websites over some period of time to provide a personalized form of advertising.[38] This "behavioral marketing" attempts to develop a rich profile of consumer interests in order to match them with products and services.[39] For example, if an attorney searched a newspaper website for "hit and run" and then used a maps website to find more information about a particular location in Sacramento, the network advertising company working with these two websites could connect these two searches and attempt to match its advertising clients' products or services with this information. The attorney might see online advertisements for Sacramento law firms specializing in automobile accidents on any of the websites in the advertiser's network of websites.[40]

Some advertisers claim that they protect the privacy of online researchers by avoiding the use of "sensitive information" as a basis for targeted ads,[41] but definitions and practices vary,[42] and the wide range of issues involved in legal representation are poorly addressed through these types of exceptions to the use of data collected. While

[37] The Federal Trade Commission defines "contextual advertising" as "advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result." FTC STAFF REPORT ON BEHAVIORAL ADVERTISING, *supra* note 37, at iii. Cookies and web bugs can send information about website visitors directly to third parties. Angwin, *supra* note 9.

[38] The Federal Trade Commission has worked with advertisers and consumers to address conflicting interests relating to behavioral advertising. The FTC proposed a set of principles to guide industry self-regulation including: (1) transparency and consumer control, (2) reasonable security and limited data retention, (3) express consent from the consumer for material changes in privacy policies, and (4) express consent from the consumer before sensitive data such as data about children, health, or finances are used for behavioral advertising. FTC STAFF REPORT ON BEHAVIORAL ADVERTISING, *supra* note 37, at 11–12.

[39] Angwin & McGinty, *supra* note 3; Angwin, *supra* note 9; Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J., Aug. 4, 2010, at A1 (demonstrating the use of aggregated data about online activity and public records to profile potential credit card applicants); *see also* Center for Digital Democracy, U.S. PIRG, and World Privacy Forum, "In the Matter of Real-Time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy. Complaint, Request for Investigation, Injunction, and Other Relief: Google, Yahoo, PubMatic, TARGUSinfo, MediaMath, eXelate, Rubicon Project, AppNexus, Rocket Fuel, and Others Named Below," FTC filing, 8 Apr. 2010 [hereinafter *Complaint Before the FTC In the Matter of Real-Time Targeting*], *available at* http://www.democraticmedia.org/files/u1/20100407-FTCfiling.pdf (detailing and protesting integration of information about online browsing habits and offline information about individuals and other tracking practices for targeting marketing).

[40] This example illustrates the benefits of online tracking for attorneys who wish to advertise their services to potential clients.

[41] *See, e.g.*, *Testimony of Dr. Alma Whitten*, *supra* note 17, at 5 (testifying that "Google does not serve interest-based ads based on sensitive interest categories such as health status or categories relating to children under 13").

[42] The Federal Trade Commission has called for more specific standards on what constitutes sensitive information. FTC STAFF REPORT ON BEHAVIORAL ADVERTISING, *supra* note 37, at 44. Pending legislation would give highest protection to "sensitive information" defined as: (1) medical history, physical or mental health, or provision of health care to the individual; (2) race or ethnicity; (3) religious beliefs and affiliation; (4) sexual orientation; (5) financial information or records; and (6) precise geo-location information; (7) unique biometric data; and (8) social security number. "Building Effective Strategies to Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act" or BEST PRACTICES Act, H.R. 5777, 111th Cong. (2010) [hereinafter BEST PRACTICES Act], *available at* http://hdl.loc.gov/loc.uscongress/legislation.111hr5777.

such categories could add some level of protection for issues attorneys and their clients might address in online research, legal representation involves a variety of issues, not all of which are likely to qualify as "sensitive information."

Attorneys must adjust their research strategies and take a number of steps to implement technologies to block the tools of third party advertiser tracking. Mastering the privacy settings on internet browser software can limit a number of tracking tools either directly or indirectly.[43] Because tracking tools have adapted to elude these precautions, online researchers now have to take additional steps beyond electing browser settings.[44] A bevy of additional opt-out steps address tracking by particular third parties.[45] In addition, attorneys must confirm that subscription contracts and no-fee sites' privacy policies promise not to share with third parties the information they collect using first party tools. Of course, these precautions are effective only until the tools of tracking and counter-tracking are updated.

[43] Setting browsers to avoid collection of third-party cookies prevents the use of this tool and may disable web bugs as well. Gomez et al., *supra* note 9, at 4 ("Our analysis of web bugs revealed that they are ubiquitous on the web . . . and effective controls for this tracking technology are lacking."). "Web beacons cannot be removed or deactivated by the user because they do not reside on the user's computer. Some sites—such as Yahoo—offer users the ability to click on an 'opt-out' button, which blocks web beacons placed by the website." Francoise Gilbert, *Beacons, Bugs, and Pixel Tags: How the United States and Europe Regulate Behavioral Targeting* 702–03 (PLI Pats., Copyrights, Trademarks, & Literary Prop. Course, Handbook Ser. No. 969, 2009), *available at* 969 PLI/Pat 699. If web bugs work in conjunction with cookies, blocking or deleting cookies can disable the web bug. In addition, some developers have created programs that can be added onto particular browsers to disrupt the function of web bugs. Jennifer Valentino-Devries, *How to Avoid the Prying Eyes: The Internet is Rife with Surveillance Technology, but You Can Cover Some of Your Tracks*, WALL ST. J., July 31, 2010, at W3.

[44] "Flash cookies" are short programs downloaded from websites through Flash Player software and used to support animation and related media used by some websites. Flash cookies have been adapted to reinstall regular cookies after consumers delete them. Flash cookies themselves are not controlled by browsers, so researchers must take other steps to limit their use for third party tracking. Adobe, the maker of the Flash Player software, has updated its software to allow internet users to adjust settings on Flash Player to prevent third party tracking. *See Flash Player Security and Privacy*, ADOBE, http://www.adobe.com/products/flashplayer/security/ (last visited Feb. 23, 2011). In addition, several "plug-in" pieces of software are available to work with some browsers to allow varying levels of control over Flash cookies. Valentino-Devries, *supra* note 45.

[45] *See Opt Out of Behavioral Advertising,* NETWORK ADVERTISING INITIATIVE, http://networkadvertising.org/managing/opt_out.asp (last visited Aug. 30, 2010); Ng *supra* note 14, at 385 (noting that NAI opt-out does not cover all advertisers because not all have joined the consortium). Google's Ads Preferences Manager allows users to adjust their profiles or opt-out of receiving advertisements through Google's advertising services. This choice requires the downloading of an opt-out cookie that Google has said may not be cleared by the researcher's browser settings. See *Testimony of Dr. Alma Whitten*, *supra* note 17, at 5; *Privacy Center: Advertising and Privacy*, GOOGLE, http://www.google.com/privacy/ads (last visited Jan. 21, 2011). Some websites allow site visitors to opt-out of tracking by web bugs that are embedded on web page displays. *See* Gilbert, *supra* note 45, at 703. Google Analytics, a software and service provided by Google to websites for collecting "web log" analysis of site visitors and their visits, allows consumers to opt-out by going to Google's website. *See Google Analytics Opt-Out Browser Add-On Download Page*, GOOGLE, http://tools.google.com/dlpage/gaoptout (last visited Jan. 21, 2011).

More systemic approaches are available in the form of software designed to support an anonymous online presence.[46] Unfortunately, these systems have drawbacks and may not succeed in protecting anonymity from third parties.[47]

3. Website Affiliates

Some websites share information about site visitors with their corporate parent and sibling companies, all of whom may be considered "affiliates."[48] Whether affiliate access to information about individuals' online research habits is first party or third party access is murky territory, both in terms of the expectations of website visitors and the actual practices of website owners. For example, an attorney researching immigration law in LexisNexis might trigger the mailing of a flyer or sending of an email promoting a handbook on immigration law published by Matthew Bender, a legal publishing business managed by LexisNexis Group, the same business group that manages LexisNexis the online legal research company.[49] In this example, the attorney likely recognizes LexisNexis and Matthew Bender as connected and relevant to her legal research. This sharing might fit within the attorney's broad definition of a first party legal research service provider. But LexisNexis Group also contains LexisNexis Risk Holdings companies, including data aggregators and resellers long known as Choicepoint and Accurint, so these data resellers could be treated by LexisNexis Group as affiliates of the LexisNexis legal research service.[50] An attorney, however, might consider sharing legal

[46] Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1465–66 (explaining how Tor and TrackmeNot create some anonymity online and concluding that drawbacks have led to low use of these anonymizers).

[47] Christopher Soghoian points out that use of sophisticated tools to anonymize all internet use have steep costs to the user such as inability to take advantage of any cookie technologies or slowed communications. Soghoian also warns that selected use of encryption can draw attention from entities employing internet traffic analysis through wiretap or network level access to users' data. Soghoian, *supra* note 28 (commenting on the selected use of encryption and on implementation of tools such as Tor and TrackMeNot); Richard Abbott, *An Onion a Day Keeps the NSA Away*, J. INTERNET L., May, 2010, at 22, 27–28 (2010) (explaining that Tor does not work with all internet browsers and that "new users should consult an expert before trusting Tor with anything important"); *see also* Jeremy Clark, P.C. van Oorschot & Carlisle Adams, Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability (2007) (unpublished manuscript, presented at the Symposium on Usable Privacy and Security 2007), *available at* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.8672 (finding none of the deployment options for anonymizer Tor to be satisfactory from a usability perspective).

[48] *See* Gomez et al., *supra* note 9, at 4 (reporting that a majority of the fifty most visited U.S. websites posted policies stating site visitor information could be shared with affiliates, and reporting that parent companies for these websites had on average 297 subsidiaries that could be considered affiliates). For example, Google owns an advertising service called DoubleClick, *DoubleClick*, GOOGLE, http://www.google.com/doubleclick (last visited Aug. 11, 2010), and another such service is owned by Yahoo!, YAHOO! ADVERTISING SOLUTIONS, http://advertising.yahoo.com/media-kit/ (last visited Feb. 13, 2011). *See also* Tene, *supra* note 48, at 1447–50 (positing the possibility that Google Search could link query records with personally identifying information supplied by an individual who registers for affiliate services such as Gmail or Google Calendar).

[49] *See Company Profile, LexisNexis Group, Corporate Affiliations*, LEXISNEXIS CORPORATE AFFILIATIONS, http://corporateaffiliations.com/ (profile generated March 3, 2011).

[50] *Id*. The LexisNexis online legal research service privacy policy states that information it collects from website visitors is used to support the visitor's customer relationship with LexisNexis Group, not simply with the LexisNexis legal research service. *See LexisNexis Privacy Statement*, LEXISNEXIS, http://www.lexisnexis.com/privacy/statement.aspx (last visited Aug. 30, 2010). Whether this sort of sharing actually happens is a separate question. A spokesperson for LexisNexis stated that "[i]nformation

research details with these services to be more like sharing with a third party, particularly if the information shared could be added to a profile of the attorney or of the attorney's client in the data resellers' databases. So, while limiting tracking to first party collection and use of data may prevent exposure of data to unrelated third parties, the affiliate problem blurs the line between first and third party tracking.

4. Data Resellers

Aggregation and resale of data about individuals or households is another expanding business that could make use of search query and web search habits. The practices of data resellers or data brokers have been described as "opaque,"[51] but some evidence points to the potential for, and even current practice of, merging online tracking data with other information collected by data resellers.[52] This integration of data sets presents the opportunity for previously anonymous online tracking information tied only to IP addresses or browser identifiers to become tied to email addresses, street addresses, and other personal identifiers. The resulting profiles also present a threatening scenario for access to the topics, if not the details, of online legal research.

Data resellers generally assemble information from public records, information available publicly, and nonpublic information.[53] Established data brokers tend to limit access to their collected information to businesses and to governments.[54] Some data resellers, though, market their services through the internet to any purchaser willing to pay a fee.[55] Reseller Acxiom testified before a House subcommittee in 2009 that its practices exceeded industry standards for protection of consumer information.[56] Acxiom explained that it collected data from "public sources, self-reported data from consumers, and data from companies who sell products and services to consumers." [57] Acxiom defended its practices, stating that the company does not "sell detailed or specific

---

about an individual's use of LexisNexis legal research services is not shared with the Accurint service or any ChoicePoint service. Searches through the LexisNexis legal research service that access our public records databases are stored by LexisNexis Risk Solutions, which operates those public records databases. However, such searches are stored and used only for billing, data security and regulatory compliance purposes. Thus data about individuals' use of LexisNexis legal research service are never merged with data that are within the Accurint and Choicepoint databases used to offer services." E-mail from LexisNexis spokesperson to author (Sept. 8, 2010) (on file with author).

[51] *FTC Statement on Consumer Online Privacy*, *supra* note 3, at 18.

[52] *See* Whoriskey, *supra* note 13.

[53] *Identity Theft: Governments Have Acted to Protect Personally Identifying Information, but Vulnerabilities Remain: Testimony Before the Subcomm. on Info. Policy, Census & Nat'l Archives, Comm. on Oversight and Gov't Reform, H.R.*, 111th Cong. 10 (2009) (statement of Daniel Bertoni, Dir., Educ., Workforce, and Income Sec., U.S. Gov't Accountability Office), *available at* http://www.gao.gov/new.items/d09759t.pdf (explaining gaps in regulation of data resellers).

