DON'T BE EVIL: THE FOURTH AMENDMENT IN THE AGE OF GOOGLE, NATIONAL SECURITY, AND DIGITAL PAPERS AND EFFECTS

Andrew William Bagley[*]

TABLE OF CONTENTS

[*] Andrew William Bagley, Alexander von Humboldt German Chancellor Fellow; J.D., University of Miami School of Law, 2009; M.A. Mass Communication, University of Florida, 2006; B.A. Political Science, University of Florida, 2005; B.S. Public Relations, University of Florida, 2005. I would like to thank Professor Mario Barnes for his invaluable help and feedback as I explored this topic and the Alexander von Humboldt Foundation for its generous support.

I. ABSTRACT

This Article offers an overview of current Fourth Amendment law in light of evolving concepts of papers and effects, expectations of privacy online, and the third party and state action doctrines. Scholars have addressed some of these issues individually, but this Article analyzes the legal issues that subsist in the wake of the NSA Terrorist Surveillance Program dilemma and during Congress' current push to update the Electronic Communications Privacy Act. Individuals are increasingly turning to third party technology companies such as Google to host their most private papers and effects, yet in doing so are subjecting themselves to non-negotiated Terms of Service and their information to the mercy of a corporate slogan.

Citizens are dependent on third party online service providers for their daily lives at the same time that these companies are becoming more intermingled with government agencies. However, current statutes are too antiquated to apply Fourth Amendment protections to today's digital papers and effects. Moreover, the existing third-party doctrine ignores the anonymity of email and media service providers in the cloud, and the state action doctrine has not adapted to restrain these entities from voluntarily divulging amounts of data more vast than that traditionally collected by state actors through normal investigative means. This article advocates the modification of current Fourth Amendment doctrine to adjust to an era in which private entities voluntarily share potentially private data with governmental entities.

II. INTRODUCTION

The federal government often has solicited cooperation, assistance, and information from large private-sector companies, particularly during the past decade, to pursue national security investigations.[1] However, these roles recently reversed when information giant Google chose to voluntarily provide data to the National Security Agency (NSA) in hopes of boosting its own security.[2] This incident made clear the pertinence of privacy and

[1] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 901, 910 (2008) (exposing the relationship between the government and telecommunication industries as a prime example).

[2] Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*,

constitutional concerns left unresolved when immunity was granted to companies involved in the NSA's Terrorist Surveillance Program[3] and their prevalence during the current expansion of public-private information sharing partnerships.[4] Americans are turning increasingly to cloud computing solutions and the private sector to create, store, and publish their personal *papers and effects*.[5] Simultaneously, governments around the world are pressuring communication providers to make content more easily accessible.[6] Therefore, it is necessary to explore the application of the Fourth Amendment to the realities of a converged digital world and to ponder whether citizens would change their online behaviors if they expected the government to have unfettered access to their data.[7]

Private companies increasingly provide vital services to citizens, some for free and others for a fee.[8] In doing so, third

WASH. POST, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html. Google has also met on multiple occasions with members of the National Security Council. Byron Acohido, *Consumer Advocacy Group Calls for Hearing on Alleged Google Spying*, USA TODAY, July 20, 2010, http://content.usatoday.com/communities/technologylive/post/2010/07/consumer-advocacy-group-calls-for-hearing-on-google-spying/1.

[3] *See* Zachary Keller, Note, *Big Brother's Little Helper's: Telecommunication Immunity and the FISA Amendment Act of 2008*, 70 OHIO ST. L.J. 1215, 1218-21, 1232-33 (2009) (stating that the FISA Amendment Act of 2008 granted immunity to telecommunication companies that assisted in the NSA's Terrorist Surveillance Program); Associated Press, *Bush Signs Bill on Government Wiretapping*, MSNBC.COM (July 10, 2008, 4:45 PM), http://www.msnbc.msn.com/id/25622627/ [hereinafter *Bush Signs Bill on Government Wiretapping*] (describing the debate over the Act as "a battle that pitted privacy and civil liberties concerns over the desire to prevent terror attacks").

[4] *See* Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J., July 8, 2010, http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html. Private sector companies are now allowing the NSA to install network monitoring sensors to protect critical infrastructure. *Id.*

[5] *See* JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING 2 (2010), *available at* http://pewinternet.org/~/media//Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf.

[6] Miguel Helft et al., *For Data, Tug Grows Over Privacy vs. Security*, N.Y. TIMES, Aug. 3, 2010, http://query.nytimes.com/gst/fullpage.html?res=9504E4D6113CF930A3575BC0A9669D8B63&sec=&spon=&pagewanted=1

[7] Google's own CEO predicts that some people would change their names if the rest of the world had access to their online footprints. Murray Wardrop, *Young Will Have to Change Names to Escape 'Cyber Past' Warns Google's Eric Schmidt*, TELEGRAPH, Aug. 18, 2010, http://www.telegraph.co.uk/technology/google/7951269/Young-will-have-to-change-names-to-escape-cyber-past-warns-Googles-Eric-Schmidt.html.

[8] *See, e.g.*, *Sample Bill*, AT&T, https://www.customerservice.att.com

parties such as information service provider, Google, and telecommunication giant, AT&T, amass large amounts of personal user data.[9] In many instances, citizens relinquish personal data in exchange for free services, such as email and instant messaging, or low-cost long distance phone calls.[10] Traditionally, such data has been used by companies for niche marketing and research purposes.[11] However, in recent years the United States government has built national security databases with personal user data allegedly obtained from cooperating telecommunication companies such as Bellsouth,[12] AT&T[13] and Verizon.[14]

In 2006, lawsuits against Bellsouth, AT&T and Verizon alleged that the companies violated consumer confidentiality by

/sample_bills/sample_print_lld.html (last visited Nov. 29, 2010) (AT&T provides phone services for a fee); *Welcome to Gmail,* GMAIL, http://mail.google.com/mail/help/open.html (last visited Nov. 29, 2010) (Google provides email service for free). An enormous population is transmitting their personal data through computer servers owned by private parties. *See* Solarina Ho, *Poll Finds Nearly 80 Percent of U.S. Adults Go Online*, REUTERS (Nov. 5, 2007, 8:35 PM), http://www.reuters.com/article/internetNews/idUSN05598284200711O6?feedType=RSS&feedName=internetNews&rpc=22&sp=true (nearly 80% of American adults use the Internet).

[9] *See* Elinor Mills, *Google Balances Privacy, Reach*, CNET NEWS (July 14, 2005, 4:00 AM), http://news.cnet.com/Google-balances-privacy,-reach/2100-1032_3-5787483.html; Eric Benderoff & Jon Van, *Privacy? What Privacy?*, CHI. TRIB., May 14, 2006, http://articles.chicagotribune.com/2006-05-14/news/0605140367_1_google-privacy-digital.

[10] *See* Robert Luke, *Web Portals as Purchasing Ideology*, 8 TOPIA: CAN. J. OF CULTURAL STUD. 61, 61, 64, 70–71, 71 n.11 (2002), *available at* http://pi.library.yorku.ca/ojs/index.php/topia/article/viewFile/142/133 (explaining that to use ISP services such as email and instant messaging "clients must relinquish their personal data"); *Teach Your Phone New Tricks*, GOOGLE VOICE, https://www.google.com/accounts/ServiceLogin?service=grandcentral&passive=1209600&continue=https://www.google.com/voice&followup=https://www.google.com/voice&ltmpl=open (last visited Nov. 29, 2010) (showing that by creating a Google account, users can access Google Voice which provides free calls to the U.S. and Canada and provides "[s]uper low rates everywhere else").

[11] Simon Lazarus & Brett Kappel, *Europeans Spur U.S. Debate: Protecting Privacy From Prying Eyes*, LEGAL TIMES, June 15, 1998.

[12] Cheryl Bronson & Pam Benson, *BellSouth, AT&T Added to NSA Lawsuit,* CNN.COM (May 17, 2006), http://edition.cnn.com/2006/POLITICS/05/16/NSA.suit/.

[13] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls,* USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[14] Marguerite Reardon, *Verizon Sued for Alleged NSA Cooperation*, CNET NEWS (May 15, 2006, 3:16 PM), http://news.cnet.com/Verizon-sued-for-alleged-NSA-cooperation/2100-1036_3-6072483.html.

partnering with the National Security Agency (NSA) to monitor phone calls and turn over phone records.[15] Although the lawsuits eventually were mooted by legislation,[16] larger constitutional questions emerged.[17] The U.S. government did not obtain warrants to monitor the phone calls, nor did it rely upon subpoenas to obtain user information as part of the wiretapping program.[18] Thus, the traditional legal process was evaded, and the government obtained potentially incriminating information through voluntary agreements with private corporations.[19] The Fourth Amendment likely was not triggered because private companies did the data gathering and managed the phone calls; therefore, no explicit state action was present.[20] The companies waived their own Fourth Amendment rights by consenting to the government's requests and did not necessitate the government's use of the subpoena or warrant process.

Modern citizen behavior makes it important to reexamine aspects of the third party and state action doctrines in light of blurring private-public boundaries and customer-citizen distinctions. For purposes of illustrating the epitome of private-

[15] Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 900, 911 (N.D. Ill. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978, 988 (N.D. Cal. 2006); *In re* Nat'l Sec. Agency Telcomms. Records Litig., 444 F. Supp. 2d 1332, 1333-34 (J.P.M.L. 2006).

[16] *See Bush Signs Bill on Government Wiretapping*, *supra* note 3 (describing the bill signed into law by President Bush to grant immunity to telecommunications companies that helped the U.S. government "spy on Americans in suspected terrorist cases").