[54] *Id.*

[55] *Id.*; *see also* Jennifer Barrett, *Written Testimony of Acxiom Before the Subcommittee on Commerce, Trade & Consumer Protection and the Subcommittee on Communications, Technology & the Internet*H. COMM. ON ENERGY & COMMERCE 8 (Nov. 19, 2009) http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/111909_Privacy Joint Offline Online collection/Testimony/Barrett Testimony.pdf [hereinafter *Written Testimony of Jennifer Barrett, Acxiom*] (stating that reseller Acxiom "licenses data . . . to qualified businesses, non-profits, political organizations and candidates" and provides some of its services "directly to the consumer").

[56] *Written Testimony of Jennifer Barrett, Acxiom*, *supra* note 57, at 17.

[57] *Id.* at 2 (Executive Summary).

transaction-related information on individuals or households."[58] Acxiom further offered that it only provides access to sensitive information in some of its databases,[59] and "does not collect or acquire online browsing or search activity on consumers."[60] A complaint filed with the Federal Trade Commission, however, asserts that advertising companies are merging information from data resellers with proprietary online behavioral data to create targeted marketing "at the household level."[61] Just how far this merging of data and use of profiles has developed is not clear, but if the profiles can target a household, anonymity of online activity has been lost. This downstream use of online research data could mean an attorney's online search queries for hit-and-run law and maps of a Sacramento intersection might trigger a postcard from a local auto accident firm to be delivered to his home or office. Even more startling, these merged records and resulting profiles might be available for purchase by businesses, the government, and other attorneys.

5. Internet Service Providers

Internet service providers (ISPs) have a number of reasons to track the content of traffic that comes through their systems, including limiting malicious activity, managing heavy or light traffic, cooperating with copyright holders concerned about illegal access to proprietary material, and monetizing data reflecting their customers' activities on the internet.[62] ISPs have access to the full range of content traveling across their portion of

[58] *Id.* at 18. Acxiom either acquires or translates detailed customer data into "very general summary data that indicates possible lifestyle or interest intelligence" and does not "use detailed transaction data." *Id.* at 15.

[59] *Id*. at 7–8 (explaining that Acxiom did not provide sensitive information that could contribute to identity theft to its marketing customers, but did provide such information as a key part of "identity and risk solutions").

[60] *Id.* at 15. Acxiom did not explain whether this omission is a result of market factors such as the high cost of such information or whether forbearance was part of a policy that Acxiom described as exceeding industry standards for protection of consumer information. *Id.* at 17. Presumably, Acxiom would have to match data elements in the anonymous online browsing and search activity with data elements in other records to be able to link the formerly anonymous information with specific individuals or households. *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1455–1460 (explaining how anonymization is ineffective in protecting privacy of individual researchers).

[61] *Complaint Before the FTC In the Matter of Real-Time Targeting*, *supra* note 41, at 15. Data reseller Acxiom testified in November 2009 that seventy percent of the company's revenue came from "interactive marketing services and advertising solutions." *Written Testimony of Jennifer Barrett, Acxiom*, *supra* note 57, at 3.

[62] Armen Aghasaryan et al., *Personalized Application Enablement by Web Session Analysis and Multisource User Profiling*, BELL LABS TECHNICAL J., Jun. 2010, at 67 (outlining methods for internet, cell phone, and web television service providers to monetize access to individual subscribers' communications); Ohm, *supra* note 62, at 1423–27 (describing the motivations for ISPs to monitor the contents of communications passing through their systems); Mike Coward, *Deep Packet Inspection Optimizes Mobile Applications*, EDN, Oct. 8, 2009, at 37, *available at* http://www.edn.com/article/458406-Deep_packet_inspection_optimizes_mobile_applications.php (explaining how inspection of the contents of internet communications can allow service providers to prioritize or set tiered pricing by type of communication in order to address challenges to capacity of internet infrastructure); Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, at D1 (reporting that NebuAd, Phorm, and Front Porch data collection and network advertising companies were working with several internet service providers to track subscribers' internet activities). For more about the related "net neutrality" debate over whether internet service providers should be prevented from filtering or creating tiers of internet access based on deep packet inspection, see generally John G. Palfrey, Jr. & Robert Rogoyski, *The Move to the Middle: The*

the internet through a technique called "deep packet inspection."[63] If internet service providers were to track the online activity of attorneys, the impact to confidentiality would be severe, because these providers could review and retain the full record of websites visited, time of those visits, queries entered, and documents viewed, along with other online activities such as emails sent and received and documents shared electronically.

The researcher can prevent deep packet inspection by using encryption.[64] Website addresses that begin with "https" rather than "http" indicate the use of encrypted internet communications.[65] While some research websites such as LexisNexis, Westlaw, and Google Search allow for this encrypted communication,[66] a number of websites that attorneys use in developing legal advice for a client do not support encryption.[67] For example, twenty-seven state bar associations provide access to the legal research service Casemaker as a benefit of membership, but this service does not offer encrypted access.[68]

6. Government

The government can conduct its own sort of third party tracking of internet research by using law enforcement or national security tracking techniques. In addition, a wealth of law and policy information is published on government websites, so attorneys' legal research can be tracked by the government acting as a first party tracker when attorneys use those sites. To some extent, both of these government threats to attorney and client confidentiality raise different questions than commercial tracking does

---

Enduring Threat of "Harmful" Speech to the End-to-End Principle, 21 WASH. U. J.L. & POL'Y 31 (2006) (examining a trend toward regulation of internet communications intermediaries).

[63] Ohm, *supra* note 62, at 1437–40 (explaining how ISPs can monitor their subscribers' internet use).

[64] Encrypted internet communication is available through what is called the Secure Socket Layer protocol. *See* Ohm, *supra* note 62, at 1439.

[65] *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 375 (2010) (explaining the protections offered by "HTTPS encryption").

[66] See https://www.lexisnexis.com, https://web2.westlaw.com, and https://encrypted.google.com. Wikipedia, which attorneys and courts consult for a number of background topics relevant to client and litigation issues, provides encrypted access at https://secure.wikimedia.org/wikipedia/en/wiki/Main_Page. Regarding Factcase, *see infra* note 69.

[67] For example, Microsoft's search engine Bing (http://www.bing.com/) does not support encrypted searching, nor do legal research providers Casemaker (http://www.casemaker.us/) or Findlaw (http://www.findlaw.com/) or search service Google Scholar-Legal Opinions and Journals (http://scholar.google.com/). This lack of support likely stems from the fact that encryption can be difficult and expensive for the website owner, and may slow the communication process for the website visitor. *See* Ohm, *supra* note 62, at 1439; Soghoian, *supra* note 67, at 377–78.

[68] *See* CASEMAKER, http://www.casemaker.us (last visited Aug. 30, 2010). At the time of this writing, Casemaker has promised that it is working on providing encrypted access. Emails from Shannon R. Morris, Casemaker Customer Service Representative, to author (Aug. 30, 2010) (on file with author). Fastcase, a legal research service provided as a benefit of membership in seventeen states and other smaller bar associations, does support encryption at https://www.fastcase.com/. Robert J. Ambrogi, *Legal Research Pits Casemaker vs. Fastcase*, L. TECH. NEWS, July 31, 2009, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202432654587 (comparing features of Casemaker and Fastcase other than confidentiality); Greg Lambert, *Don't Know What Free Legal Resources Your State Bar Provides You? Here's a Map!*, 3 GEEKS & A L. BLOG (Mar. 9, 2010, 11:32 AM), http://www.geeklawblog.com/2010/03/dont-know-what-free-legal-resources.html.(displaying an interactive map of state bar associations' legal research service choices).

because constitutional, statutory, and policy protections against government collection and use of information operate separately from the law of private collection of data.[69] These issues are equally important to attorney and client confidentiality of legal research, but this article focuses on commercial tracking of online behavior, so these first and third party government tracking practices are reviewed only for their relationship to commercial tracking.

The tracking practices of government websites vary and may or may not be governed by law.[70] Executive policy for federal agency websites recently relaxed restrictions on the use of tracking devices such as cookies,[71] but the policy includes a number of protections that could preserve confidentiality of an attorney's legal research on these sites. Federal agency websites now track site visitors in order to measure use and to improve and customize site design, but agencies are restricted from sharing collected data with other agencies and may not cross-reference the data with any personally identifying information.[72] These restrictions on sharing and on identification of anonymous site visitors should protect the anonymity of research on these systems. For example, if an attorney researched a client company's filings on the U.S. Securities & Exchange Commission (SEC) website, the fact that she viewed those files on a particular date could be of evidentiary value in an SEC investigation. But the policy prevents the

---

[69] *See* Robert P. Mosteller & Kenneth S. Broun, *The Danger to Confidential Communications in the Mismatch Between the Fourth Amendment's "Reasonable Expectation of Privacy" and the Confidentiality of Evidentiary Privileges*, 32 CAMPBELL L. REV. 147, 188 (2010) (comparing Fourth Amendment and attorney-client privilege applications); William Wetmore, Note, *Hijacking the Privilege: Balancing Fairness and Security When Warrantless Wiretapping Threatens Attorney-Client Communications*, 2 HARV. L. & POL'Y REV. 187 (2008) (raising questions about warrantless wiretapping for national security and the threat to attorney-client confidential communications); *see also* Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 310–315 (2008) (describing current oversight of government surveillance under federal statutes as ineffective "privacy theater" and arguing for specific reporting requirements). Professor Kenneth W. Graham Jr. has suggested that attorney-client privilege may not survive government surveillance if the attorney or client has reason to believe the surveillance is occurring, but that if the client cannot prevent government surveillance, the privilege might yet apply to prevent use of the information at trial. 24 CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE, FEDERAL RULES OF EVIDENCE § 5484 (West 2010).

[70] A number of states require privacy policies and procedures for their government websites. *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 41-4151, 41-4152 (2010); TEX. GOV'T CODE ANN. § 2054.126 (West 2010); VA. CODE ANN. § 2.2-3800-03 (2010). The National Conference of State Legislatures maintains a list of state statutes addressing privacy policies for state government websites, last updated October 19, 2009. *State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13463#govpolicies (last visited Aug. 25, 2010).

[71] A federal executive policy limiting tracking tools on agency websites was relaxed in June of 2010. "For government agencies, the potential benefits of web measurement and customization technologies are clear. With the help of such technologies, agencies will be able to allow users to customize their settings, avoid filling out duplicative information, and navigate websites more quickly and in a way that serves their interests and needs. These technologies will also allow agencies to see what is useful to the public and respond accordingly. Services to customers and users can be significantly improved as a result." Memorandum from Peter R. Orszag, Dir., Off. of Mgmt. & Budget, Exec. Off. of the President, to the Heads of Exec. Dep'ts and Agencies, M-10-22, 1 (June 25, 2010) [hereinafter *Federal Agencies Website Memorandum*], *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf; *see also* McCarthy & Yates, *supra* note 23 (exploring the implications of planned expansion of tracking of visitors to federal agency websites).

[72] *Federal Agencies Website Memorandum*, *supra* note 73, at 4.

SEC from tracing the IP address in order to connect the files viewed with the attorney and client.[73] This example serves as a possible model for terms of use that attorneys might seek with commercial research websites.

Because internet service providers may try to monitor and monetize the details of the full range of online activity, government website use can become the subject of commercial tracking. If the government website offers encrypted access, however, the ISP is unable to track research details. The PACER database containing court filings for most federal courts is a good example of a government site that supports encryption,[74] but a number of government websites used by lawyers do not provide the confidentiality protection of encrypted connections. For example, the Supreme Court of the United States site, the Thomas website of federal legislative information, and the GPO Access website with federal regulations all fail to support encryption.[75]

Another interaction between government data collection and commercial tracking of online legal research is the potential for stored user data to be made available to government for a variety of purposes. Government may use legal process to obtain tracking information from commercial entities such as websites and internet service providers for law enforcement and national security purposes.[76] Depending on the commercial entity's practices, government may acquire information about online activity through a simple request or by purchasing the data.[77] Google has posted a map to report the number of government requests it has received for data about the use of some Google services through any of these methods.[78] The federal government is reportedly a large customer for many commercial data brokers[79] and has sought information about internet

---

[73] *But see* Soltani et al., *supra* note 12, at 4 (reporting that the Whitehouse.gov site disclosed tracking technology but did not specify that Flash cookies were used).

[74] In fact, PACER allows only encrypted access to its system. *See, e.g.*, PACER, https://pacer.login.uscourts.gov/cgi-bin/login.pl (last visited Aug. 30, 2010).

[75] *See, e.g.*, SUPREME COURT OF THE UNITED STATES, http://www.supremecourt.gov/ (last visited Aug. 30, 2010); THOMAS, LIBRARY OF CONGRESS, http://thomas.loc.gov (last visited Aug. 30, 2010); GPOACCESS, U.S. GOV'T PRINTING OFFICE, http://www.gpoaccess.gov/ (last visited Aug. 30, 2010). Over nineteen percent of attorneys in the United States report that a government website is the free website they use most often for legal research. 2010 AMERICAN BAR ASSOCIATION LEGAL TECHNOLOGY SURVEY REPORT, ONLINE RESEARCH VOL. 5, at 43 (2010). Just under five percent of attorneys report regularly beginning their legal research on government websites. *Id.* at 39.

[76] *See infra* Part II.D on the law of tracking.

[77] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (chronicling law enforcement access to some website and data broker information and citing to documents obtained by privacy advocacy organization EPIC through Freedom of Information Act requests detailing FBI reliance on records available through public records aggregator Choicepoint (citing *Choicepoint*, EPIC, http://epic.org/privacy/choicepoint/ (last visited Aug. 26, 2010))).

[78] *See Government Requests—Google Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/governmentrequests/ (last visited Aug. 11, 2010). The number of requests for disclosure of user data from United States government agencies between July 1, 2009 and December 31, 2009 was 3,580. Most of these requests are reported to be related to criminal investigations. *FAQ – Google Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/faq (last visited Aug. 29, 2010).

[79] Accurint markets itself as "the most widely accepted locate-and-research tool available to government, law enforcement and commercial customers." ACCURINT, http://www.accurint.com/hr (last visited Feb. 16, 2011). A whole set of Accurint services is marketed specifically to government through Accurint for Government. These services are touted as being "[u]sed by more than 3,000 agencies across

browsing records for national security and law enforcement purposes and defense of legislation.[80]

Attorneys can adopt the contractual and technological precautions already discussed to limit commercial access to government website use and to limit government access to online research details that could be collected and stored by first party and third party commercial tracking. To secure a greater level of protection by first party commercial legal research systems, attorneys could negotiate for assurance that, when legally possible, the provider will contact the subscriber before complying with government requests for information that describes the attorney's use of the service.

7. Bad Actors

Bad actors intent on spreading destructive software, collecting information for the purpose of identity theft or trade secret theft, or otherwise disrupting online traffic could find ways to track online legal research.[81] Malicious tracking flourishes through flaws in security, so the best precautions are steps to reduce third party tracking in general and to avoid websites that deliver malicious tracking tools. Virus or malware protection software, particularly a program that integrates with a browser, can warn of potentially harmful sites.[82]

---

the country." *Accurint for Government*, LEXISNEXIS INVESTIGATIVE SOLUTIONS, http://www.lexisnexis.com/government/solutions/investigative/accurint.aspx (last visited March 3, 2011).

[80] Ellen Nakashima, *White House Proposal Would Ease FBI Access to Records of Internet Activity,* WASH. POST, July 29, 2010, at D1 (reporting that some internet service providers have resisted the FBI's use of national security letters to obtain data about internet browsing histories because it is not clearly authorized under current law) ("One senior administration government official, who would discuss the proposed [legislative] change only on condition of anonymity, countered that 'most' Internet or e-mail providers do turn over such data."); *see also* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards,* 94 MINN. L. REV. 1514, 1543–44 (2010) (noting the types and low number of law enforcement requests for internet service provider records that could be considered fishing expeditions).

[81] Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent,* 43 VAND. J. TRANSNAT'L L. 57, 79–80 (2010) (describing vulnerabilities of the internet to a variety of malicious tools that track or worse); *see also [Prepared] Testimony of Ari Schwartz, Deputy Director, Center for Democracy and Technology, before the Financial Services and General Government Subcommittee of the House Committee on Appropriations, on "Consumer Protection Issues"*, CDT, 1–2 (Feb. 28, 2007), http://old.cdt.org/privacy/20070228schwartzftc.pdf (advocating increased support to the Federal Trade Commission to combat the threat to online commerce and expression from increases in malicious online tracking); Wayne R. Barnes, *Rethinking Spyware: Questioning the propriety of Contractual Consent to Online Surveillance,* 39 U.C. DAVIS L. REV. 1545, 1558–62 (2006) (describing how spyware can track keystrokes and so all the information about online and offline activities on one's computer).

[82] Daniel E. Harmon, *Effective PC Defense: Expert Guardians Are Emerging, But Smart Computing is Central*, LAW. PC (Thompson Reuters/West, St. Paul, MN), May 15, 2010, at 1 (recommending security features for software that screens and removes malware).

C. The Law Governing Online Tracking

Commercial tracking of internet use is minimally regulated. Website privacy policies, required by a few states[83] and investigated by the Federal Trade Commission if found to be unfair or deceptive,[84] provide insights into tracking practices linked to particular websites, but in general, these policies are criticized as confusing, incomplete, difficult to locate,[85] of unclear contractual status, and easily changed, even retroactively.[86] Subscription-based online research services, especially legal research services whose primary clients are attorneys or even bar associations, provide more opportunity for negotiation and enforcement of confidentiality-protecting contractual protections. Other laws have limited or unclear effect on tracking internet research. Minnesota and Nevada prohibit internet service providers from reselling personally identifying information about their customers, and the Minnesota statute goes so far as to require the customer's authorization before most instances of sharing information about search queries and information viewed, but the vast majority of states have no such law.[87] Scholars have proposed tort or property remedies, but these approaches have not been

[83] CAL. BUS. & PROF. CODE §§ 22575–79 (West 2009) (requiring prominent posting of a policy which outlines collection of particular types of information and describes any third-party uses); CONN. GEN STAT. *§ 42-471*(2010) (requiring privacy policy for websites that collect social security numbers).

[84] Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices in the marketplace. 15 U.S.C. §§ 41–58 (2006). For information relating to FTC enforcement of website privacy policy cases, see *Privacy Initiatives: Enforcement*, FEDERAL TRADE COMM'N, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Aug. 11, 2010). At least two states also have statutes that prohibit making a false or misleading statement in a privacy policy displayed on a website. *See* Neb. Rev. Stat. § 87-302(14) (2009); 18 PA. CONST. STAT. § 4107(a)(10) (2010).

[85] Ty Tasker & Daryn Pakcyk, *Cyber-Surfing on the High Seas of Legalese: Law and Technology of Internet Agreements*, 18 ALB. L.J. SCI. & TECH. 79 (2008) (critiquing website policies and terms that are difficult for site visitors to find); Soltani et al., *supra* note 12, at 4 (finding website installation of tracking tools known as flash cookies was rarely disclosed in privacy policies of sample websites).

[86] The applicability of contract law to website privacy policies has been rejected by a number of scholars. *See, e.g.*, Haynes, *supra* note 13 (noting that consumers are most likely to dispute rather than support contractual validity of website privacy policies that give notice of broad collection and use of consumer data); Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 475–76 (2006) (arguing that "browsewrap" online terms of use that do not require the consumer to click through the terms fail to establish consumer agreement and should not be enforced as a contract against the unsuspecting consumer). *But see*, Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1 (2009). Website privacy policies that reserve the right to change the terms unilaterally may be unenforceable. *See* Peter A. Alces & Michael M. Greenfield, *They Can Do What!? Limitations On The Use Of Change-Of-Terms Clauses*, 26 GA. ST. U. L. REV. 1099, 1130–45 (2010) (arguing that reservation of the right to alter contract terms should be presumptively unenforceable and noting such terms in the terms of use of internet service provider Comcast, online legal research systems LexisNexis and Westlaw, and internet seller of books and other things Amazon, among others).

[87] *See* MINN. STAT. § 325M.01–09 (2011). This law requires "the authorization of the consumer" before the internet service provider may disclose "personally identifiable information," except in certain situations. MINN. STAT. § 325M.03–04. "Personally identifiable information" is defined in Minnesota to include "Internet or online sites visited by a consumer," any information that identifies "a consumer as having requested or obtained specific materials or services from an Internet service provider," and the consumer's "physical or electronic address or telephone number." MINN. STAT. § 325M.01.

widely tested.[88] Any sectoral privacy laws that apply online offer insufficient confidentiality for the range of topics attorneys may research on behalf of their clients.[89]

Fourth Amendment and First Amendment protections might provide limits on government access to commercially collected information about online research, but scholarly proposals have not yet produced doctrine that clarifies this intersection of protections.[90] Fourth Amendment precedent provides minimal barriers to government access to information voluntarily shared with commercial parties,[91] although the application of this "third-party doctrine" to the content of information sought and viewed online is not clear.[92] National security investigations are limited by more relaxed

[88] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 125–27 (2007) (arguing that the English tort of confidentiality could inform U.S. privacy law); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (proposing a property model for personal information that would protect information privacy); Michael R. Siebecker, *Cookies and the Common Law: Are Internet Advertisers Trespassing on Our Computers?* 76 S. CAL. L. REV. 893, 894 (2003) (arguing that cookies stored on a user's computer may constitute a trespass to chattels); *see also* Max Stul Oppenheimer, *Internet Cookies: When is Permission Consent?* 85 NEB. L. REV. 383, 403–04 (2006) (describing government use of a cookie to collect information from a corporate visitor to a government website as a taking of a trade secret).

[89] *See, e.g.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006).

[90] Neil M. Richards, *Intellectual Privacy,* 87 TEX. L. REV. 387 (2009) (arguing that privacy of search engine use and other actions or expressions revealing intellectual activity should be protected by the First Amendment); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U.L. REV. 112 (2007) (arguing that the intersection of First and Fourth Amendments should produce heightened protection against government access to speech records such as search queries and ISP records of anonymous speakers); *see also* Julie Cohen, *A Right to Read Anonymously: A Close Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (advocating statutory protection for First Amendment values threatened by commercial tracking of readers); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002) (arguing for both federal and state constitutional protection for information privacy).

[91] Under the "third party doctrine" of the Fourth Amendment no reasonable expectation of privacy protects from government intrusion the "voluntary" disclosures of information to a third party. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."); *see also* City of Ontario, Cal. v. Quon, 130 S.Ct. 2619 (2010) (declining to determine whether a reasonable expectation of privacy in the online environment of a public employer supplied text messaging service, explaining that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior"); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Gathering in the War on Terror*, 96 CAL. L. REV. 901 (2008) (examining the ease with which government can obtain data from commercial sources such as data brokers and online service providers).

[92] Orin S. Kerr, *Applying The Fourth Amendment To The Internet: A General Approach,* 62 STAN. L. REV. 1005 (2010) (arguing that a content/envelope distinction should apply to information communicated through the internet and that warrants specifying particular persons should be required for government access to this content). *But see* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009) (proposing constitutional protection for content-revealing IP addresses or URLs of websites an online research visits). Law enforcement nonetheless seeks greater ease of access to information including requiring internet service providers to retain records of browsing history for two years and to share that data when presented with a national security letter, a form of administrative subpoena. *See* Delcan McCullagh, *FBI Wants Records Kept of Web Sites Visited,* CNET NEWS, Feb. 5, 2010, http://news.cnet.com/8301-13578_3-10448060-38.html (reporting FBI's call for legislation to require internet service providers to collect and retain browsing records for subscribers for at least two years); Nakashima, *supra* note 82 (reporting on executive branch requests for amendment to the Electronic

standards under the Fourth Amendment and under various statutes, including provisions that would prevent cooperating parties from revealing that they have disclosed data to the government.[93] Other legal restraints on monitoring online activity include the Electronic Communications Privacy Act[94] and the Stored Communications Act,[95] but these laws were written for older technologies, and their utility in the evolving symbiotic web has been questioned, particularly when the data collector is agreeable to sharing tracking data.[96] Attorney-client privilege itself may bar government access to or use of commercially collected legal research records, but the research must have been performed under conditions that meet privilege standards for confidentiality.[97]

Legislation has been introduced to provide greater transparency and more consumer control over the collection of data about their online research.[98] Agencies have angled for authority over online privacy or confidentiality,[99] and the Federal Trade Commission in particular has been active in investigating related complaints and publishing guidelines to support industry self-regulation.[100] But the stakes are high for information collectors both commercial and governmental, and consumers are only just

---

Communications Privacy Act to allow law enforcement access to internet browsing records without court involvement).

[93] *See* Fred H. Cate, *Government Data Mining: The Need for A Legal Framework,* 43 HARV. C.R.-C.L. L. REV. 435, 444–51 (2008) (reviewing national security laws governing access to individuals' information).

[94] 18 U.S.C. § 2510 (2006).

[95] 18 U.S.C. §§ 2701–2712 (2006).

[96] If one of the parties to a communication consents to disclosure, the Electronic Communications Privacy Act is not violated. 18 U.S.C. § 2511(a). *See In re* Doubleclick, 154 F. Supp. 2d. 497 (S.D.N.Y. 2001) (finding that website owners had consented to advertisers' collection of user data and finding no violation of the Electronic Communications Act, Stored Communications Act or Computer Abuse and Fraud Act); *In re* Pharmatrack, 329 F. 3d. 9 (1st Cir. 2003) (holding that neither users nor website consented to range of data collected by advertiser). *But see In re* Pharmatrack, Inc. Privacy Litigation, 292 F.Supp. 2d 263 (D. Mass. 2003) (finding on remand that advertiser did not have intent required for violation of Electronic Communications Act); Ohm, *supra* note 62, at 1477–89 (arguing that the Electronic Communications Act may prevent many forms of monitoring by internet service providers but that the statute also needs to be updated); Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (outlining and identifying gaps in the Stored Communications Act).

[97] Mosteller & Broun, *supra* note 71.