[17] *See* David Kravets, *Courts*, *Congress Shun Addressing Legality of Warrantless Eavesdropping,* WIRED.COM (Jan. 29, 2010, 4:00 PM), http://www.wired.com/threatlevel/2010/01/legality-of-warrantless-eavesdropping/ (noting that AT&T's alleged "funneling . . . of its customers' electronic communications to the [NSA] – without warrants" precipitated a lawsuit claiming "major violations of the Fourth Amendment right to be free from warrantless searches and seizures").

[18] Reardon, *supra* note 14; *Verizon Sued over NSA Surveillance*, SPAM DAILY NEWS (May 13, 2006), http://www.spamdailynews.com/publish/Verizon_sued_over_NSA_surveillance.shtml; David Kravets, *Judge Tosses Telecom Spy Suits*, WIRED.COM (June 3, 2009, 2:30 PM), http://www.wired.com/threatlevel/2009/06/telecom_suit/.

[19] *See* Cauley, *supra* note 13.

[20] The state action doctrine allows for liabilities to attach to government actors for private actions in certain circumstances. Villegas v. Gilroy Garlic Festival Ass'n, 541 F.3d 950, 954–55 (9th Cir. 2008) ("'[S]tate action may be found if, though only if, there is such a 'close nexus between the State and the challenged action' that seemingly private behavior 'may be fairly treated as that of the States itself.'" (quoting Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 295 (2001))). However, such circumstances were not present here.

sector data collection, this research focuses on the evolution of *papers and effects* increasingly stored by third party Internet giants such as Google. Congress is currently holding hearings to update the Electronic Communications Privacy Act which provides the bulk of statutory protection for email privacy.[21] However, this article argues that statutory protections alone are inadequate to protect the evolving concept of a person's papers and effects and that Fourth Amendment jurisprudence must adapt to modern digital trends. Moreover, these legal issues must be resolved so that the government and third party service providers alike can unambiguously comply with constitutional requirements while cooperating.[22] Part I of this article provides an overview of the current Internet age privacy dilemma. Part II identifies current statutory protections afforded to online data and exposes ambiguous and unprotected areas.

Part III explains how the *papers and effects* protected by the Fourth Amendment are increasingly migrating into the digital domain and identifies the extent of a reasonable expectation of privacy in an online world controlled by third parties. Part IV discusses the prospect of implicit consumer consent to searches via contracts of adhesion. Part V highlights the state action doctrine and addresses the possibility of applying it to prevent another NSA dragnet debacle. Lastly, the conclusion advocates the recognition of full Fourth Amendment protections for digital papers and effects to adequately address the realities of the privacy and national security roles played by private actors.

[21] *See* Gabriel Perna, *Congress Eyes Reform of Wiretapping Law*, INT'L BUS. TIMES, (June 25, 2010, 2:59 AM), http://uk.ibtimes.com/articles/30636/20100624/congress-eyes-reform-of-wiretapping-law.htm.

[22] A whole coalition of communication providers supports reforming the ECPA to update privacy laws to match the realities of consumer behavior. *See* Sam Gustin, *Google, Microsoft, ACLU Form 'Digital Due Process' for E-Privacy Reform*, DAILY FIN. (Mar. 30, 2010, 3:40 PM), http://www.dailyfinance.com/story/company-news/google-microsoft-aclu-form-digital-due-process-for-e-privacy/19420228/. This coalition includes companies such as Google and Microsoft who provide cloud computing services and even AT&T which participated in the NSA Terrorist Surveillance Program. *See id.*; *About the Issue*, DIGITAL DUE PROCESS, http://www.digitaldueprocess.org (last visited Nov. 29, 2010).

III. INFORMATION FREE FLOW IN THE AGE OF THE INTERNET

A. The NSA Terrorist Surveillance Program and Unresolved Issues

The Bush administration authorized a large scale electronic communications interception program after the attacks of September 11, 2001 dubbed the Terrorist Surveillance Program (TSP).[23] While the aim of the program was to intercept evidence in order to prevent terrorist attacks, the lack of court authorization by way of subpoena or warrant raised the prospect of government fishing expeditions.[24] Moreover, questions emerged challenging whether or not the administration violated the Foreign Intelligence Surveillance Act which governs surreptitious domestic intelligence gathering. The Electronic Frontier Foundation alleged that the telephone companies allowed the government to utilize their networks to capture telephone, e-mail, and web browsing activities of millions of people.[25]

Companies such as AT&T claimed that they merely complied with government requests for national security purposes that were lawful under the Wiretap Act,[26] which permits the Attorney General to certify that communications may lawfully be intercepted without a warrant.[27] Wholly domestic phone calls and data were monitored by the NSA in at least some instances, despite initial government claims that the TSP merely monitored calls where at least one party was abroad.[28] Moreover, the NSA engaged in "significant and systemic" overuse of unwarranted, non-FISA interception of e-mails and phone calls well into 2009

[23] John Diamond & David Jackson, *Surveillance Program Protects Country, Bush Says*, USA TODAY, Jan. 23, 2006, http://www.usatoday.com/news/washington/2006-01-23-bush_x.htm.

[24] Mark Hosenball, *Hold the Phone*, NEWSWEEK (May 22, 2006), http://www.newsweek.com/2006/05/21/hold-the-phone.html#.

[25] Declan McCullagh, *Legal Loophole Emerges in NSA Spy Program*, CNET NEWS (May 17, 2006, 5:15 PM), http://www.news.com/Legal-loophole-emerges-in-NSA-spy-program/2100-1028_3-6073600.html?tag=nefd.lede [hereinafter *Legal Loophole Emerges in NSA Spy Program*].

[26] 18 U.S.C. § 2511 (2010).

[27] *Legal Loophole Emerges in NSA Spy Program*, *supra* note 25.

[28] James Risen & Eric Lichtblau, *Spying Program Snared U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, http://www.nytimes.com/2005/12/21/politics/21nsa.html?ex=1292821200&en=91d434311b0a7ddc&ei=5088&partnpa=rssnyt&emc=rss.

that exceeded limits imposed by Congress.[29]

Two lawsuits filed against telecommunication companies in 2006 initially were permitted to continue on their merits despite the government's invocation of the state secrets doctrine. However the cases effectively were mooted by the FISA Amendments Act of 2008.[30] In *Hepting v. AT&T Corp.*, the District Court for the Northern District of California initially held that the state secrets privilege could not be used to dismiss a lawsuit against AT&T for its alleged involvement in the TSP because plaintiffs could proceed on other well known information about AT&T's collusion with the government.[31] However, the case later was remanded to the district court, consistent with the immunity granted in the act.[32] In *Al-Haramain Islamic Found., Inc. v. Bush*, the U.S. Court of Appeals for the Ninth Circuit held that the state secrets privilege could not be used to dismiss a TSP lawsuit against the government in which public knowledge existed about the contents of a classified document.[33] However, the case never was decided on its merits, and litigation is still pending with a group of other TSP lawsuits that challenge the constitutionality of the immunity clause in the FISA amendments.[34]

The legal issues left unresolved by the thwarted TSP lawsuits are dwarfed by the prospect of larger data gathering schemes involving online service providers. The government's unwarranted seizure of phone data, while alarming, likely was insufficient to obtain convictions without further evidence.[35]

---

[29] Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 15, 2009, http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=3.

[30] *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2467–69, 2471 (2008) (granting electronic communication service providers immunity from suit for assisting the government pursuant to a directive from the Attorney General and the Director of National Intelligence).

[31] Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 993–94, 1011 (N.D. Cal. 2006), *remanded by* 539 F.3d 1157 (9th Cir. 2008).

[32] Hepting v. AT&T Corp., 539 F.3d 1157, 1158 (9th Cir. 2008).

[33] Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1195–96, 1198, 1203–06 (9th Cir. 2007).

[34] *See In re* Nat'l Sec. Agency Telecomms. Records Litig., 700 F. Supp. 2d 1182, 1185–92, 1197, 1203–04 (N.D. Cal. 2010).

[35] However, criminal convictions were obtained based on phone data collected without a warrant by the FBI in an incident unrelated to the NSA program. *See* Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET NEWS (Feb. 11, 2010, 4:00 AM), http://news.cnet.com/8301-13578_3-10451518-38.html

Despite this, the information an entity such as an email and information provider possesses on a single user conceivably can be enough to convict them or to create an arbitrary and embellished character profile of an individual. For example, incriminating web searches, emails, documents, photos, location data, and even evidence of acquaintanceship can be extracted from a user account.[36]

B. Privacy and Fourth Amendment concerns in the age of Google

Citizens increasingly are trusting private companies with personal information in exchange for innovative, and sometimes necessary,[37] services. For decades banks have been entrusted with sensitive personal information about their clients in order to facilitate financial transactions.[38] Shortly after the attacks of September 11, 2001, lawsuits were launched against airlines for turning over private passenger information to government contractors.[39] In 2003, the FBI requested personal data from hotels, rental-car agencies and airlines in an effort to thwart then-looming Las Vegas terrorist threats.[40] In some instances,

[hereinafter *Feds Push for Tracking Cell Phones*] (demonstrating that while collected phone data does not fulfill the elements of the specific crime, it can be used in drawing an inference about the defendant's connection to the crime).

[36] *See, e.g.*, Julia Lewis, *Petrick Prosecutors to Reopen Case with New Computer Evidence*, WRAL.COM (Nov. 28, 2005), http://www.wral.com /news/local/story/122105/ (explaining how evidence gathered from Google searches was used in a trial against a man who allegedly killed his wife); Kim Zetter, *NSA-Intercepted E-Mails Helped Convict Would-Be Bombers*, WIRED.COM (Sept. 8, 2009, 6:26 PM), http://www.wired.com/threatlevel/2009/09/nsa-email/ (explaining how evidence gathered by the NSA from email user accounts was passed to British prosecutors and presented at trial to convict three airplane bomb plotters). *See also* U.S. DEP'T OF HOMELAND SEC., BEST PRACTICES FOR SEIZING ELECTRONIC. EVIDENCE (3d ed.), *available at* http://www.forw *ardedge2.com/pdf/bestpractices.pdf (characterizing the types of electronic evidence seized according to the crimes they are associated with).*

[37] An email address has become almost as ubiquitous as a home address for employment, education, and billing purposes.

[38] *See* PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 49–56 (2004) (examining the history of the anti-money laundering regime and the laws passed in the United States effectuated to prevent money laundering).

[39] Drew Shenkman, Comment, *Flying the Not-So-Private Skies: How Passengers' Personal Information Privacy Stopped at the Airplane Door, and What (If Anything) May Be Done To Get It Back*, 17 ALB. L.J. SCI. & TECH. 667, 668–70 (2007).

[40] Ellen Nakashima, *From Casinos to Counterterrorism*, WASH. POST, Oct. 22, 2007,http://www.washingtonpost.com/wp-dyn/content/article/2007/10

the data was voluntarily handed over.[41] The Department of Defense even undertook a data-mining venture called the Total Information Awareness Project, which was later defunded by Congress.[42] Now, the number of industries accumulating such information is more numerous, and the scope of inquiries is exponentially wider.[43]

Although much attention has focused on controversies surrounding telephone company cooperation with the NSA, any of the most popular information service providers, such as Google, Microsoft, or Yahoo!,[44] could just as easily hand over user data from emails, calendars, voicemails, phone and instant message logs, web keyword searches, or photos. Government agencies already have used administrative subpoenas such as national security letters to compel disclosure of subscriber information.[45] Yet, consumers do not definitively waive Fourth Amendment rights merely by clicking "I agree" to an end-user license agreement. Nonetheless, private companies are not restrained as state actors when they voluntarily hand consumer data to the government. Instead, they are treated as a third party in whom a consumer is placing their trust.

Google perhaps epitomizes the data accumulation trend more

/21/AR2007102101522.html

[41] *Id.*

[42] John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, http://www.nytimes.com/2002/11/09/politics/09COMP.html?scp=1&sq=Pentagon%20Plans%20a%20Computer%20System%20That%20Would%20Peek%20at%20Personal%20Data%20of%20Americans&st=cse; Mark Williams, *The Total Information Awareness Project Lives On*, TECH. REV., (Apr. 26, 2006), http://www.technologyreview.com/Infotech/16741/?a=f (stating that Congress terminated funding of the Total Information Awareness Project but conditionally allows funding for projects involving component technology used for foreign intelligence or military use against non-U.S. citizens).

[43] For a thorough discussion of the Fourth Amendment issues surrounding government contractors and private-sector data-mining services, see Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 319–21, 336–40 (2008).

[44] *See* Mark Brownlow, *Email and Webmail Statistics*, EMAIL MKTG. REPS. (Apr.2008),http://www.email-marketing-reports.com/metrics/email-statistics.htm.

[45] *See* Joshua A. Altman, Note, *A Schrodinger's Onion Approach to the Problem of Secure Internet Communications,* 7 WASH. U. GLOB. STUD. L. REV. 103, 123–25, 128, 130 (2008). Moreover, the Patriot Act allowed mere administrative requests via national security letters to compel ISPs to turn over user data without user knowledge or judicial oversight. *Id.* at 126–28; 18 U.S.C. § 2703 (2010).

than any other private entity.[46] Google's profit model is based on offering free services to consumers in exchange for their consent to non-negotiable terms of service.[47] The services provided by Google encourage users to submit information that is organized and utilized to provide innovative and efficient means of online communication and digital media interaction.[48] However, Google's advertising system even tracks users' web browsing habits when they stray from Google's own website.[49] The information collected by Google allows the company to sell targeted advertising spots. Thus, the more information Google has about a user, the better the company can tailor the ads and increase their value.

Aside from tracking search and web browsing habits, Google also amasses data on emails, photos, healthcare records, phone calls, voicemails, and documents created on and sent through its servers.[50] Additionally, Google and similar companies boast the ability to pinpoint a user's exact location via their Internet Protocol address or through cell phone triangulation, allowing users to share this data with their friends.[51] Thus, the

[46] Although Facebook might have more personal details about users and lax privacy concerns, users are opting to share much of this information with other users. *See* Sharon Gaudin, *Q&A: Facebook Users Aren't Outraged Over Privacy Issues,* NETWORK WORLD (May 7, 2010, 6:22 AM), http://www.networkworld.com/news/2010/050710-qa-facebook-users-arent-outraged.html. A Google account, on the other hand, is seemingly private unless users opt into sharing specific documents or photo albums. *See Frequently Asked Questions for the Google Analytics Data Sharing Options*, GOOGLE ANALYTICS, http://www.google.com/support/analytics/bin/answer.py ?hl=en&answer=87515 (last visited Nov. 29, 2010).

[47] *See Google Terms of Service,* GOOGLE (Apr. 16, 2007), http://www.google.com/accounts/TOS.

[48] *See Privacy Principles*, GOOGLE, http://www.google.com/corporate/privacy_ principles.html (last visited Nov. 29, 2010) (stating that Google uses the information its users share to "build services and products that are valuable to them").

[49] Murad Ahmed, *Google Ad Service Raises Privacy Fears*, TIMES (London), Mar.11,2009,http://technology.timesonline.co.uk/tol/news /tech_and_web/article5887701.ece.

[50] *See About Google Voice*, GOOGLE VOICE, http://www.google.com/sup port/voice/bin/answer.py?hl=%20en&answer=115061 (last visited Nov. 29, 2010); *About Google Health*, GOOGLE HEALTH, http://www.google.com/intl/en-US/health/about/index.html (last visited Nov. 29, 2010); *More Google Products,* GOOGLE, http://www.google.com/intl/en/options/ (last visited Nov. 29, 2010).

[51] *See* Stephen E. Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 381-85 (2006) (describing the advantages of refined location tracking). Yahoo also offers a location awareness service. *Yahoo Launches Latitude-like App for Facebook*,

accumulation of a citizen's email, documents, voicemails, phone logs, records, photos, and even location by Google rivals and perhaps exceeds the data gathering capabilities of traditional law enforcement methods. Google's database of consumer information is valuable to an outside government entity or advertiser. However, the aggregate of data collected on a person is even more invasive when analyzed to create a profile of a user's habits.[52]

The synthesis of data from a user's web search history coupled with email, photos, documents, voicemails, phone logs, and location, creates a profile of an individual that serves as behavior modeling for advertisers.[53] This same data could just as easily be disclosed to law enforcement officials for criminal profiling. Social networking sites such as MySpace and Facebook likewise create additional privacy concerns. However, in these instances a user often controls who can view their information, although such a company potentially could voluntarily disclose such information to a law enforcement entity.[54] The United Kingdom is already considering plans to use data obtained by such sites to monitor users and prevent terrorism and crime.[55] Additionally, it is alleged that Google employees have met with members of the National Security Council to discuss potential collaborations.[56]

TECHTREE.COM (Mar. 17, 2009, 2:54 PM), http://www.techtree.com/India/News/Yahoo_Launches_Latitude-like_App_for_Facebook/551-100105-580.html (Fire Eagle from Yahoo allows Facebook users to share their location with friends). Google recently confirmed that it was logging WLAN routers and MAC addresses. Kevin J. O'Brien, *New Questions over Google's Street View in Germany*, N.Y. TIMES, Apr. 29, 2010, http://www.nytimes.com/2010/04/30/technology/30google.html.

[52] *See* Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, http://www.nytimes.com/2010/03/17/technology/17privacy.html (discussing the "power of computers to identify people from social patterns").

[53] *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 261–63, 272 (2008) (explaining how data mining and profiling work).

[54] *See* Eric Kuhn, *Senators Urge Facebook to Change Privacy Settings*, CNN.COM (Apr.28,2010), http://edition.cnn.com/2010/POLITICS/04/27/senators.facebook/index.html (explaining that Facebook recently drew the ire of members of the U.S. Senate when it made previously private user data public).

[55] Murray Wardrop, *Facebook Could Be Monitored by the Government*, TELEGRAPH, Mar. 25, 2009, http://www.telegraph.co.uk/technology/facebook/5046447/Facebook-could-be-monitored-by-the-government.html.

[56] Byron Acohido, *Consumer Advocacy Group Calls for Hearing on Alleged Google Spying*, USA TODAY, July 20, 2010, http://content.usatoday.com/communities/technologylive/post/2010/07/consumer-advocacy-group-calls-for-hearing-on-google-spying/1.

Private data is amassed not only by many different companies but also is dispersed lawfully, unlawfully, and by accident.[57] Even traditional law enforcement means of retrieving online data by subpoenas is not limited merely to requests for relevant data from individual accounts. In 2005, the Department of Justice issued subpoenas to Google, America Online, Yahoo!, and Microsoft to compel the release of randomly selected user search records.[58] The DOJ's request was not intended to help solve a crime or prevent a terrorist attack.[59] Instead the data was requested for analytical purposes to support a new attempt to pass Internet child protection legislation.[60] While AOL and Yahoo! complied, Google remained defiant and refused to abide by the request.[61]

In *Gonzales v. Google*, the Department of Justice sued the Internet search giant for its failure to comply with the subpoena.[62] Among other things, Google argued that even randomly selected search strings could be revealing if a user searched for their own name, social security number, or credit card number.[63] Additionally, Google argued that its business was predicated on protecting its users' privacy.[64] The U.S. District Court for the Northern District of California was quick to point to Google's own privacy policy, which did not protect users' search strings but merely their personal information.[65] Nonetheless, the court acknowledged that the fact that a quarter of all web searches are for pornography was evidence that there exists some expectation of privacy by at least some users.[66] In the end, Google was compelled only to generate a list of URLs, rather than actual user search queries.[67]

Although marketplace and public relations forces likely

---

[57] *See* Karim Z. Oussayef, Note, *Selective Privacy: Facilitating Market-Based Solutions to Data Breaches by Standardizing Internet Privacy Policies*, 14 B.U. J. SCI. & TECH. L. 104, 112–14, 116, 118 (2008).