[98] Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act' or the "BEST PRACTICES Act," H.R. 5777, 111th Cong. (2010); *Boucher-Stearns Staff Discussion Draft: A Bill to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual* H. COMM. ON ENERGY & COMMERCE (May 3, 2010), http://democrats.energycommerce.house.gov/documents/20100719/BoucherStearnsprivacydiscussiondraft.pdf.

[99] Federal Trade Comm'n, Comments In the Matter of Info. Privacy & Innovation in the Internet Econ., Before the Nat'l Telecomm. Info. Admin., U.S. Dept. of Commerce (June 7, 2010), *available at* http://www.ntia.doc.gov/comments/100402174-0175-01/attachments/FTC%20Comments.pdf (pointing out overlapping interests of the Department of Commerce, the Federal Communications Commission and the Federal Trade Commission in regulating privacy in the online environment).

[100] FTC STAFF REPORT ON BEHAVIORAL ADVERTISING, *supra* note 37. A number of relevant enforcement actions are chronicled by the Federal Trade Commission on their website. *See Privacy Initiative*, FEDERAL. TRADE COMM'N, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Aug. 29, 2010).

beginning to appreciate the extent to which their personal information is tracked and used, so any new legislative or regulatory approaches face conflicts among these various stakeholders.

D. The Need for Technology in Market Solutions

Because commercial tracking of internet legal research is not effectively limited by law, attorneys and their clients must rely on technological control and market influence to protect confidentiality. The previous overview of online tracking identified some counter-tracking strategies for individual attorneys, but these precautions are cumbersome and ever-evolving and may not provide enough protection to meet requirements under the law and rules of attorney and client confidentiality. The next section considers how the law and rules of confidential legal representation might address online research that is tracked. Following that analysis, a summary of reasonable precautions is proposed, as well as recommendations for collective efforts that can help individual attorneys create and preserve a confidential environment for online research.

III. CONFIDENTIALITY INTERESTS IN LEGAL RESEARCH

A. Two Threats from Online Tracking

The law and rules of attorney and client confidentiality indicate that tracking presents two threats. First, tracking could prevent recognition of the online environment as a place where a reasonable expectation of confidentiality is possible. The second threat is that tracking will produce a limited or general disclosure that constitutes waiver of privilege and work product and violates the attorney's ethical commitment to confidentiality.

B. Attorney-Client Privilege

The attorney-client privilege is recognized in every state and federal jurisdiction in the United States[101] and is the oldest communications privilege in the United States,[102] with over five hundred years of recognition at common law.[103] Like other evidentiary privileges, the attorney-client privilege allows "a person who communicated in confidence or who possesses confidential information to shield the communication of information from compelled disclosure during litigation."[104]

---

[101] GRAHAM C. LILLY, PRINCIPLES OF EVIDENCE 325 (4th ed. 2006); EDWARD J. IMWRINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE: EVIDENTIARY PRIVILEGES, app. D (2d ed. 2010) [hereinafter THE NEW WIGMORE] (identifying relevant statutes in rules in the states).

[102] *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (citing 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2290 (McNaughton rev. 1961)).

[103] 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2290 (McNaughton rev. 1961).

[104] THE NEW WIGMORE, *supra* note 103, at § 1.1 (describing the operation of evidentiary privileges).

Most states have codified the privilege as a rule of evidence.[105] In federal courts, when federal law applies, Federal Rule of Evidence 501 directs that the law of privileges "shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience."[106]

The attorney-client privilege may serve a number of purposes. The generally accepted purpose is to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice."[107] Other justifications relate to recognition of the attorney's moral duty to maintain confidentiality of the client relationship or respect for autonomy of the client through protection of the fiduciary nature of the attorney's role.[108]

The privilege is held by the client, and the attorney has a duty to protect the confidentiality of the communications to preserve the privilege.[109] In federal court, the application of the privilege is said to be a "question of fact, to be determined in the light of the purpose of the privilege and guided by judicial precedents."[110] The federal common law and the law of the states on attorney-client privilege have produced some jurisdictional variations on the scope and application of attorney-client privilege.[111]

In a much-cited opinion from 1978, the Fifth Circuit held that one who claimed attorney-client privilege must establish the following elements:

(1) the asserted holder of the privilege is or sought to become a client;
(2) the person to whom the communication was made
    (a) is (the) member of a bar of a court, or his subordinate and
    (b) in connection with this communication is acting as a lawyer;
(3) the communication relates to a fact of which the attorney was informed
    (a) by his client
    (b) without the presence of strangers
    (c) for the purpose of securing primarily either

---

[105] *See, e.g.*, OR. REV. STAT. §40.225 (2007); CAL. EVID. CODE § 952 (West 2010). For a chart of state privilege laws, *see* THE NEW WIGMORE, *supra* note 103, at app. D.

[106] FED. R. EVID. 501. Rule 503 specifically outlining the contours of the attorney-client privilege was promulgated by the Supreme Court but not enacted by Congress which favored the more flexible common law approach of Rule 501. Prop. Fed. R. Evid. 503, reprinted in 56 F.R.D. 183 (1972).

[107] *Upjohn*, 449 U.S. at 389; *see also In re* Grand Jury Investigation, 399 F.3d 527, 531–32 (2d Cir. 2005); United States v. Kovel, 296 F.2d 918, 921 (2d Cir. 1961) (citing Jessel, M.R. in Anderson v. Bank, 2 Ch. D. 644, 649 (1876)); WIGMORE, *supra* note 105, § 2290. Another purpose, not often recognized by modern courts, is linked to the historical barrister's code of honor, loyalty, and fairness. *See In re Grand Jury Investigation*, 399 F.3d at 531 (comparing JOHN W. STRONG, MCCORMICK ON EVIDENCE § 87, at 343–46 (5th ed. 1999) with CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE § 5472, at 71–77 (1986) on whether the honor purpose co-exists with the utilitarian purpose or was supplanted by it). When the attorney's honor held sway as the dominant rationale, the privilege was available only to the attorney, so the client had no claim for confidentiality of communications with his attorney. WIGMORE, *supra* note 105, § 2290.

[108] Professor Edward J. Imwrinkelried is a proponent of the client autonomy justification as a humanistic normative approach. THE NEW WIGMORE, *supra* note 103, § 5.3.3.

[109] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 68(c), 86 (2000).

[110] *In re* Auclair, 961 F.2d 65, 68 (5th Cir. 1992).

[111] *See, e.g.*, FED. R. EVID. 501, which states that privileges such as attorney-client are "governed by the principles of the common law as they may be interpreted by the courts of the United States in light of reason and experience."

(i) an opinion on law or
(ii) legal services or
(iii) assistance in some legal proceeding, and not
(d) for the purpose of committing a crime or tort; and
(4) the privilege has been
(a) claimed and
(b) not waived by the client.[112]

The Restatement of the Law Governing Lawyers adopted in 2000 describes the elements of attorney-client privilege as "(1) a communication (2) made between privileged persons (3) in confidence (4) for the purpose of obtaining or providing legal assistance for the client."[113] This later articulation reflects the evolution of the privilege to embrace not just communications from the client to the attorney, but all communications between the attorney and client.[114]

The attorney-client privilege has also evolved to embrace sharing confidential communications with some categories of persons other than the attorney and client.[115] The traditional rule is that third party access to otherwise-privileged information prevents the establishment of or constitutes waiver of confidentiality.[116] However, a number of exceptions have been recognized. Confidentiality is maintained despite the sharing of privileged information with a subordinate[117] or agent[118] of the attorney, the functional equivalent of the client's employees,[119] or someone necessary to the provision of legal

[112] United States v. Kelly, 569 F.2d 928, 938 (5th Cir. 1978), *cert. denied*, 439 U.S. 829 (1978).

[113] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §68 (2000).

[114] Protection of attorney communications to clients was already in development in the federal courts at the time of United States v. Kelly. *See* Mead Data Central v. U. S. Dept. of Air Force, 566 F.2d 242, 254 n.25 (D.C. Cir. 1977) (privilege protects communications from attorney to client as well as from client to attorney); Gregory C. Sisk & Pamela J. Abbate, *The Dynamic Attorney-Client Privilege*, 23 GEO. J. LEGAL ETHICS 201, 217 n.92 (2010) (noting changes in the scope of attorney-client privilege).

[115] Michele DeStafano Beardslee, *The Corporate Attorney-Client Privilege: Third-Rate Doctrine for Third-Party Consultants*, 62 SMU L. REV. 727 (2009) (arguing for application of the privilege to communications shared with third-party consultants whenever the nexus between outside expertise and legal advice is strong); Mark D. Hinderks, *Attorney-Client Privilege: The Presence of Third Parties Necessary to Facilitate Attorney-Client Communication or Legal Advice*, 76 J. KAN. B. ASS'N 16 (2007) (reviewing cases in which third parties have been embraced by the attorney-client privilege).

[116] WIGMORE, *supra* note 105, § 2317.

[117] United States v. Kovel, 296 F.2d 918, 921–22 (2d Cir. 1961) (holding accountant's involvement in attorney-client communications did not waive the privilege because expertise allowed lawyer to give better legal advice). "[T]he complexities of modern existence prevent attorneys from effectively handling clients' affairs without the help of others; few lawyers could now practice without the assistance of secretaries, file clerks, telephone operators, messengers, clerks not yet admitted to the bar, and aides of other sorts." *Id.* at 921.

[118] *Id.* ("[T]he privilege must include all the persons who act as the attorney's agents.") (quoting WIGMORE, *supra* note 105, § 2301; Annot., 53 A.L.R. 369 (1928)). *See also Kelly*, 569 F.2d at 938 (distinguishing between communications shared with a subordinate of the attorney and those shared with strangers).

[119] *See, e.g.*, In re Bieter Co., 16 F.3d 929, 938 (8th Cir. 1994). In some circumstances, an employee of the client communicating with the attorney may be considered covered by the privilege. Gifford v. Target Corp., Civ. No. 10-1194, 2010 WL 2771896, at *8 (D. Minn. 2010) (citing Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 609 (8th Cir. 1977)).

advice.[120] Foreign language translators, accountants, appraisers, financial consultants, engineers, and even public relations consultants have been found to be necessary to informed provision of legal advice and not therefore destroyers of privilege.[121]

An attorney's consultation of a legal research tool or service should easily meet a test of necessity in the rendering of legal advice.[122] For some types of research, courts have held that consultation of internet-based research tools is a necessary part of due diligence. Certainly, lawyers are using online research tools on a regular basis, with a majority reporting that they regularly begin legal research using online sources.[123]

Courts have held that attorney-client privilege protects legal research,[124] legal research memoranda,[125] and bills detailing cost and content of legal research.[126] The

[120] *See, e.g.*, Westinghouse Electric Corp. v. Republic of the Phil., 951 F.2d 1414, 1425 (3d Cir. 1991) ("The traditional waiver doctrine provides that disclosure to third parties waives the attorney-client privilege unless the disclosure serves the purpose of enabling clients to obtain informed legal advice."); Exp.-Imp. Bank of U. S. v. Asia Pulp & Paper Co., 232 F.R.D. 103, 113 (S.D.N.Y. 2005) ("[C]ommunications with a financial advisor are covered by the attorney-client privilege if the financial advisor's role is limited to helping a lawyer give effective advice by explaining financial concepts to the lawyer." (citing *Kovel*, 296 F.2d at 922)).

[121] *See* In re Grand Jury Investigations, 918 F.2d 374, 384 (3d Cir. 1990) ("[T]he presence of third parties, if essential to and in furtherance of the communication, should not void the privilege."); Hawes v. State, 7 So. 302, 313 (Ala. 1890) ("It is equally well established law that an interpreter, intermediary, agent, or clerk of an attorney, through whom communications between attorney and client are made, stands upon the same footing as his principal, and will not be allowed to divulge any fact coming to his knowledge as the conduit of information between them."); *see also* Beardslee, *supra* note 117; WIGMORE, *supra* note 105, §§ 2301, 2311. Instances of sharing with third parties necessary for the rendering of legal advice have been called "facilitative revelations." CHARLES ALAN WRIGHT & KENNETH W. GRAHAM, JR., 24 FEDERAL PRACTICE AND PROCEDURE § 5485 (2010)(Westlaw).

[122] The author concedes her bias as a law librarian.

[123] Thirty-four percent of attorneys responding to a recent American Bar Association survey begin a research project using internet/online services that are fee-based, and forty-four percent of respondents begin research projects using internet/online services that are free. AM. BAR ASS'N LEGAL TECH. RESOURCE CENTER, 2010 LEGAL TECHNOLOGY SURVEY REPORT: ONLINE RESEARCH (vol. V), at 21 (2010). Some courts have suggested due diligence requires online research, including research of the internet using a search engine such as Google. *See, e.g.*, Davis v. Dept. of Justice, 460 F.3d 92, 103 (D.C. Cir. 2006) (questioning the adequacy of FBI search techniques in identifying parties relevant to documents requested under FOIA, stating "one has to ask why—in the age of the Internet—the FBI restricts itself to a dead-tree source . . . . Why, in short, doesn't the FBI just Google the [two parties]?"); Munster v. Groce, 829 N.E.2d 52, 62 n.3 (Ind. App. 2005) (dismissing claim for insufficient service of process because of failure to prove due diligence where court found a Google search would have produced a potential lead for missing litigant); Dubois v. Butler, 901 So.2d 1029, 1031 (Fla. App. 2005) (dismissing on insufficient service of process grounds because of lack of due diligence in failure to use, among other things, the internet or other modern technology to conduct search). *See also* Hagopian v. Justice Admin. Comm'n, 18 So. 3d 625, 642 (2009) ("Lawyers have also become expected to use computer-assisted legal research to ensure that their research is complete and up-to-date." (citing Michael Whiteman, *The Impact of the Internet and Other Electronic Sources on an Attorney's Duty of Competence Under the Rules of Professional Conduct,* 11 ALB. L.J. SCI. & TECH. 89, 103 (2000))); Carol Levitt & Mark Rosch, *Making Internet Searches Part of Due Diligence*, 29 LOS ANGELES LAWYER 46 (2007).

[124] Nguyen v. Excel Corp., 197 F.3d 200, 206 (5th Cir. 1999) ("[T]he research undertaken by an attorney to respond to a client's request also falls within the reaches of the privilege.").

[125] Guy v. United Healthcare Corp., 154 F.R.D. 172, 179 (S.D. Ohio 1993); Hewes v. Langston, 853 So.2d 1237, 1247 (Miss. 2003) (finding that the legal research memo falls within the purview of attorney-client privilege).

[126] Chaudhry v. Gallerizzo, 174 F. 3d 394, 402 (4th Cir. 1999); In re Grand Jury Witness, 695 F.2d 359, 362 (9th Cir. 1982) ("[B]ills, ledgers, statements, time records and the like which also reveal the nature of

inclusion of legal research in attorney-client communications has been used as a measure for whether communications are sufficiently law-related to fit within the scope of the privilege.[127] By identifying permissible ways that attorneys might re-use or share their expanded understanding of the law gained from legal research performed on behalf of a particular client, the Restatement implicitly acknowledges that legal research details reflect privileged communications.[128] Some online research tools provide non-legal information, but research using these tools should be well within the scope of the privilege if the information sought is necessary for the rendering of legal advice, and the search terms and documents viewed reflect privileged communications between the attorney and client.[129]

In addition, some state legislatures have expanded the definition of confidentiality to accommodate potential exposure of privileged information to providers of electronic communication services.[130] If this approach is followed, the use of the internet in and of itself will not be a barrier to a finding of confidentiality.

Recognition of these third parties as possible participants in confidential communications, though, is insufficient to protect privilege if these actors fail to preserve confidentiality.[131] Courts have not required the attorney and client to explicitly discuss or

---

the services provided, such as researching particular areas of law, also should fall within the privilege."); Cardenas v. Prudential Ins. Co. of Am., No. Civ. 99-1421, 2003 WL 21302957 (D. Minn. May 16, 2003) (sustaining trial court's finding that billing records revealing the subjects of legal research were protected by attorney-client privilege).

[127] *See, e.g.*, State ex rel. Toledo Blade Co. v. Toledo-Lucas City Port Auth., 905 N.E.2d 1221, 1228 (Oh. 2009) ("[T]he absence of legal research in an attorney's communication is not determinative of privilege, so long as the communication reflects the attorney's professional skills and judgments. Legal advice may be grounded in experience as well as research." (quoting Spectrum Sys. Intern. Corp. v. Chem. Bank, 581 N.E.2d 1055 (N.Y. 1991))).

[128] "During legal research of an issue while representing a client, a lawyer may discover a particularly important precedent or devise a novel legal approach that is useful both in the immediate matter and in other representations. The lawyer and other members of the lawyer's firm may use and disclose that information in other representations, so long as they thereby disclose no confidential client information except as permitted [under other exceptions.]" RESTATEMENT (THIRD) OF LAW GOVERNING LAWYERS § 59(e) (2000). The Restatement identifies no cases on this point but bases the statement on "the principles behind the concept of generally known information, the customary and accepted practices of lawyers, and the public interest in effective professional practice consistent with the general protection of confidential client information*." Id.* at cmt. e.

[129] If the attorney provides services other than legal advice, and those services are not intertwined with legal advice, the privilege is generally not extended in order to avoid abuse of the deviation from a larger commitment to revelation of truth. *See* Sisk & Abbate, *supra* note 116, at 240 (advocating application of the privilege when attorneys provide advice in matters relating to or overlapping with the law).

[130] *See, e.g.*, CAL. EVID. CODE § 917(b) (2010) ("A communication between persons in a relationship listed in subdivision (a) does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication."); N.Y. C.P.L.R. 4548 (MCKINNEY 2010) (same); *See also* Ford Motor Co. v. Hall-Edwards, 997 So. 2d 1148, 1153 (Fla. Dist. Ct. App. 2009) (citing Florida Stat. § 90.502 which explicitly protects as confidential communications shared with third parties in furtherance of the rendering of legal advice and with those third parties necessary to deliver those communications).

[131] *See, e.g.*, Fed. Trade Comm'n v. GlaxoSmithKline, 294 F.3d 141, 147 (D.C. Cir. 2002) (finding privilege was maintained in privileged documents when "each intended recipient was bound by corporate policy or, in the case of the contractors, by a separate understanding, to keep confidential the contents of the documents.").

agree to contractual terms for confidentiality,[132] but similar assumptions are not realistic in the context of internet research given the growth of online tracking and data re-use.

The level of secrecy required for confidentiality varies by jurisdiction and by the circumstances in each case.[133] Most courts look for a "reasonable expectation of confidentiality," which requires both a subjective expectation and implementation of objectively reasonable precautions.[134] Importantly, these standards are generally distinct from the test for Fourth Amendment privacy protections, where the focus is on an individual's privacy; here, the focus is on a relationship.[135]

Reasonable precautions play several pivotal roles in privilege analysis and, of course, in the protection of confidentiality. First, courts may look to precautions as contemporaneous evidence of intent to establish or maintain confidentiality.[136] Second, reasonable precautions are required in many jurisdictions as an objective component in the establishment of a reasonable expectation of confidentiality.[137] Third, reasonable precautions can help protect privilege even when disclosure nonetheless occurs.[138]

---

[132] WIGMORE, *supra* note 105.

[133] United States v. Adlman, 68 F.3d 1495, 1500 n.1 ("Deciding whether the attorney-client privilege exists requires 'common sense . . . in light of reason and experience,' and should be determined 'on a case-by-case basis.'") (quoting *In re* Six Grand Jury Witnesses, 979 F.2d 939, 944 (2d Cir.1992), *cert. denied,* 509 U.S. 905 (1993)).

[134] *See, e.g.*, Gordon v. Boyles, 9 P.3d 1106, 1123 (Colo. 2000) ("[T]he 'privilege applies only to statements made in circumstances giving rise to a reasonable expectation that the statements will be treated as confidential.'") (quoting Lanari v. People, 827 P.2d 495, 499 (Colo.1992)). *See also* Mosteller & Broun, *supra* note 71 at 164–70 (reviewing cases characterizing the nature of confidentiality under privilege law).

[135] Mosteller & Broun, *supra* note 71, at 187–88; The terms "privacy" and "confidentiality" have a multitude of definitions in common parlance and in the law. *See* Daniel J. Solove, *A Taxonomy of Privacy,* 154 U.PA. L. REV. 477 (2006) ("Privacy is a concept in disarray. Nobody can articulate what it means."); Richards & Solove, *supra* note 90 at 125 ("Rather than protecting the information we hide away in secrecy, confidentiality protects the information we share with others based upon our expectations of trust and reliance in relationships.")

[136] *Adlman*, 68 F.3d at 1500 n.1 (looking to contemporaneous documentation for evidence of intention of confidentiality); Suburban Sew 'n Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 260 (D.C. Ill. 1981) ("the relevant consideration is the intent of the defendants to maintain the confidentiality of the documents as manifested in the precautions they took"); In re Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984) ("Taking or failing to take precautions may be considered as bearing on intent to preserve confidentiality." (citing *In Re Horowitz,* 482 F.2d 72, 82 n.10 (2d Cir.), *cert. denied,* 414 U.S. 867 (1973))).

[137] Attorneys and their clients may be no better informed than the average consumer about tracking and precautions to prevent tracking. *Supra* note 3. Yet, unanticipated vulnerability has not been sufficient to protect privilege in a number of cases. *See, e.g.*, Banks v. Mario Industries of Va. 650 S.E.2d 687, 695–96 (2007) (holding deletion of a file created on an employer's computer not sufficient to protect confidentiality of document retrievable by forensic computer expert); *Suburban Sew 'n Sweep, Inc.*, 91 F.R.D. 254 at 260–61 (holding in a "close" case that defendants could have taken "extreme" measures to protect against that unlikely situation in which privileged documents could be found within their garbage dumpster).

[138] *See, e.g.*, Corey v. Norman, Hanson & DeTroy, 742 A.2d 933, 940–42 (Me. 1999) (protecting privilege despite inadvertent disclosure to opposing counsel because the highest protection best serves the goal of encouraging clients to communicate with their attorneys); United States *ex rel.* Mayman v. Martin Marietta Corp., 886 F. Supp. 1243, 1246 (D. Md. 1995) (explaining that privilege was not waived when a document was stolen because reasonable security precautions had been taken).

Fourth, reasonable precautions actually protect confidentiality, and some courts require actual confidentiality to establish and maintain the privilege.[139]

In recent years, reasonable precautions have been a major factor in many courts' consideration of whether inadvertent disclosure of privileged information should constitute waiver of the privilege. Intent is not at issue in cases of inadvertent disclosure, so the question is whether privilege should be maintained even in light of a disclosure to opposing counsel or to some other third party not recognized as a participant in the privileged communication. Courts have developed three general approaches to inadvertent disclosures. Some courts hold privilege is waived if confidentiality is not achieved, despite demonstrated intent and precautions to maintain the confidential nature of the communications.[140] A few courts take the opposite approach and protect privilege even when attorney-client communications are mistakenly revealed, concluding that the privilege is so important that it requires a high level of protection.[141] The most popular approach to inadvertent disclosure is embodied in new Federal Rule of Evidence 502.[142] This rule, enacted in 2008, takes a middle-ground balancing approach to inadvertent disclosure of communications in particular circumstances.[143] Rule 502 protects the privilege from waiver by balancing factors including whether a lawyer takes reasonable

[139] *See, e.g.*, *In re* Sealed Case, 877 F.2d 976 (D.C. Cir. 1989) (finding no need to distinguish between voluntary and inadvertent disclosures because risk fell on the party seeking to enforce the privilege); Commonwealth v. Edwards, 370 S.E. 2d 296, 301 (1988) ("[T]he privilege is an exception to the general duty to disclose, is an obstacle to investigation of the truth, and should be strictly construed."); Int'l Bus. Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 450 (D. Mass 1988) ("[M]istake or inadvertence is, after all, merely a euphemism for negligence, and, certainly . . . one is expected to pay a price for one's negligence." (citing *In re* Financial Management Corp., 77 B.R. 324, 330 (Bankr. D.Mass 1987))). The strict accountability approach was advanced by John Henry Wigmore. "[T]he privilege remains an exception to the general duty to disclose. Its benefits are all indirect and speculative; its obstruction is plain and concrete." WIGMORE, *supra* note 105, at § 2291. "The law . . . leaves to the client and attorney to take measures of caution sufficient to prevent being overheard by third persons." *Id.* at § 2325. Of course, clients too may be extremely concerned about actual confidentiality.

[140] Wigmore discouraged preservation of the privilege in cases of inadvertent waiver. "The investigation of truth and the enforcement of testimonial duty demand the restriction, not the expansion, of these privileges." 8 WIGMORE, *supra* note 104, § 2192. In jurisdictions using this strict accountability approach, an attorney might need to employ sophisticated anonymizing technologies as a screen for internet-based research, although these tools have drawbacks. *See supra* Part II. B. 2. and *infra* Part IV item 5.

[141] *See supra* note 140.

[142] *See, e.g.*, Save Sunset Beach Coal. v. City and Cnty. of Honolulu, 78 P.3d 1, 21–22 (Hawaii 2003) (reviewing the three distinct approaches to inadvertent waiver taken by the states and adopting a reasonableness approach based on consideration of several factors including reasonableness of precautions to prevent disclosure, time taken to remedy the error, and overall fairness); *see also* Paula Schaefer, *The Future of Inadvertent Disclosure: The Lingering Need to Revise Professional Rules*, 69 MD. L. REV. 195, 213–14 (2010). *See* An Act to Amend the Federal Rules of Evidence to Address the Waiver of the Attorney-Client Privilege and the Work Product Doctrine, Pub. L. No. 110-322, § 1(a), 122 Stat. 3537–57 (2008) (codified as FED. R. EVID. 502).