[58] *Latest Google Lawsuits*, LINKS & LAW.COM (Apr. 4, 2006), http://www.linksandlaw.com/news-update38.htm ; Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, http://www.nytimes.com/2006/01/20/technology/20google.html.

[59] *See id.*

[60] *Id.*

[61] *Id.*

[62] Gonzales v. Google, Inc., 234 F.R.D. 674, 678 (N.D. Cal. 2006).

[63] *Id.* at 687.

[64] *See id.* at 683.

[65] *Id.* at 683–84.

[66] *Id.* at 684.

[67] *Id.* at 688.

influenced Google's willingness to comply with a non-investigative government request, Google and other companies might not always feel so restrained. In 2006, America Online (AOL) released data on its customers' search queries for academic purposes. However, the data was matched with unique identifying numbers that could be used to pinpoint a user's identity.[68] One revelation from the data was that of a user whose searches "morphed over several weeks from 'you're pregnant he doesn't want the baby' to 'foods to eat when pregnant' to 'abortion clinics charlotte nc' to 'can christians be forgiven for abortion.'"[69] Thus, the potential for exposure of personal, non-national security related information is apparent.

In reference to the NSA warrantless surveillance program, Yahoo! refused to disclose whether or not it released user data to the government, citing only that it complied with its own privacy policy.[70] Moreover, it was recently revealed that Project Vigilant, a private group of hackers who cooperate with the federal government, receives traffic data from ISPs.[71] The ISPs voluntarily hand over the data about their customers on the basis of End User License Agreements (EULA), which give them permission to do so, and Project Vigilant passes information onto the federal government.[72] Therefore, any privacy interests that may exist are circumvented through a contract of adhesion. These examples demonstrate that the prospect of companies voluntarily providing seemingly-private information to the government is not merely a hypothetical but an increasingly-likely reality.

---

[68] Paul Boutin, *You Are What You Search*, SLATE MAG. (Aug. 11, 2006, 5:30 PM), http://www.slate.com/id/2147590/. S*ee also* Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1 (The New York Times tracked down an AOL user based on her "anonymous" number and asked her about her searches).

[69] *See* Boutin, *supra* note 68.

[70] Declan McCullagh, *Yahoo on NSA surveillance: No comment*, CNET NEWS (Feb. 15, 2006, 1:55 PM), http://news.cnet.com/Yahoo-on-NSA-surveillance-No-comment/2100-1030_3-6040129.html.

[71] Andy Greenberg, *Stealthy Government Contractor Monitors U.S. Internet Providers, Worked with Wikileaks Informant*, FORBES BLOGS (Aug. 1, 2010, 5:44 PM),http://blogs.forbes.com/firewall/2010/08/01/stealthy-government-contractor-monitors-u-s-internet-providers-says-it-employed-wikileaks-informant/.

[72] *Id.*

IV. STATUTORY PROTECTIONS FOR ONLINE DATA

The Electronic Communications Privacy Act (ECPA) affords some privacy guarantees to users of electronic communications by establishing a regime of legal protections for users of any electronic communication service (ECS) or remote computing service (RCS).[73] The law, originally passed in 1986, is a statutory supplement to the Fourth Amendment's third party and private actor doctrines, placing restrictions only on services offered to the public.[74] The ECPA provided a potential cause of action for plaintiffs who sued phone companies that participated in the NSA's warrantless surveillance program until immunity was granted.[75]

Comprised of three main parts, the codified statute incorporates the laws regarding the Wiretap Act, the Stored Communications Act (SCA), and the use of pen register information.[76] The U.S. Court of Appeals for the First Circuit interpreted interception of email stored during the communication process to fall under the wiretap provisions of the ECPA.[77] If this is accepted, then the government is required to obtain a warrant authorized by the Department of Justice and certified by a federal judge in order to intercept such communications.[78] However, if modern-day server-based email content is not analogized to fully-protected voice content then the lesser protections of the Stored Communications Act apply. The SCA merely requires a court order issued upon a reasonable belief that the material requested will be relevant to the investigation, thus falling short of a probable cause burden.[79]

Although aspects of Google and other popular commercial services fall into the ECPA public communication category, other parts of the 1986-era definitions are ambiguous when applied to web-based services such as email.[80] An electronic communication service (ECS) is defined as "any service which provides to users thereof the ability to send or receive wire or electronic

---

[73] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208, 1214 (2004).

[74] *See id.* at 1212.

[75] *See* 18 U.S.C. § 2511 (2010)

[76] *See id.* §§ 2701–03; Kerr, *supra* note 73 at 1208 nn.1–2, 1231 n.151.

[77] United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005).

[78] 18 U.S.C. §§ 2516–18 (2010).

[79] *See id.* § 2703(d).

[80] Kerr, *supra* note 73, at 1216–18.

communications."[81] Communications that are sent within the past 180 days fall under this definition. However, after 180 days then such communications are considered part of a remote computing service (RCS).[82] The government cannot compel disclosure of user content data, such as unopened email,[83] from an ECS within this 180-day period without a warrant. However, the government can compel an RCS provider to release content information without use of a warrant, instead relying only on a subpoena and notice to the subscriber or an 18 U.S.C. § 2703(d) statutory order and prior notice.[84]

The pre- and post-180 day distinctions stem from the concept that email originally was stored only temporarily on third party servers when in route from sender to receiver. This is no longer the case today with web-dependent cloud computing services such as Gmail, Yahoo! and Hotmail. Neither a public ECS nor RCS is permitted to voluntarily disclose content-laden data[85] to the government unless there is a § 2702(b) exception such as a good faith belief that "an emergency involving danger of death or serious physical injury" is imminent.[86] However, an ECS or RCS is permitted to divulge the contents of the electronic communication to another party with the permission of the subscriber of the service.[87] Moreover, the envelope information regarding who sent the email along with billing records are subject only to the aforementioned pen-register administrative subpoena requirements.[88]

Today, many websites require user accounts and permanently store both content and non-content user information. Despite

[81] 18 U.S.C. § 2510(15).

[82] JAMES A. ADAMS, THE NAT'L INST. FOR TRIAL ADVOCACY, OVERVIEW OF CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORD ACCESS (2010).

[83] There is a dispute as to whether or not this covers opened mail as well. The U.S. Court of Appeals for the Ninth Circuit afforded opened emails with the same protections as unopened emails in electronic storage. *See* Theofel v. Farey-Jones, 341 F.3d 978, 985 (9th Cir. 2003). However, other courts disagree with this interpretation, and reason that opened emails can be divulged merely through the subpoena process. *See* United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).

[84] Kerr, *supra* note 73, at 1223.

[85] Content data would include email. This is distinguished from non-content data such as a subscriber's name and address, which is more akin to a pen register.

[86] 18 U.S.C. § 2702(b)(8) (2010).

[87] *See id*. § 2702(b)(3).

[88] *See supra* Part II; 18 U.S.C. § 2703(d).

this, the application of the Electronic Communications Privacy Act is not obvious. In *Re Jet Blue Airways Corp.,* the U.S. District Court for the Eastern District of New York held that the mere fact that Jet Blue provided a website and web service did not qualify the company as a provider under the definition of the ECPA.[89] Even the restrictions placed on relevant services by the ECPA are ambiguous. In *Freeman v. America Online*, the Connecticut Federal District Court interpreted the language in the ECPA broadly not only to restrict when the government can *require* information from ISPs, but also to prevent the government from *merely seeking* such information without adhering to the provisions of the statute.[90]

The Electronic Communications Privacy Act fails to sufficiently protect the privacy rights of users of web-based services such as Gmail, Hotmail, Yahoo! Mail, etc.[91] A Google account could conceivably be both an ECS and an RCS.[92] However, much of its appeal is in its RCS functions because email, documents, photos, search histories, and more are all stored on a Google server, not a user's home computer. Thus, potentially personal and private documents or emails older than 180 days could be disclosed to law enforcement officers without any probable cause or warrant threshold.[93] Moreover, the Terms of Service agreements to which users assent might trigger the subscriber consent exception to the ECPA if the language is worded in such a way as to allow for voluntary disclosure. Due to the ECPA's seemingly ambiguous

[89] *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 307, 309-10 (E.D.N.Y. 2005).

[90] Freedman v. Am. Online, Inc., 303 F. Supp. 2d 121, 127 (D. Conn. 2004).

[91] For a thorough discussion of the ECPA's inadequacies see Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1068–73 (2008).

[92] The U.S. Court of Appeals for the Ninth Circuit has categorized a service hosting opened email on its service as an ECS and some other courts have adopted this position. However, many academics criticize the position as inconsistent with the intent of the legislation. William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1211–12 (2010).

[93] Forced compliance with a subpoena by the service provider may occur even if the service provider believes its users have stronger legal protections. Microsoft, for example, interprets opened and unopened email to have the same protections. *See* Ryan Singel, *Microsoft Takes Down Whistleblower Site, Read the Secret Doc Here*, WIRED.COM (Feb. 24, 2010, 7:03 PM), http://www.wired.com/threatlevel/2010/02/microsoft-cryptome/. However, Microsoft has still been forced to violate its own privacy policies and comply with a subpoena. *See also* Unites States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009).

application to the modern World Wide Web, Congress has held hearings on updating the law – a cause that has received broad support from the service provider community, including Microsoft, Google, and Yahoo!.[94] Regardless of the statutory regime, constitutional issues persist.