[143] "The rule makes no attempt to alter federal or state law on whether a communication or information is protected under the attorney-client privilege or work-product immunity as an initial matter." FED. R. EVID. 502 advisory committee's note. *See* Elizabeth King, *Waving Goodbye to Waiver? Not So Fast: Inadvertent Disclosure, Waiver of Attorney-Client Privilege, and Federal Rule of Evidence 502,* 32 CAMPBELL L. REV. 467 (2010) (evaluating courts' application of Rule 502 and arguing against interpretations that avoid a true middle-ground approach and instead apply the functional equivalent of a strict waiver approach).

precautions against inadvertent disclosure and whether overall fairness would be better served by waiver or maintenance of the privilege.[144] One of the purposes of the rule was to address the potentially prohibitive costs of preventing waiver during the technologically complex process of electronic discovery.[145]

By analogy, an attorney might be protected against a finding of waiver if she took reasonable precautions to avoid online research tracking, such as adjusting the settings on her internet browser software to prevent third-party cookies, using encryption to avoid deep packet inspection where possible, and adding software to the browser to prevent tracking by web bugs.[146] Similarly, if the attorney could show she kept records of contract terms and privacy policies of research websites in which confidentiality is promised, she might be able to meet Rule 502-style standards.[147]

Even if Federal Rule 502 were applied by analogy to determine whether a reasonable expectation of confidentiality was established for internet-based research, attorneys might be held to high standards for reasonable precautions. One court has interpreted the rule to require "all reasonable means."[148] Most courts, though, have merely required "reasonable precautions." Whatever the standard, if the exposure of otherwise privileged internet-based research is widespread, Rule 502's fairness factor, and even a common-sense assessment of the situation, would argue against preservation of the privilege. For example, if research data is tracked, sold, merged with identifying profile information, and made available for sale,[149] opposing parties would have a strong argument that the claim of confidentiality simply cannot fit reality.[150]

Waiver due to inadvertent disclosure is a danger with serious consequences for the disclosing party because courts generally hold that all records and communications of

---

[144] The rule's Advisory Notes explain that "the rule is really a set of non-determinative guidelines that vary from case to case." FED. R. EVID. 502 advisory committee's note. *See also* King, *supra* note 145 (reviewing the trend towards a balancing of factors to determine whether privilege is waived due to inadvertent waiver, especially after enactment of Federal Rule of Evidence 502 in 2008).

[145] FED. R. EVID. 502 advisory committee's note. The impact of new technologies, an increasing need for consultants as part of the complex development of legal advice, and the growth of regulatory pressures that impinge upon the privilege continue to be debated even after the corrective provisions of Federal Rule of Evidence 502. *Id. See* Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence 502*, 58 S.C. L. REV. 211, 219–24 (2006) (demonstrating the need for predictable uniformity for recurring problems with inadvertent waiver prior to the enactment of Rule 502); Schaefer, *supra* note 144, at 195 (describing the continuing challenge of preventing inadvertent disclosure because of modern technologies and the limits of FED. R. EVID. 502).

[146] *See supra* Part II. B. 4–5.

[147] *See supra* Part II. B. 1–3.

[148] Relion, Inc. v. Hydra Fuel Cell Corp., 2008 WL 5122828 (D. Or. 2008) (finding company did not pursue all reasonable means of preserving the confidentiality of documents delivered during discovery and so failed to disprove waiver). *See* King, *supra* note 145, at 476 (arguing that this standard is impossible to meet and inconsistent with the purpose of the new rule).

[149] *See supra* Parts II. B. 4–5.

[150] Courts resort to metaphors to express the inability of the law to fully rectify the harm from such disclosures. *See, e.g.*, Victor Stanley, Inc. v. Creative Pipe, Inc. 250 F.R.D. 251, 263 (2008) ("[A]ny order issued now by the court to attempt to redress these disclosures [of documents mistakenly delivered to opposing counsel during electronic discovery] would be the equivalent of closing the barn door after the animals have already run away."); F.D.I.C. v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992) (noting the general problem with inadvertent disclosures) ("Once persons not within the ambit of the confidential relationship have knowledge of the communication, that knowledge cannot be undone. One cannot 'unring' a bell.").

the same subject matter are also waived.[151] Legal research that reveals communication between attorney and client can have far-reaching applications because many aspects of representation may be reflected in the search terms and strategies.

Tracking of internet-based research could require courts to develop more nuanced descriptions or definitions of confidentiality. For example, since trackers collect and re-use research details but link them only to IP addresses and unique browser cookies, courts would have to assess whether this sort of anonymity were sufficient for a finding of confidentiality.[152] Traditionally, anonymity was not recognized as protection, and exposure of communications to strangers prevented application of the privilege.[153] Courts may also be confronted with the question of insecure anonymity, since some actors in the online industry are merging anonymous records of online behavior with demographic data that could link offline identity with the details of the legal research. Courts might consider this risk in their analysis of whether attorneys took sufficient precautions for the purpose of establishing a reasonable expectation of confidentiality in their online research. In addition, if this sophisticated tracking and merging of data resulted in commercially-available profiles, the destruction of anonymity could be considered inadvertent disclosure that constitutes subject matter waiver.

The goals of attorney-client privilege are all served by attention to precautions to protect confidentiality in internet-based research. If privilege law were to accommodate tracking that produced commercially-available profiles or records revealing legal research relating to representation, clients might indeed have reason to withhold information from their attorneys. Similarly, acceptance of the intrusions of advertisers and diversifying internet service providers would fail to respect the integrity of the decision-making autonomy of the client and the importance of the fiduciary relationship of the attorney. In light of these goals, courts should encourage precautions that secure a balance between effectiveness and manageability, and attorneys should take care to identify and implement reasonable precautions for online research.

C. Work-Product Protection

Work-product protection allows the attorney to "assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal theories and plan his strategy without undue and needless interference."[154] Work-product protection can be invoked by the client, but may in some cases also be claimed by the attorney independently of the client.[155] At the federal level, work product protection draws heavily on the common law recognized in the case of Hickman v. Taylor, 329 U.S. 495 (1947), now largely codified in rules of procedure.[156] Federal Rule of Civil Procedure 26(b)(3) provides some immunity from discovery for materials "prepared in anticipation

[151] FED. R. EVID. 502 advisory committee's note.

[152] *See supra* Parts II. B. 1–3.

[153] United States v. Kelly, 569 F.2d 928, 938 (5th Cir. 1978), *cert. denied*, 439 U.S. 829 (1978).

[154] Hickman v. Taylor, 329 U.S. 495, 511 (1947).

[155] 2 EDNA SELAN EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 805 (5th ed. 2007).

[156] *See generally Hickman*, 329 U.S. 495 **(**holding that while attorney-client privilege did not protect opposing counsel's files and mental impressions, long-standing policy protected the privacy of an attorney's work-product against discovery).

of litigation or for trial."[157] Federal Rule of Criminal Procedure 16(b)(2) provides that "reports, memoranda, or other documents made by the defendant, or the defendant's attorney or agent, during the case's investigation or defense" are not subject to disclosure.[158] Similar protections are provided in the states through statutes or court rules reflecting pre- or post-*Hickman* doctrine as well as some common law approaches.[159] Work product can be either materials that reveal an attorney's opinion about the client's legal situation or simply materials representing factual information. Opinion work product is highly protected,[160] while other work product materials may be discoverable if an opposing party can show "substantial need" and cannot obtain substantially similar information through alternative means "without undue hardship."[161]

The justifications for work-product protection overlap with those for attorney-client privilege insofar as both ultimately are intended to support competent guidance on compliance with the law and the administration of justice.[162] Without work product protection, attorneys might avoid recording their thoughts, leading to "[i]nefficiency, unfairness and sharp practices" in the practice of law and "demoralizing" lawyers.[163] The result could be harm to the justice system and to the interests of clients.[164] Work product also serves to protect fairness in the adversarial practice of law. "Discovery was hardly intended to enable a learned profession to perform its functions either without wits or on wits borrowed from the adversary."[165] The *Hickman* Court stated, "it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel."[166] The Court explained that without this protection "[a]n attorney's thoughts, heretofore inviolate, would not be his own."[167]

Electronic legal research is likely to be considered attorney work-product, even opinion work-product.[168] As one court held, "[t]he search terms used to gather these cases [from Lexis-Nexis] does [sic] provide a window into the attorney's thinking."[169]

---

[157] FED. R. CIV. P. 26(b)(3) codifies protections recognized in *Hickman*, 329 U.S. 495.

[158] FED. R. CRIM. P. 16(b)(2).

[159] 2 EPSTEIN, *supra* note 157, at 800; Susan R. Martyn, *Selected Sections of the Restatement of the Law 3rd—The Law Governing Lawyers*, SR057 ALI-ABA 41 § 87 (2010) (noting that state courts often look to federal decisions when applying work product protection).

[160] Burroughs Wellcome Co. v. Barr Labs. Inc., 143 F.R.D. 611 (E.D.N.C. 1992); United States v. Segal, No. 02-CR-112, 2004 WL 830428 (N.D. Ill. Mar. 31, 2004).

[161] FED. R. CIV. P. 26(b)(3)(A)(ii); FED. R. CRIM. P. 16(b)(2); *In re* Grand Jury Subpoenas Dated June 5, 2008, 329 Fed. App'x 302, 2009 WL 1269487 (2d Cir.2009) (making distinctions between opinion and fact work product and finding that fact work product was discoverable due to substantial need and the absence of alternative means of access to information).

[162] Hickman v. Taylor, 329 U.S. 495, 511 (1947).

[163] *Id.*

[164] *Id.*; *Id.* at 516 (Jackson, J., concurring) ("Law-abiding people can go nowhere else to learn the ever changing and constantly multiplying rule by which they must behave and to obtain redress for their wrongs.").

[165] *Id.* at 516.

[166] *Id.* at 510 (majority opinion).

[167] *Id.* at 511.

[168] Soc'y of Prof'l Eng'g Emps. in Aerospace, IFPTE Local 2001, AFL-CIO v. Boeing Co., 2009 WL 3711599, at *4 (D. Kan. 2009) ("Counsels' drafts and legal research" held "protected by the attorney work product doctrine.").

[169] United States v. Segal, No. 02-CR-112, 2004 WL 830428, at *8 (N.D. Ill. Mar. 31, 2004) (holding cases retrieved from LexisNexis to be protected as opinion work-product).

Courts have protected billing records when those records itemize "motive of the client in seeking representation, litigation strategy, or the specific nature of the service provided, such as researching particular areas of law."[170] Some states' rules of procedure specifically identify legal research as an example of opinion work product that is protected from discovery in criminal and civil cases.[171] One court stated, "It is hard to imagine a document that memorializes legal research done by a lawyer or law clerk that is not work product."[172]

But an opposing party could argue that the work product protection was waived because the attorney's legal research was conducted through the intermediary legal research system if the system lacked confidentiality features. Although waiver can be found simply through voluntary disclosure "to a person other than the client who has no interest in maintaining the confidentiality" of the legal research,[173] the main concern with work-product disclosure is access by an opposing party in litigation. The Restatement of the Law Governing Lawyers describes the potential for waiver of work-product immunity when "the client, the client's lawyer, or another authorized agent of the client . . . (4) discloses the material to third persons in circumstances in which there is a significant likelihood that an adversary or potential adversary in anticipated litigation will obtain it."[174] The Restatement approach is consistent with one of the purposes of the work-product rule, which is to prevent use of the attorney's work by opposing counsel.[175]

So, even if the attorney has reason to believe that the online legal research service shares the content of the research, work-product may yet be protected.[176] If the

[170] Chaudhry v. Gallerizzo, 174 F.3d. 394, 402 (4th Cir. 1999) (quoting Clarke v. Am. Commerce Nat'l Bank, 974 F.2d 127, 129 (9th Cir. 1992). *But see* United States *ex rel.* Wiser v. Geriatric Psychological Servs., No. CIV. Y-96-22-2219, 2001 WL 286838 (D. Md. Mar. 22, 2001) (finding attorney bills to be unprotected at later stages of litigation when attorney's legal strategies and opinions were already made public).

[171] *See, e.g.*, ARIZ. R. CRIM. P. 15.4(b)(1) ("*Work Product*. Disclosure shall not be required of legal research or of records, correspondence, reports or memoranda to the extent that they contain the opinions, theories or conclusions of the prosecutor, members of the prosecutor's legal or investigative staff or law enforcement officers, or of defense counsel or defense counsel's legal or investigative staff."); CAL. CIV. PROC. CODE § 2018.030 (West 2010) (dividing attorney work product into opinion and non-opinion categories, explicitly providing higher protection of opinion work product to legal research: "(a) A writing that reflects an attorney's impressions, conclusions, opinions, or legal research or theories is not discoverable under any circumstances.").

[172] N.L.R.B. v. Jackson Hosp. Corp., 257 F.R.D. 302, 310 (2009).

[173] McKesson HBOC, Inc. v. Superior Court, 115 Cal. App. 4th 1229, 1239 (2004) (citing BP Alaska Exploration, Inc. v. Superior Court, 199 Cal. App. 3d 1240, 1261 (1988)).

[174] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 91; Schanfield v. Sojitz Corp. of Am., 258 F.R.D. 211, 214 (S.D. N.Y. 2009) (finding waiver occurs when third-party disclosure party "substantially increases the opportunity for potential adversaries to obtain the information." (quoting Merrill Lynch & Co. v. Allegheny Energy, Inc., 229 F.R.D. 441, 445–46 (S.D.N.Y. 2004)).

[175] Hickman v. Taylor, 329 U.S. 495, 510–11 (1947).

[176] Unlike the attorney-client privilege, the attorney work-product doctrine "is not automatically waived by disclosure to a third party." Cellco P'ship v. Nextel Comm., Inc., Civ. A 03-725-KAJ, 2004 WL 1542259, at *1 (S.D.N.Y. July 9, 2004). "[D]isclosure simply to another person who has an interest in the information but who is not reasonably viewed as a conduit to a potential adversary will not be deemed a waiver of the protection of the rule." Bowne of N.Y. City, Inc. v. AmBase Corp., 150 F.R.D. 465, 479 (S.D.N.Y. 1993). Most courts will find waiver if the disclosure "substantially increases the opportunity for potential adversaries to obtain the information." Lawrence E. Jaffe Pension Plan v. Household Int'l, Inc. (Jaffe I), 237 F.R.D. 176, 183 (N.D. Ill. 2006) (citations omitted). "The work product privilege should not

disclosure is to affiliate advertising companies or for marketing by sibling companies, and if the details of the research or the offline identity of the research are redacted or anonymized sufficiently, work-product may survive even a somewhat porous system for confidentiality. Furthermore, Federal Rule of Evidence 502 applies to work-product protection as well as to attorney-client privilege to prevent waiver based on a balancing of factors including whether an attorney has taken reasonable precautions to protect confidentiality.[177]

D. Ethical Requirements of Confidentiality and Competency

As licensed members of bar associations, lawyers must conform to an ethical requirement to maintain confidentiality of information relating to the representation of a client. The American Bar Association Model Rules of Professional Conduct, upon which nearly all state rules are based,[178] contains Rule 1.6, which prohibits disclosure of information relating to the representation of a client without the client's consent.[179] Comment 16 provides that "[a] lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Comment 17 advises an attorney to "take reasonable precautions to prevent the information from coming into the hands of unintended recipients" when transmitting communications.[180]

This ethical obligation requires confidentiality both within and outside of the context of litigation. Because Rule 1.6 covers transactional as well as litigation practice, precautions against disclosure to "unintended recipients" must describe a broader category of persons than just opposing parties. In transactional work, the client may have no opposing parties, and yet the ethical rule still requires confidentiality.

The purpose of the attorney's ethical obligation to confidentiality, as outlined in comments to Model Rule 1.6, is to cultivate "the trust that is the hallmark of the client-lawyer relationship."[181] The rule is said to serve the purpose of encouraging clients to seek the assistance of attorneys, to provide full details of their situations so that attorneys can assist them in the determination of their rights under and full compliance with complex law.[182] This ethical rule can be seen to advance the profession of the lawyer, serve in the administration of justice and compliance with the law, and honor the integrity of the lawyer-client relationship.

---

be deemed waived unless disclosure is inconsistent with maintaining secrecy from possible adversaries." Stix Prods. Inc. v. United Merchs. & Mfrs., 47 F.R.D. 334, 338 (S.D.N.Y. 1969).

[177] FED. R EVID. 502.

[178] Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 15 n.97 (2010) (noting that "California remains the only state whose legal ethics rules do not comport with the ABA Model Rule format.").

[179] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2004); *see also* Jason Popp, *The Cost of Attorney-Client Confidentiality in Post 9/11 America*, 20 GEO. J. LEGAL ETHICS 875, 878–80 (2007) (describing uniformity among the ABA and state bar associations on the general purpose of rule 1.6).

[180] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2004).

[181] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 2 (2004).

[182] *Id.*

Violation of the ethical requirement of confidentiality has several potential consequences. The attorney may be disciplined through the state's disciplinary process. In addition, violation of the duty of confidentiality could form a basis of a claim of malpractice by the client against the attorney, particularly if disclosure harmed the client's interests.[183] More rarely, courts may consider violation of rules as evidence of waiver of attorney-client privilege or work-product protection.[184]

Not surprisingly, since ethics rules apply to all information relating to representation, state bar associations have treated legal research as protected information relating to the representation of a client.[185]

Third party services and reliance on new technologies have generally been approved by bar associations, but attorneys are advised to take "reasonable precautions,"[186] "reasonable care,"[187] or "reasonable steps"[188] to protect confidentiality. New Jersey has articulated a two-part test for reliance on third-party services that expose confidential client information. Attorneys must secure "an enforceable obligation to preserve confidentiality and security" and must make use of "available technology to guard against reasonably foreseeable attempts to infiltrate the data."[189] Most jurisdictions have identified an attorney's obligation to employ varying levels of protection, depending on the sensitivity of the confidential information.[190]

Applying these tests of reasonableness, opinions have provided cautious acceptance of new technologies and tools such as Software as a Service,[191] online files

---

[183] Fred. C. Zacharias, *Are Evidence-Related Ethics Provisions "Law"?*, 76 FORDHAM L. REV. 1315 (2007).

[184] "Although the bar construes confidentiality broadly and exceptions narrowly, courts construe privilege in the opposite way because of its potential negative impact on truth seeking." *Id.* at 1320.

[185] *See, e.g.*, State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 1992-127 (citing cases construing the work product immunity as authority for client's entitlement to the "attorney's impressions, conclusions, opinions, legal research, and legal theories prepared in the client's underlying case").

[186] N.C. State Bar, 2005 N.C. Formal Ethics Op. 10 (2006) ("[C]yberlawyers must take reasonable precautions to protect confidential information transmitted to and from the client.").

[187] *See, e.g.*, Colo. Bar Ass'n Ethics Comm., Formal Op. 90 (1992) (requiring that attorneys exercise "reasonable care" in the use of mobile phones, cellular phones, facsimile machines, and other "modern communications technology").

[188] State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2007-174 (requiring reasonable steps to remove metadata); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995) (requiring reasonable steps to ensure persons working with client information protect confidentiality).

[189] N.J. Sup. Ct. Adv. Comm.on Prof. Ethics, Op. 701 (2006). *See also* Me. Bd. of Overseers of the Bar, Op. 194 (2007) (requiring attorneys who store client files electronically to "take steps to ensure that the company providing . . . confidential data storage has a legally enforceable obligation to maintain the confidentiality"); The North Carolina State Bar has approved the use of a recycling company if the attorney ascertains that the company uses procedures "which effectively minimize the risk that confidential information might be disclosed." N.C. State Bar, RPC Op. 133 (1992) (requiring the attorney to "take particular care to ensure that custodial personnel under his or her supervision are conscious of the fact that confidential information may be present . . . and [of] the attorney's professional obligations").

[190] *See, e.g.*, N.C. Op. 133, *supra* note 191 (requiring attorneys to shred waste paper containing highly sensitive confidential information).

[191] N.C. State Bar Council, Proposed 2010 Formal Ethics Opinion 7, Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property (April 15, 2010), *available at* http://law.gsu.edu/ccunningham/FLP/CloudComputing-CarolinaEthicsOpinion.pdf, last visited March 3, 2011. The North Carolina Bar Ethics Committee voted to withdraw this proposed opinion for

accessible to clients,[192] email,[193] cell phones, and fax machines.[194] The steps required to meet standards for reasonable precautions vary, so attorneys must conform to applicable rules.[195]

The special challenge of email which mines message content for targeted advertising was addressed by the New York Bar Association Committee on Professional Ethics in 2008.[196] This opinion provides insight into the limits of ethical accommodation for tracking for the purpose of delivering advertisements. While the opinion did not mention a particular provider, Google's Gmail was and is a prominent example of this type of service.[197] The Bar concluded that the computer-generated contextual advertisements based solely on Gmail message content did not violate confidentiality.[198] However, the opinion did state that a violation would occur "if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order)."[199] Subsequently, Google mined Gmail content to automatically display on the public web the names of those with whom Gmail users exchanged the most messages when it introduced a new social networking service called Buzz.[200] Google responded to complaints by changing the system, but lawsuits were filed based on federal privacy statutes and other claims.[201]

---

further study on January 20, 2011. *Proposed Actions*, N.C. STATE BAR, http://www.ncbar.gov/ethics/propeth.asp (last visited Mar. 5, 2011).

[192] Ariz. Ethics Op. 09-04, Dec. 2009 (approving online file system with multi-level security including Secure Socket Layer encryption for remote access by clients and their attorneys).

[193] State bar opinions have generally concluded that the use of unencrypted email is not in and of itself a failure to protect confidential content. Some states require "due care." *See, e.g.*, Mass. Bar Ass'n Ethics Opinion 00-01 (2000). Other jurisdictions require evaluations of specific situations when using email to communicate confidential client information. D.C. Bar Ass'n, Transmission of Confidential Information by Electronic Mail, Op. No. 281 (1998). *But see* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (advising that threats to confidentiality of internet-based activity have grown since these email opinions; that attorneys' obligations to employ stronger protections have increased; and that, while unencrypted email retains reasonable confidentiality, highly sensitive information might require a higher level of protection).

[194] *See* Hill, *supra* note 180, at 17–21 (reviewing bar association opinions on confidentiality obligations regarding the use of email and cell phones).

[195] *See* Elizabeth W. King, 113 PENN. ST. L. REV. 801, 817–18 (2009) (comparing different state bar association guidelines for reasonable precautions relating to metadata).

[196] N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 820 (2008), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=13652&TEMPLATE=/CM/ContentDisplay.cfm ("A lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, where the e-mails are not reviewed by or provided to other individuals.").

[197] Commentators referred to the opinion in terms of Gmail. Kevin Raudebaugh, *Trusting the Machines: New York State Bar Ethics Opinion Allows Attorneys To Use Gmail,* 6 WASH. J. L. TECH. & ARTS 83, 86 (2010) (providing details about Google's forbearance from using Gmail content to the full extent of its patent description which includes the ability to create logs of user profiles and comparing Gmail scanning of content to virus and spam scanning activities).

[198] N.Y. State Bar Ass'n, *supra* note 198.

[199] *Id.*

[200] Miguel Helft, *Anger Leads to Apology from Google About Buzz,* N.Y. TIMES, Feb. 15, 2010, at B3 (describing the controversial introduction of the Google Buzz service).

[201] Rick Carroll, *Aspen Law Firm, Two Attorneys Take On Google,* ASPEN TIMES, Jun. 1, 2010, *available at* http://www.aspentimes.com/article/20100601/NEWS/100539969/1077&ParentProfile=1058

Current cross-site tracking of internet research by network advertisers might fail New York's test of exposure of confidential information to humans, so attorneys would need to take reasonable precautions to block this type of third-party tracking. The Gmail example also highlights an attorney's obligation to update confidentiality-protecting approaches as technologies change.[202]

The escape valve for ethical confidentiality protection is informed client consent.[203] To the extent that the attorney can competently inform a client of the risks to confidentiality from online research, consent would seem to secure compliance for confidentiality.

In sum, ethical standards, though variable in application by jurisdiction, cover all online research related to representation of the client and tend to require reasonable precautions for confidentiality reflecting the level of sensitivity of the information. While an attorney should avoid disclosure not only to opposing parties but to all persons unnecessary to the rendering of legal advice, accommodations for new technologies and outsourcing indicate a standard that might excuse some tracking of online research if the practice conforms to this limitation. As a final protective measure, the attorney might seek client consent.

E. Synthesis of Criteria for Confidentiality

Synthesis of the applicability and requirements of attorney-client privilege, work-product protection, and ethical rules for confidentiality requires collapse of jurisdictional variations and differences in the purposes and applications of these confidentiality interests.[204] But attorneys have to make decisions based on some type of synthesis in order to develop approaches that will address all three. Reasonableness may be a useful, if optimistically simplistic, characterization of the collective attorney and client requirements for confidentiality protection. While not all jurisdictions have followed the balancing approach to inadvertent disclosure of privilege or work-product, a majority has adopted this test, and the momentum is with this approach. As long as reasonable precautions are taken to avoid disclosure to third-parties unnecessary to the provision of legal advice, attorney-client privilege is likely to be protected from waiver. Work-product standards may be the lowest of the three, perhaps requiring only that precautions are taken to prevent opposing parties' access in the context of litigation. Ethical rules

---

(reporting several lawsuits filed against Google for introduction of the Buzz service which exposed information about use of the Gmail service).

[202] *See, e.g.*, Ariz. Ethics Op. 09-04 (2009) ("As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."). The expanded use of scanned Gmail content serves as a good example of how new features of a website service can impose new burdens on attorneys to opt-out of the feature or withdraw from the service.

[203] The ABA has concluded that outsourcing of legal work requires informed consent from the client. Am. Bar Ass'n Standing Comm. on Ethics and Prof'l Responsibility in Formal Opinion 08-451 (2008) (finding no implied authorization to outsource legal work). *See also* Kathryn A Thompson, *Do Tell: Client Consent is a Safe Step When Lawyers Outsource Work on Cases,* 96 A.B.A. J. 26 (June 2010) (reviewing ABA and state bar association approaches to confidentiality and client consent relating to outsourcing of legal work).

[204] *See* Fred C. Zacharias, *Harmonizing Privilege and Confidentiality,* 41 S. TEX. L. REV. 69 (1999) (exploring the practical issues that different secrecy rules create).

require confidentiality of all online research related to representation, but even targeted marketing may be acceptable as long as human beings do not gain access to confidential information. Informed client consent for online research can secure compliance with ethical rules.

Taking the three interests as a whole, an attorney is required to take reasonable precautions to prevent tracking that exposes any online research to a party not necessary to the provision of legal advice. Although some jurisdictions may have higher standards, and some relaxation of this standard may apply to work-product or ethical requirements, this approach should suffice for an examination of online legal research systems' risks to confidentiality for attorneys and clients.