V. "DIGITAL PAPERS" AND "EFFECTS"?

A. Expectation of Privacy

Justice Louis Brandeis, in a dissenting opinion in *Olmstead v. United States*, predicted that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[95] This once farfetched notion is now a reality as Americans' papers go digital. The dawn of cloud computing has arrived, and the attractiveness of data-portability means that individuals are migrating their personal documents from in-home hard drives to the machines of remote third parties.[96] With this trend, people are expanding their privacy expectations from the physical confines of their home to that of password-protected accounts for everything from online banking to Internet-based word processing.[97] Users even divulge personal information with

[94] Nancy Scola, *A 21st-Century Fourth Amendment*, THE AMERICAN PROSPECT, TAPPED BLOG (Mar. 31, 2010, 2:04 PM), http://www.prospect.org/csnc/blogs/tapped_archive?month=03&year=2010&base_name=a_21st_century_4th_amendment.

[95] Olmstead v. United States, 277 U.S. 438, 474 (1927) (Brandeis, J., dissenting) (predicting that technological innovations would soon lead the Court to the opposite conclusion). *See also* Katz v. United States, 369 U.S. 347, 358–59 (1967) (holding electronic surveillance of a telephone booth requires prior authorization and a showing of probable cause).

[96] Google is entering a market already populated by other vendors. *See* Kevin J. Delaney & Vauhini Vara, *Google Plans Service to Store Users' Data*, WALL ST. J., Nov. 27, 2007, http://online.wsj.com/article/SB119612660573504716.html.

[97] As of 2008, 69% of Americans were using cloud computing services, with more than half using web-based mail and a third storing their photos or files online. Fawn Johnson, *Most People Who Store Data on Web Want It Private - Study*, DOWJONES VENTUREWIRE (Sept. 15, 2008), http://fis.dowjones.com/products/vw_sample.html. According to a 2010 Zogby International poll, 88% of American adults believe they should be afforded the same privacy protections online as they receive offline. *See* ZOGBY INT'L, RESULTS FROM JUNE 4-7 NATIONWIDE POLL 1(June 7, 2010), *available at* http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf. The notion of a password protected and encrypted online account is akin to a locked container and therefore

an expectation of privacy when conducting search engine queries.[98] However, current case law leaves more questions than answers about the extent of Fourth Amendment protections.

A central issue in applying the Fourth Amendment to technology is determining what is content versus non-content and what a person reasonably expects to remain private. The Court held in *Smith v. Maryland* that a mere list of the phone numbers dialed by a caller is not protected content data.[99] By analogy, email to and from headers as well as IP addresses were interpreted by the U.S. Court of Appeals for the Ninth Circuit to be the same as unprotected pen register data.[100] However, the U.S. Supreme Court hinted in *City of Ontario, Cal. v. Quon* that the pervasiveness of cell phones might strengthen the case for a reasonable expectation of privacy in the content of text messages.[101] For content, the Court applies the Fourth Amendment test from Justice John Harlan's concurring opinion in *Katz v. United States*,[102] which was adopted by the majority in *Smith*, providing a two-pronged defense against Fourth Amendment intrusion.[103] First, an individual must exhibit a subjective expectation of privacy in their relevant activity or communication.[104] Second, the expectation must be one that society is willing to accept as legitimate.[105]

At present, the Supreme Court has been reluctant to recognize an express privacy interest in electronic communication, going so far as to assume the existence of privacy interests in cell phone

deserves Fourth Amendment protections. Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 364–65 (2003). A federal district court initially found an expectation of privacy in a user's Yahoo! email account despite arguments from the U.S. government that the petitioner had no reasonable expectation of privacy. However, the U.S. Court of Appeals for the Sixth Circuit vacated the decision on ripeness grounds. Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008).

98 Matthew Werner, *Google and Ye Shall be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege*, 34 RUTGERS COMPUTER & TECH. L.J. 273, 300–01 (2007). Additionally, as previously mentioned in the article, even Google defended the privacy of search strings when the DOJ requested them. *See supra* Part I.b.

99 *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

100 United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2007).

101 130 S.Ct. 2619, 2630 (2010).

102 Katz v. United States, 389 U.S. 347, 361–63 (1967) (Harlan, J., concurring).

103 *Smith*, 442 U.S. at 740–41.

104 *Id.* at 740 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

105 *Id.*

text messages merely *arguendo* to decide a case on much narrower grounds.[106] While certain information in the hands of third parties, such as traditional business records, is not afforded Fourth Amendment protection equivalent to "papers" or "effects,"[107] there is ambiguity over the constitutional protection afforded to private email or online documents.[108]

A federal district court in Rhode Island found that a Yahoo! email account user had a reasonable expectation of privacy in their password-protected account despite the fact that the user accessed it from a public library.[109] However, if higher courts adopt a narrower standard of privacy, then a user's location might be a decisive factor. A web-based email user does not need to access their documents in public. Instead, consumers of Gmail, Google Docs, and other services are just as likely to view and modify their personal files from the confines of their own home. Traditionally more Fourth Amendment protection has been afforded to the home. Police cannot use a beeper to track the movements of a person within their own home without a warrant.[110] Nor can police use thermal imaging devices to conduct a remote warrantless search of a home.[111] By analogy, a user should, at the bare minimum, have a reasonable expectation of privacy in their home even when accessing their digital documents and effects, whether or not the data is local.[112]

On the contrary, location data is used by Google's email service, Gmail, when scanning information and text contained in

106 *See City of Ontario, Cal.*, 130 S. Ct. at 2630.

107 *See* U.S. CONST. amend. IV. *See also* Seth Rosenbloom, *Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act*, 39 COLUM. HUM. RTS. L. REV. 529, 534–35 (2008).

108 *See generally*, United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002) (explaining when email files are protected under the Fourth Amendment); Kerr, *supra* note 72, 1210–12 (outlining three reasons why the Fourth Amendment does not afford protections for online documents); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 522 (2005) (detailing that courts have yet to clarify if the "sender of email[s] retain[ ] a reasonable expectation of privacy . . . .").

109 *See* Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006).

110 *See* United States v. Karo, 468 U.S. 705, 717–18 (1984).

111 Kyllo v. United States, 533 U.S. 27, 37, 40 (2001).

112 Alternatively, a person does not always enjoy a reasonable expectation of privacy in their location data. At present, the Obama administration argues that individuals enjoy no expectation of privacy in the location of their cell phones. *See Feds Push for Tracking Cell Phones*, *supra* note 35.

email and documents to generate relevant advertisements.[113] Therefore, such a knowing relinquishment of information might affect a *Katz*-analysis of a person's reasonable expectation of privacy and perhaps be analogous to items in the plain view of the public. Or, alternatively, the Internet Protocol location data indicating that a person is in their home might afford them greater Fourth Amendment protection when they are home. However, these concepts ignore the fact that although individuals might voluntarily allow their data to be scanned by an automatic system that generates tailored advertisements for their eyes only, it is not a foregone conclusion that they are therefore consenting to unfettered law enforcement or personified third party access to their data. Moreover, a person's privacy in their documents and effects should hinge more on their property and privacy interests in the documents and effects, rather than their technical location. Thus, password-protected, encrypted digital storage containers should be a Fourth Amendment-protected place to store the "most intimate occurrences of the home."[114]

B. Third-party doctrine

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[115]

The Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[116] Such a blanket concept is troublesome enough when dealing with issues of "shared privacy" between individuals.[117] However, the doctrine appears

---

[113] Laura Rohde, *GMail Still Dogged by Privacy Issues*, COMPUTERWEEKLY.COM(Apr.16,2004,10:33AM), http://www.computerweekly.com/Articles/2004/04/16/201808/Gmail+still+dogged+by+privacy+issues.htm.

[114] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[115] United States v. Miller, 425 U.S. 435, 443 (1976).

[116] Smith v. Maryland, 442 U.S. 735, 743–44 (1979). This sentiment is echoed in *S.E.C. v. Jerry T. O'Brien, Inc.* 467 U.S. 735, 743 (1984).

[117] Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the*

increasingly archaic and problematic when the third party is a seemingly anonymous and automated online media service provider.[118] The doctrine was articulated before digital documents and effects were stored in the cloud and should be distinguished from the relationship between a communication server provider and its users.

One argument promoted to limit this doctrine advances the notion that the Fourth Amendment third party test should relinquish protection only for information volunteered for a third party's use.[119] However, Google scans virtually all text from user emails, documents, and searches to determine which advertisements to display.[120] Therefore, such a doctrine conceivably would fail to afford any Fourth Amendment protections to a user entrusting their data to a third party. Moreover, a user usually does not have standing to sue the government for taking information from a third party. The U.S. Court of Appeals for the Eleventh Circuit recently opined that "voluntary delivery of emails to third parties constituted a voluntary relinquishment of the right to privacy in that information" when dismissing a lawsuit against the government for subpoenaing the content of the plaintiff's emails from an ISP.[121]

The fact that the government was able to obtain the emails from the service provider, rather than the email recipient, without triggering the Fourth Amendment exemplifies the current problem. The Internet is run primarily by private entities beginning with the cable, telephone wire, or wireless network running into a user's home all the way to the webpage on a remote server accessed by their computer. Therefore, users interact with a myriad of digital third parties in every online activity from sending an email to navigating the Web. As such,

Rights of Relationships, 75 CALIF. L. REV. 1593, 1616–19 (1987).

[118] Cracks have begun to emerge in the doctrine through some state constitutional protections, but the doctrine remains largely unchanged. *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 412–13 (2006).

[119] *Id*. at 378.

[120] Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271–73 (2008); *More on Gmail and Privacy*, GOOGLE, http://mail.google.com/mail/help/about_privacy.html#scanning_email(last visited Nov. 29, 2010).

[121] Rehberg v. Paulk, 598 F.3d 1268, 1282 (11th Cir. 2010).

users' expectations of privacy appear inconsistent with traditional notions of third-party "false friends" when applied to online communications.

A strong argument in favor of preserving the third-party doctrine is the necessity of maintaining the public parts of crimes and allowing evidence to come to light for investigation and prosecution.[122] Even absent Fourth Amendment protection, other legal protections from "[c]ommon law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections" offer some defenses for those targeted based on their Gmail accounts.[123] However, sidestepping the Fourth Amendment ignores the technological evolution of papers and effects in the digital era. Moreover, it fails to acknowledge that individuals might be willing to share their documents and effects with online service providers but not offer them for warrantless review by law enforcement entities. Therefore, the third-party doctrine should not be oversimplified.

A service provider's voluntary disclosure of users' emails and documents to the government might find support in the false friend theory. However, in *United States v. James*, the U.S. Court of Appeals for the Eighth Circuit rejected the government's claim that the defendant abandoned his privacy interests in a CD when he handed it to a third party with instructions to destroy it.[124] Moreover, the false friend notion is inconsistent with the distinctions drawn in *Smith v. Maryland* between subscriber data and a phone conversation itself.[125] An argument advanced in support of the third-party doctrine contends users divulging information to a third party "implies consent" under the Fourth Amendment.[126] However, this argument removes the reasonable expectation of privacy framework in exchange for a presumptive

[122] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564–65 (2009).

[123] *Id.* at 565.

[124] *See* 353 F.3d 606, 616 (8th Cir. 2003).

[125] The Fourth Amendment protects private conversations where the party has not consented to surveillance or monitoring, but not where the party has given consent to such activity, signifying the existence of a reasonable expectation of privacy. *See* United States v. White, 401 U.S. 745, 747, 749, 752–54 (1971). *C.f.,* Smith v. Maryland 442 U.S. 735, 742–44 (1979) (stating that Pen registers only record numbers, and not the content of the phone conversations. Since the Fourth Amendment applies only to privacy, recording phone numbers falls outside the gambit of a person's reasonable expectation of privacy).

[126] Kerr, *supra* note 122 at 565.

conclusion of search acquiescence. This argument is especially weak when the party is not a person but instead an automated digital document repository.

Contrary to traditional third party information exchanges, Google's "secure"[127] services might lead a user reasonably to believe that their contents are in a virtual closed container, justifying a reasonable expectation of privacy.[128] This analogy allows users reasonably to assume that their data is safe from unwarranted governmental intrusion even if Google's automated algorithms can access it for advertising purposes.[129] One could argue that users might reasonably risk betrayal by a service provider playing the role of a false friend. Moreover, users could reasonably expect that Google might read their email and disclose it to the government. However, the fact that a user protects their Google account, which contains email, documents, photos, location information, and more, with encryption and a password lends credence to both a subjective and perhaps objective expectation of privacy from both personal access by Google employees and unwarranted law enforcement access. Therefore, some authors have applied the analogy of a traditional closed container to encrypted, password-protected email.[130]

The contents of a user's encrypted, password-protected account is beyond public view and is perhaps an extension of a filing cabinet in a private single-user home office or at least a locked container.[131] Unlike a home dwelling, which a person may share

[127] Google advertises Gmail as a "secure" email service. *Gmail: Google's Approach to email*, GMAIL, http://mail.google.com/mail/help/intl/en/about.html#faq (last visited Nov. 29, 2010).

[128] A user might conceivably assume that "deleted" mail is inaccessible too. Such mail, however, can remain on both online third party servers as well as offline backups. *See Google Privacy Policy,* GOOGLE, http://mail.google.com/mail/help/intl/en/privacy.html (last visited Nov. 29, 2010); *see generally*, *Email*, SURVEILLANCE SELF DEFENSE, https://ssd.eff.org/tech/email (last visited Nov. 29, 2010) (discussing that e-mails can be stored in third party computers through channels such as the service provider, employers, ISP, webmail provider, or can be stored by those you communicate with).

[129] Google advertises that no human is involved in this email-scanning process. Thus, a user might not have a reasonable expectation of privacy from a computer that it might from a human. *See Ads in Gmail and Your Personal Data*, GMAIL HELP, http://mail.google.com/support/bin/answer.py?hl=en&answer=6603 (last visited Nov. 29, 2010); *see also* Paul Hartsock, *HP's Wallet-Busting Win*, E-COM. TIMES, (Sept. 3, 2010, 9:58 AM), http://www.ecommercetimes.com/story/70758.html?wlc=1285606130.

[130] *See e.g.,* Henderson, *supra* note 108 at 533–35.

[131] Courts traditionally have found a reasonable expectation of privacy in locked containers and even unlocked containers. The password-protected aspect

with others, a user is likely the only individual with access to their account password.[132] Thus, by analogy, emails and digital documents within the account should warrant the same Fourth Amendment protection as those in the locked storage container or locker. However, a rigid and technologically agnostic reading of the Fourth Amendment fails to extend the same protections when a user voluntarily chooses to put their documents online, in the hands of a third party cloud computing service. This is similar to some courts' view that the Fourth Amendment does not offer protection to users of certain types of technology, for example cell phones that broadcast personal information such as location data.[133] Yet, such an approach ignores users' expectations of privacy in the devices, which store their personal data. A person's digital papers and effects may be accessible from virtually anywhere.

If a U.S. person keeps their documents in the cloud on a remote server abroad, then the privacy reality might change. A U.S. company holding a U.S. person's papers and effects on a U.S. server abroad still would be governed by the statutory restrictions of the ECPA.[134] However, in the areas where the

of user accounts in the cloud-computing domain lends credence to a reasonable expectation of privacy with digital papers and effects. *See* David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2209–11, 2218–19, 2224–27 (2009). Yet, the same author has analogized password-protected accounts to landlord tenant relationships because the landlord might have a limited right of entry but not unfettered access. *Id*. at 2236–38. This analogy is good as long as it is not dealing with a shared-dwelling. In that case, the locked container analogy would be more appropriate.

[132] If the account was shared then this might be more akin to a shared residence in which any of the parties living at a place could grant consent. *See* United States. v. Matlock, 415 U.S. 164, 169–70, 177 (1974) (holding a search that was conducted after another resident consented to search of the shared dwelling reasonable).

[133] Henderson, *supra* note 108 at 384–90.

[134] Google, among other companies, hosts their servers in various parts of the world. *See, e.g.,* Rich Miller, *Google Data Center FAQ*, DATA CENTER KNOWLEDGE (Mar. 27, 2008), http://www.datacenterknowledge.com/arc hives/2008/03/27/ google-data-center-faq/ (listing countries where Google has data centers that host servers, outside the U.S., such as in Germany, London, Netherlands, and Italy, to name a few); Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27 wiretap.html?pagewanted=all (listing Research Motion as a company that operates servers abroad); David Schellhase, Exec. Vice President & Gen. Counsel, Salesforce.com, Testimony before the U.S. House of Representatives: ECPA Reform and the Revolution in Cloud Computing 11 (Sep. 23, 2010), *available at*

ECPA is ambiguous, or in cases where a U.S. person is hosting their documents and effects with a company that does not operate from the U.S., then only constitutional protections triggered by a relevant search would apply.[135] If the country hosting the servers seizes the data for any reason, or if the company voluntarily discloses the data to another party, then the new party possessing the data conceivably could pass it on to U.S. law enforcement as a fourth party without ever triggering the Fourth Amendment or the ECPA.[136] From a tort and contractual standpoint, users might even explicitly acquiesce to or at least be on notice of such a possibility through their Terms of Service agreement.

VI. TERMS OF SERVICE: AN IMPLIED CONSENT?

The digital age has made consumer assent to contracts of adhesion-like terms, as found in the ubiquitous "Terms of Service" clauses (TOS).[137] Often, language in a TOS agreement merely disclaims liability for any damage to a user's computer or data and forbids unauthorized use or redistribution of intellectual property. However, Terms of Service are not relegated to limits on consumer behavior. Such terms also dictate the terms by which the entity will retain, control, and own a user's information. Thus, a user of free services is (often unbeknownst to them) effectively exchanging valuable personal information for the use of online services.[138]

The fact that the terms of a website agreement are not negotiated does not diminish the enforceability of such Terms of

http://judiciary.house.gov/hearings/pdf/Schellhase100923.pdf.

[135] The Fourth Amendment reasonableness requirement, but not the warrant requirement, applies to searches of U.S. persons conducted overseas "when the participation of United States agents in the investigation is so substantial that the action is a joint venture between the United States and foreign officials." United States v. Stokes, 710 F. Supp. 2d 689, 695–699 (N.D. Ill. 2009).

[136] According to the U.S. Court of Appeals for the Second Circuit, the "Fourth Amendment's requirement of reasonableness-and not the Warrant Clause-governs extraterritorial searches of U.S. citizens." This concept could therefore regulate a direct search or seizure of a server abroad by U.S. authorities. *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 159 (2d Cir. 2008).

[137] Cory S. Winter, *The Rap on Clickwrap: How Procedural Unconscionability is Threatening the E-Commerce Marketplace*, 18 WIDENER L.J. 249, 271–73 (2008).

[138] Nikki Tait & Tim Bradshaw, *EU to Probe Web User Profiling by Advertisers,* FIN. TIMES, Mar. 29, 2009, http://www.ft.com/cms/s/0/ef387d70-1ca2-11de-977c-00144feabdc0.html.

Service.[139] However, despite the popularity of broad TOS agreements for efficiency in the digital age, the non-dickered terms are not limitless and can be found unconscionable, particularly when there are no market alternatives to a service.[140] Yet, this is difficult to demonstrate in the search engine, email, and digital media services market, where there are many companies even though only a few giants dominate. Under the weak statutory protections of the Electronic Communications Privacy Act, the possibility of compelled subscriber permission provides law enforcement officers with a much easier avenue for retrieving digital rather than traditional evidence. The Fourth Amendment requirement of probable cause is a much higher threshold than the amorphous standards of using a subpoena, which does not always require court approval.[141]

A Title III order is required to obtain the contents of email in real time, which must be approved by the DOJ, granted by a federal judge, and renewed every 30 days.[142] For stored, unopened email a traditional search warrant is required.[143] However, only a subpoena with notice is necessary for the government to compel the disclosure of opened emails or stored files. An *ex parte* pen register order is necessary for the government to obtain real time subscriber data,[144] but a mere subpoena is sufficient for past non-content subscriber information.[145] While these requirements appear to provide sufficient safeguards for users, protections for non-real time data are trumped by consent, and users may unwittingly consent to such disclosure.