IV. REASONABLE PRECAUTIONS

As the Section on tracking showed, a number of precautions can significantly reduce tracking of online activity to create and preserve confidentiality. The outline of steps that follows, however, demonstrates that securing confidentiality online is not easy. To maintain confidentiality of online legal research, one must take a broader approach to limiting online tracking than simply checking for privacy protections from individual legal research services or websites.[205]

1. *Contract terms with subscription services*

Attorneys should make sure their contracts with fee-based legal research services include specific assurances for confidentiality. First, the services should provide support for encrypted access. Second, terms should promise nondisclosure of search data to third parties and promise notice to the subscriber if legal process served by government entities allows. At the very least, the terms should assure effective redaction of the information to provide anonymity of the search topics. Third, sharing with affiliate companies should not include affiliates that are unrelated to legal research or could represent a prohibited disclosure to a party unnecessary for the rendering of legal advice. Fourth, attorneys should seek provisions for limited data retention or prompt anonymization of retained data.

2. *Privacy policy terms of "free" services*

Attorneys should seek the same terms as with subscription services. In addition, if the website allows site users to opt-in or opt-out of confidentiality protections, attorneys should take advantage of those options. Attorneys should update this process on a regular basis, perhaps twice a year or more often to monitor changes in the policy.

[205] Not only do some tracking devices collect information about use of more than one web resource, but lawyers are also likely to implement a variety of approaches to research on behalf of a client. *See* Joe Custer, *The Universe of Thinkable Thoughts Versus the Facts of Empirical Research*, 102 LAW LIBR. J. 251 (2010) (reporting survey of Douglas County, Kansas attorneys in which almost all respondents used more than one source for legal research and approximately eighty-three percent searched at least one source online); Heidi W. Heller, *The Twenty-First Century Law Library: A Law Firm Librarian's Thoughts*, 101 LAW LIBR. J. 517 (2009) (observing that attorneys in practice use a wide range of legal research tools both online and in print)*; see also* 5 AM. BAR ASS'N, 2010 LEGAL TECHNOLOGY SURVEY REPORT: ONLINE RESEARCH 21, 43 (2010) (reporting that the most common free website use for legal research is Google and reporting that over sixty-two percent of attorneys regularly used free online resources and nearly fifty-nine percent regularly used fee-based online legal research services).

Those with bar association access to a legal research service should work through the bar association, which should seek protections for bar members.

3. *Internet service providers contracts and policies*

Contracts for both home and work providers should be reviewed. If possible, attorneys or firms could negotiate for confidentiality protections similar to those for website providers.

4. *Practices to prevent tracking not controllable through contracts or privacy policies*

Attorneys should adjust browser software settings for privacy to prevent third party cookies and to delete browsing histories. They should also limit data collection by third parties through Flash cookies by adjusting Flash Player settings. Whenever possible, encryption should be used to secure confidentiality against deep packet inspection by internet service providers. In addition, attorneys should avoid linking to outside websites from query results produced by unencrypted websites. Attorneys should also consider opting out of advertiser tracking and website analytics services such as Google Analytics when those options are available.

5. *Extreme measures*

Attorneys could also consult technology experts on the utility of software to anonymize use of the internet, such as Tor or TrackmeNot for highly sensitive client research.

V. THE NEED FOR EXPERTS

The cost of protecting confidentiality online is high, especially for individual attorneys. Just like the cost of protecting confidential information from disclosure during electronic discovery, the steps required to protect online activity from compromising tracking are cumbersome and require constant updating to address new technology. Two researchers estimated that if consumers read and compared website privacy policies, the national opportunity cost in 2008 would have been on the order of $781 billion.[206] Attorneys must read and interact with website polices in addition to taking a number of other steps to preserve confidentiality in internet research. Solo practitioners and small firm lawyers in particular need help to competently address confidentiality requirements in the online environment, because these lawyers are less likely to have the support of in-house technology experts.

A number of existing resources could devote energy and expertise to producing ongoing guidance for lawyers on confidentiality practices of legal research intermediaries, and could also help negotiate or advocate for better protections through market influence or changes in the law of tracking.

[206] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2008-2009). Studies show that researchers do not in fact read and compare privacy policies. *See* Haynes, s*upra* note 13, at 588 (citing several studies that show internet users do not read website privacy policies).

The Sedona Conference nonprofit has produced reports on electronic discovery and confidentiality and related topics and so might also examine practical and law-based solutions to the problem of tracking of online legal research.[207] The American Bar Association has established a Commission on Ethics 20/20 to "perform a thorough review of the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments" and to make policy recommendations over the next couple of years.[208] This group could consider the ethical implications of online tracking of legal research and make recommendations about how rules can address this challenge. State bar associations and any other bar associations with consortium subscriptions to legal research systems should negotiate for terms for confidentiality including encryption support.

Other groups might provide more ongoing practical guidance on how to protect the confidentiality of online legal research through technology and research habits and might in the process influence the practices of websites and internet service providers. The American Bar Association Legal Technology Resource Center already provides some guidance on the use of technology, including comparison charts on technology products and a chart on metadata ethics opinions.[209] Some organizations have expertise in assessing and responding to confidentiality risks online, including library associations and privacy advocacy organizations.[210] These organizations are likely to produce assessments and guidelines that would be useful to lawyers attempting to take reasonable precautions for online research confidentiality. A collaborative effort among some or all of these groups could produce a confidentiality seal system or regularly updated chart

---

[207] The Sedona Conference is a nonprofit research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. THE SEDONA CONFERENCE, http://www.thesedonaconference.org/ (last visited Sep. 5, 2010) (linking to a number of reports relating to best practices on topics such as The Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas: A Project of The Sedona Conference® Working Group on Electronic Document Retention & Production (WG1) April 2008).

[208] *Agenda*, THE ABA COMMISSION ON ETHICS 20/20, http://www.abanet.org/ethics2020/agenda.pdf (last visited Sep. 5, 2010).

[209] *Resources—Legal Technology Resource Center*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources.html. (last visited Feb. 18, 2011).

[210] *See, e.g.*, Trina J. Magi, *A Content Analysis of Library Vendor Privacy Policies: DO They Meet Our Standards?*, 71 COLL. & RES. LIBR. 254 (2010) (reviewing several standards for reader or researcher privacy including library organization standards, testing online research systems' promises for compliance, and reporting aggregate statistics). The American Library Association ("ALA") Office of Intellectual Freedom has a "Campaign for Reader Privacy" and pursues a number of initiatives to support librarian conformity to the ALA ethical commitment to confidentiality of library use. OFFICE OF INTELLECTUAL FREEDOM, AM. LIBR. ASS'N, http://www.ala.org/Template.cfm?Section=oif (last visited Sep. 5, 2010). Similarly, the American Association of Law Libraries ("AALL") has issued policy statements and published ethical principles to protect confidentiality. AALL members include librarians who work directly with lawyers and so would be good partners in maintaining best practices for online legal research confidentiality. A number of privacy advocacy organizations assess and report on matters relating to confidentiality of online legal research including The Center for Democracy & Technology, http://www.cdt.org/; The Electronic Frontier Foundation, http://www.eff.org/; Electronic Privacy Information Center ("EPIC"), http://epic.org/; and The Future of Privacy Forum, http://www.futureofprivacy.org/.

that could specifically address attorneys' needs for confidentiality online.[211] Even if these seals did not appear on research websites, a regularly updated chart categorizing online research systems by their level of support for confidentiality could be published on the ABA Legal Technology Resource Center website and linked from other sites. This type of evaluation system could also induce websites and internet service providers to offer options for higher protection of confidentiality.

VI. STRENGTHENING THE LAW OF ONLINE TRACKING

If the collaborative guidance and market influence of experts fails to deliver reasonable and effective precautions in light of evolving online tracking, confidential online legal research will have to be secured through legislation or regulation. Groups representing consumer interests, including the Federal Trade Commission, have made calls for greater transparency and control over online data collection and re-use so that consumers can make meaningful choices about the exchange of their search data for services.[212] However, proposals for new legislation or regulation have met with resistance from the commercial sector because new forms of advertising are argued to be the best way to fund innovation and deliver services,[213] or because of fears that regulation will unfairly apply to only part of the industry.[214] The debate about online tracking is

[211] Privacy seals are already offered through such entities as TRUSTe which provides consumer privacy assurance. *See, e.g.*, TRUSTE, http://www.truste.com/about_TRUSTe/ (last visited Sep. 5, 2010). These broader systems are not geared towards the standards necessary to protect confidentiality of online legal research for legal representation and have suffered some criticisms for their business models which are based on fees paid by sites that TRUSTe evaluates. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?* 52 STAN. L. REV. 1461, 1526–27 (2000) ("If TRUSTe were to start suspending trustmarks, it would lose revenue; if it were to get a reputation for being too aggressive toward clients, they might decide they are better off without a trustmark and the attendant hassle."); Xiaourui Hu, et al, *The Effects of Web Assurance Seals on Consumers' Initial Trust in an Online Vendor: A Functional Perspective,* 48 DECISION SUPPORT SYSTEMS 407, 409 (2010) (providing a chart comparing empirical studies on specific web assurance seals for privacy, security, and transaction-integrity).

[212] FTC STAFF REPORT ON BEHAVIORAL ADVERTISING, *supra* note 37, at 2; Letter from American Civil Liberties Union to U.S. Senator Patrick Leahy and U.S. Senator Jeff Sessions (Nov. 2, 2009), *available at* http://www.aclu.org/technology-and-liberty/letter-support-s-1490-personal-data-privacy-and-security-act (supporting legislation that would, among other things, require consumers' access to their own profiles and sources of information held in profiles maintained by data aggregators); *see also* FED. TRADE COMM'N, PRELIMINARY FTC STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010) (identifying business practices that could improve consumer privacy and raising the question of whether the agency should propose legislation if industry fails to improve consumer protections), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; DEPT. OF COMMERCE INTERNET POL. TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, (2010) (recommending baseline protections for online consumer privacy that go beyond industry self-regulation), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[213] *[Prepared] Testimony of Michael Zaneis before the Subcommittee on Commerce, Trade, & Consumer Protection*, H. COMM. ON ENERGY & COMMERCE 3–4 (July 22, 2010) http://republicans.energycommerce.house.gov/Media/file/Hearings/CTCP/072210_CTCP_Best_Practices/Zaneis.Testimony.pdf (arguing that industry-self regulation allows the evolving online industry to be nimble in response to consumer concerns and arguing against legislation that would regulate online advertising).

[214] *Legislative Hearing on Communications Networks and Consumer Privacy Before the H. Comm. On Energy & Commerce, Subcomm. On Commc'ns, Tech. & the Internet,* 111th Cong. 5 (April 23, 2009) (statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T, Inc.)

broader in scope than the question of how to protect the attorneys' and clients' interests in confidentiality of online legal research. But if non-legal approaches fail to protect these long-standing confidentiality interests, this harm surely adds weight to arguments that online privacy merits increased protection.

VII. CONCLUSION

The commercial tracking of online legal research is a growing threat to the three confidentiality interests relating to legal representation. Attorney-client privilege, attorney work-product protection, and an attorney's ethical rule of confidentiality are bedrock principles for the United States justice system and for the practice of law. The rapid expansion in data tracking technologies, decreasing cost of data storage, and advancements in data merging techniques and practices have transformed the internet into a dangerous place at the same time that legal research is shifting to website-based systems. Attorneys must take reasonable precautions to prevent exposure of confidential information to third parties not necessary for the rendering of legal advice. Currently, an array of precautions must be implemented to protect these three confidentiality interests. To assist in identifying and updating best practices, attorneys should identify experts who can provide ongoing advice and even evaluate online services' confidentiality support through a web assurance seal or evaluative chart designed specifically for attorneys. If even these collaborative steps are unsuccessful in securing reasonable and effective precautions for confidential online legal research, legislation or regulation must provide the needed protection.[215] Attorneys are not the only online researchers who seek control over tracking. Laws that support transparency and require some consumer control could address other confidentiality interests threatened by trends in data collection and re-use. Confidentiality of legal representation is not just a benefit to the attorney and client in a particular relationship, but a societal value that has withstood the test of time and should remain protected.[216]

(arguing that any legislative or regulatory restrictions on behavioral advertising must apply to "*all* entities involved in Internet advertising, including ad networks, search engines and ISPs, will need to adhere to a consistent set of principles" in order to be effective and fair); *Testimony of Dr. Alma Whitten*, *supra* note 17, at 12 (testifying that "Google supports the development of comprehensive, baseline privacy legislation" as long as the legislation has even-handed application to all data sources, both online and offline).

[215] *See* Marc Rotenberg, *Fair Information Practices Principles and The Architecture of Privacy (What Larry Doesn't Get),* 2001 STAN. TECH. L. REV. 1 (2001) (critiquing the view that market forces address consumer online privacy needs and advocating reliance on the law as the more democratic expression of citizens' privacy interests).

[216] *See* James P. Nehf, *Recognizing the Societal Value in Information Privacy,* 78 WASH. L. REV. 1 (2003) (arguing that if privacy were addressed as a societal rather than individual concern, a more comprehensive regulatory approach would emerge).