Google requires that its users adhere to its Terms of Service or not use its products and services.[146] Google defines content as "as data files, written text, computer software, music, audio files or other sounds, photographs, videos or other images" which users

---

139 *See* 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, 90-91, 116–17 (2008).

140 *Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 606 (E.D. Pa. 2007).*

141 William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 864 (2001).

142 18 U.S.C. § 2518 (2010).

143 *See id.* § 2703(a).

144 *Id.* § 3123.

145 *Id.* § 2703(d).

146 *Google Terms of Service*, GOOGLE, http://www.google.com/accounts/TOS (last visited Nov. 29, 2010).

may access or use.[147] The company then claims "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services."[148] However, the TOS agreement notes that certain services have different terms.

For example, users of Google's Gmail service accept terms which dictate that Google might retain messages, even from deleted accounts, in its offline backup servers.[149] Moreover, Google states that it will not release personal information nor content except in "limited circumstances" described in its privacy policy and when Google believes it is "required [to do so] by law."[150] Google's exceptions include when they:

> have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.[151]

Google's Gmail terms of service might appear reasonable for a free service even though the company's umbrella privacy policy sounds frighteningly vague and seems to embolden Google with the power to do anything with a user's data. Moreover, the company reserves the right to change the terms. Also, the fact that Google's Terms of Service allow for disclosure of private information to advertisers emboldens the notion that a Fourth Amendment right against unlawful searches and seizures might belong to Google, but not to a Google user.[152] Nevertheless,

---

147 *Id.*

148 *Id.*

149 *Google Privacy Policy*, *supra* note 128.

150 *Id.*

151 *Id.*

152 A recent example of Google's malleable view on privacy was demonstrated with the launch of its new "Buzz" service, which automatically linked frequently emailed Gmail contacts to each other's Twitter-like comment feeds and public photo albums. After much user uproar, the company was forced to convert these automatic connections to automatic suggestions. Jonathan Fildes, *Google Admits Buzz Social Network Testing Flaws*, BBC NEWS, Feb. 16, 2010, http://news.bbc.co.uk/2/hi/technology/8517613.stm; Hibah Yousuf, *Google Alters Buzz After Privacy Complaints*, CNNMONEY.COM (Feb. 15, 2010), http://money.cnn.com/2010/02/15/technology/Google_Buzz_privacy/index.htm?cnn=yes.

Google and other online service providers act as modern day document repositories for many people, harboring their papers and effects.[153] Despite this, it appears possible for a court to enforce a TOS agreement by which a user inadvertently contracts away their right to privacy.

The U.S. Court of Appeals for the Eleventh Circuit cited Federal Express' terms of service agreement as a main reason why a customer did not have a reasonable expectation of privacy in the contents of a package which FedEx allowed law enforcement authorities to search without a warrant. Another federal district court characterized promises regarding privacy rights in AOL's Terms of Service as merely "aspirational" because they did not "confer any rights or remedies" upon its users.[154] Thus, if a service provider is not bound by its own terms nor by the Fourth Amendment and users have no statutory protection then the government effectively can moot Fourth Amendment privacy protections through service provider cooperation.[155] However, if consent is defined by Fourth Amendment standards of expectations of privacy then users could remain protected regardless of the Terms of Service.

The number of cases in which courts have applied the Fourth Amendment to email remains limited. However, courts have applied the Fourth Amendment to a narrow set of circumstances. One prominent example is that of *United States v. Monroe*, in which the United States Court of Appeals for the Armed Forces held that a Fourth Amendment search did not occur when the government network administrator accessed a user's email, despite the government's role as the service provider for users of government computers.[156] This is due in part to the large disclaimer appearing on the screen when a user logs into a government computer.[157] However, the same court found that a

[153] As Google CEO Eric Schmidt notes, "[t]his is not a Google decision, this is a societal decision." Shane Richmond, *Google's Eric Schmidt: You Can Trust Us With Your Data*, TELEGRAPH, Jul. 1, 2010, http://www.telegraph.co.uk/technology/google/7864223/Googles-Eric-Schmidt-You-can-trust-us-with-your-data.html.

[154] Freedman v. Am. Online, Inc., 325 F. Supp. 2d 638, 640 (E.D. Va. 2004).

[155] A possible safeguard against this scenarios lies within the state actor doctrine discussed later in this paper. A user might be able to restrain Google's actions on a constitutional basis if they can prove that the government actively encouraged Google to violate the user's Fourth Amendment or other constitutional rights.

[156] United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000).

[157] *Id.* at 327.

user did have an objectively reasonable subjective expectation of privacy in a similar case, *United States v. Long*.[158]

In *Long*, the court's decision hinged on the fact that the network's Department of Defense computer disclaimer did nothing to erode a user's expectation of privacy in their email against law enforcement searches.[159] Instead, it merely implied that the computer usage reasonably was subjected to work-related non-criminal investigation monitoring.[160] Thus, it is possible, at least with a prominent enough notice and when the government is the service provider, for a user to agree to waive their Fourth Amendment protections in cyberspace. However, this is not automatically assumed, particularly when a notice fails to extinguish an objectively reasonable subjective expectation of privacy.

"Clickwrap" agreements are problematic in that they are often too ambiguous, too confusing, too obscure, or even too long for consumers to understand.[161] Privacy policies by their very nature sometimes make consumers believe private protections are being bestowed upon them.[162] The way in which Google products are marketed as a secure platform and the promotion of Google Docs as an alternative to desktop document processing exemplifies the likely expectations of consumers that their privacy is not being compromised.[163] Therefore, even though every user of these products and similar products must click through a TOS agreement, they might be expressing more of a willingness to use the product responsibly rather than an affirmative relinquishment of privacy. Even if a privacy policy puts a user on notice that their information might be analyzed, it is unlikely that users are on notice to the fact or accept the fact that their private information will receive less protection with

158 United States v. Long, 64 M.J. 57, 59 (C.A.A.F. 2006).

159 *Id.* at 63.

160 *Id.* at 65.

161 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, 20, 48 (2009).

162 JOSHUA GOMEZ, TRAVIS PINNICK, & ASHKAN SOLTANI, UNIV. OF CAL. BERKELEY, SCH. OF INFO., KNOWPRIVACY 11 (2009), *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

163 *Software-as-a-Service has Built-in Security Advantages*, GOOGLE APPS, http://www.google.com/apps/intl/en/business/infrastructure_security.html (last visited Nov. 29, 2010) (promoting the security of Google Apps, which includes products such as Google Docs, Google Calendar, and Gmail which are offered to the public for free).

regard to law enforcement. Moreover, it is sometimes difficult to ascertain with whom a user has an agreement and to whom a user gives up an expectation of privacy.[164]

VII. "DON'T BE EVIL" TO "CAN'T BE EVIL"[165]

A. The need to restrain third party service providers

The porous statutory protections afforded to online data are inadequate for protecting citizens' 21st century papers and effects. Similarly, current Fourth Amendment jurisprudence does not reflect the reasonable expectation of privacy maintained by those who trust their modern day papers and effects with third parties for commonplace electronic-age conveniences. Third parties increasingly have assumed capabilities previously held as a near monopoly by the state to conduct investigations and maintain private information about citizens.[166] However, electronic contracts of adhesion are limiting the private rights of an individual to protect their privacy in services so vital to daily life.

Current procedural safeguards are insufficient to prevent the government or even the third party service provider from trampling user privacy. Under normal circumstances, when records are subpoenaed, targeted parties may respond to a record request before such information is disclosed. Similarly, the Fourth Amendment generally requires that the government obtain a search warrant predicated on probable cause when compelling a private party to effectuate a search on its behalf. Thus, new challenges exist with regard to the NSA data

[164] Yale University recently contracted with Google to replace the school's email client with a custom version of Gmail. This creates a potentially more complicated third-party scenario depending on by whose terms of service the students must abide and how the email service is managed and data is stored. *See* David Tidmarsh, *Google to Run Yale E-mail*, YALE DAILY NEWS (Feb. 9, 2010), http://www.yaledailynews.com/news/university-news/2010/02/09/google-run-yale-e-mail/.

[165] The law should be strengthened to protect users merely at the mercy of Google's "Don't be Evil" motto and to ensure that Google cannot currently volunteer whatever data it wants to government or private entities.

[166] *See supra* Part I. The presence of a monopoly is a factor in determining whether or not a violation of a plaintiff's Fourteenth Amendment rights has occurred in situations where court access is limited. *See* Boddie v. Conn., 401 U.S. 371, 375 (1971). By analogy, a service provider's monopoly over a user's constitutional rights might be an effective bar to justice, violating their due process and equal protection rights.

collection activities and the prospects of a third party such as Google voluntarily handing over data the government.[167] Under current law, the most likely remedy for affected telecommunication or Internet service users are lawsuits against companies for breaching their own privacy policies. However, as discussed, such terms are often ambiguous and confer no definite rights upon a user.

In *United States v. Bach*, the U.S. Court of Appeals for the Eighth Circuit held that Yahoo!'s execution of a search warrant to retrieve a user's email was not unreasonable under the Fourth Amendment. Instead, the court noted that civilian searches at times might be more reasonable than law enforcement searches.[168] The *Bach* case and existing Fourth Amendment analogies make clear that Internet Service Providers (ISP) should be liable as a state actor when they execute a search warrant on behalf of law enforcement.[169] Absent an exception, a company should not disclose information in which an individual has an objectively reasonable subjective expectation of privacy unless a warrant has been issued or an exception has been met, and no such warrant shall issue without probable cause. However, it is unclear as to whether or not a private actor is restricted as a state actor when it is not executing a search warrant.

The U.S. Court of Appeals for the Fourth Circuit recently rejected the notion that a private email host should be restricted by the Fourth Amendment when it provides information to the government without a law enforcement request. In *Richardson*, a defendant sought unsuccessfully to suppress evidence against him that was initially detected and retrieved by AOL and eventually turned over to law enforcement.[170] He argued that AOL effectively was deputized by a federal law mandating that service providers report evidence of child pornography.[171] Therefore, AOL was required to comply with Fourth Amendment

---

[167] This is no longer a hypothetical in light of Google's recent decision to voluntarily provide information to the NSA in exchange for help in thwarting cyber attacks. *See* Ellen Nakashima, *Google to Enlist NSA to Help it Ward off Cyberattacks*, WASH. POST, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

[168] 310 F.3d 1063, 1067 (8th Cir. 2002).

[169] Francisco J. Navarro, *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 ALB. L.J. SCI. & TECH. 245, 263–265 (2003).

[170] *See* United States. v. Richardson, 607 F.3d 357, 360 (4th Cir. 2010).

[171] *Id.* at 367.

restrictions and utilize an automated search system to detect and extract illegal photos from his email.[172] The court rejected this concept and noted that the federal law did not require ISPs to conduct searches nor did it dictate the means by which they should execute them.[173] Thus, AOL's search was a voluntary private party action not subject to Fourth Amendment restrictions despite the fact that it later turned over information to the government in fulfillment of the statute's reporting requirements.[174]

In other cases, foreign private parties have hacked illegally into a computer, stole files, and turned them over to the government which used the evidence to initiate cases and prosecute individuals.[175] In these cases, the Fourth Amendment was not applied even though the hackers essentially acted as agents of law enforcement. Therefore, it is necessary to examine the state action doctrine to determine how it should apply to third parties, which lack personalities but boast more advanced technical knowhow and surveillance capabilities than law enforcement agencies.

B. The State Action Doctrine

Constitutional restraints on third parties only apply when state action is attached to third party actions.[176] Otherwise, users enjoy merely the statutory protections afforded to electronic data. The Fourth Amendment is a restriction on the government and does not explicitly bar a private party from searching or seizing a person's property. Moreover, Fourth Amendment jurisprudence has not always recognized restraints on private actors who illegally seize property from an individual and later turn it over to the government.[177] In the 1921 case of *Burdeau v. McDowell*, the U.S. Supreme Court held that such an action, while perhaps theft, did not trigger the Fourth Amendment even when the government refused to return the property.[178] However, this clear bright line private-public

[172] *Id* at 362–63.
[173] *Id.* at 366–67.
[174] *Id.*
[175] *See* Sagi Schwartzberg, *Hacking the Fourth: How the Gaps in the Law and Fourth Amendment Jurisprudence Leave the Right to Privacy at Risk*, 30 U. LA VERNE L. REV. 467, 484–86 (2009).
[176] Burdeau v. McDowell, 256 U.S. 465, 470–71, 475 (1921).
[177] *Id.* at 476.
[178] *Id.*

constitutional rights distinction eroded in 1974 with the U.S. Supreme Court case of *Jackson v. Metropolitan Edison Co.*[179]

In *Jackson*, the Court outlined a state action test to determine whether or not a private actor was acting as a state actor and thus could be restricted on constitutional grounds. From this precedent and subsequent case law, the Court has allowed constitutional limitations on private actors engaging in the exercise of "powers traditionally exclusively reserved to the State."[180] This initial exception allowing for constitutional restraints on private actors required both the traditional role and the exclusive role criteria to be met for the Court to accept a private actor as a *de facto* state actor. However, in today's dynamic world new technologies are replacing traditional functions, such as mail delivery, with expansive communication platforms not contemplated by traditional notions of exclusive state functions.

In *Jackson*, Metropolitan Edison was a private utility company which operated under a state-sanctioned license in a service area in the state of Pennsylvania.[181] The company was regulated under the Pennsylvania Public Utility Commission and vested with the authority to disconnect customers who did not pay.[182] Petitioner Catherine Jackson was a customer of Metropolitan Edison and her electricity was disconnected as a result of her failure to pay. She subsequently sued under the Civil Rights Act of 1871 on the grounds that Metropolitan Edison violated her Fourteenth Amendment due process rights by neglecting to give her sufficient notice, a hearing, and an opportunity to repay debts.[183] This lawsuit was based on the petitioner's insistence that Metropolitan Edison's actions constituted "state action" by virtue of its state-granted power to disconnect electricity for non-payment.[184] The state-granted power came from the company's operating agreement with the Commission.[185]

---

[179] Jackson v. Metro. Edison Co., 419 U.S. 345, 346, 350 (1974).

[180] *Id.* at 346, 352. Communication service providers have some functions that mimic traditional state functions such as postal delivery. Letters, photos, and documents are increasingly sent digitally via private actors rather than through the government run service. However, these functions, have not traditionally been exclusive to the state due to the existence of private parcel carriers such as UPS and FedEx or even the short-lived Pony Express.

[181] *Id.* at 346.

[182] *Id.*

[183] *Id.* at 347–48.

[184] *Id.* at 348–49.

[185] *Id.* at 348.

Writing for the Court, Justice William Rehnquist acknowledged that the distinction between a private action and a state action "frequently admits of no easy answer."[186] The due process clause of the Fourteenth Amendment places restraints on state actors' abilities to deprive the life, liberty, and property of an individual without due process of law. The Court stated that regulation alone does not make the actions of a private entity those of the state.[187] However, the opinion noted that the actions of a "governmentally protected monopoly" might more likely be considered state actions.[188] Justice Rehnquist wrote that the determination of state action did not rest on how state-like the actor was but instead on how closely the action was linked to the state.[189]

The Court reiterated that utility services, though perhaps a public function, never have been regarded as an exercise of a traditional state power, such as eminent domain.[190] The Court also made clear that monopoly status alone did not subject a private entity to the Fourteenth Amendment.[191] Therefore, a plaintiff suing a private actor for a constitutional violation would have to show more than evidence of heavy regulation and a partial monopoly to prove state action.[192] Additionally, the mere fact that a private actor exercises a behavior permitted under the law does not mean that a state action has occurred.[193] Ultimately, the Court asked, "[W]hether there is a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself."[194] Although state action was not found in *Jackson*, the Court set a precedent for plaintiffs to enforce their constitutional rights against private actors when the actions are so closely linked to those of the state.

C. Post-Jackson and Rethinking the State Action Doctrine

Since *Jackson*, the Court has expanded the doctrine to allow for lawsuits against private entities that do not fulfill the rigid

186 *Id.* at 346, 349–50.
187 *Id.* at 349–50.
188 *Id.* at 350–51.
189 *Id.* at 351.
190 *Id.* at 353.
191 *Id.* at 352.
192 *Id.* at 358.
193 *Id.* at 357.
194 *Id.* at 351.

public function test.[195] However, the most relevant application of the state action doctrine to the current public-private information sharing dilemma comes from the 2001 case, *Brentwood Academy v. Tennessee Secondary School Athletic Association*.[196] In *Brentwood*, the Court articulated the entwinement exception to the state action doctrine, holding that a private athletic organization which regulated the athletics programs of public and private schools in the state was constitutionally restricted in its actions against the plaintiff because of its "entwinement" with the state.[197]

The decision permitted the plaintiff to sue the athletics association for violating its First and Fourteenth Amendment rights, despite the fact that there was no legal requirement for schools to join the private entity. The Court cited the factors of overt and covert "encouragement" by the state as criteria when weighing the entwinement.[198] One of the determinative factors in *Brentwood* was the state's appointment of public officials to the board of the private entity.[199] Likewise, in the past decade communication providers have assigned employees to work onsite with the FBI to provide calling information for quick "sneak peek" inquiries.[200] Such an arrangement would appear to be evidence of an "entwinement" of the government with a private entity, at least for these specific types of searches.[201] If the concept of "entwinement" was applied more broadly to law enforcement methods then constitutional restrictions might govern private searches that effectively moot the need of the government to conduct a search. One instance would be if a

195 *See generally,* Henry C. Strickland, *The State Action Doctrine and the Rehnquist Court*, 18 HASTINGS CONST. L.Q. 587 (1991) (discussing the evolution of the State Action Doctrine since the Civil Rights Cases).

196 Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288 (2001).

197 *Id.* at 290–91.

198 *Id.* at 296 (holding a plaintiff is allowed to sue for a deprivation of property without due process of law claim when a private party acted at the encouragement of the state (citing Lugar v. Edmondson Oil Co., 457 US 922, 941 (1982))).

199 *Id. at* 291, 300.

200 OVERSIGHT AND REVIEW DIV., U.S. DEP'T OF JUSTICE OFFICE OF THE INSP'R GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 72 (Jan. 2010), *available at* http://www.justice.gov/oig/special/s1001r.pdf.

201 United States v. Attson, 900 F.2d 1427, 1429 (9th Cir. 1990) ("[T]he fourth amendment [sic] will only apply to governmental conduct that can reasonably be characterized as a 'search' or a 'seizure.'").

communication service provider such as Google, actively scanned private data for national security or criminal activity and then voluntary handed it over to the government.

A requirement necessary to apply the state action doctrine to the Fourth Amendment is that the information itself is actually protected. For example, the U.S. Court of Appeals for the Fifth Circuit refused to apply the state action doctrine when the information retrieved by a private actor acting on behalf of the FBI yielded insurance records that would be uncovered in the course of a normal audit.[202] Thus, this logic would apply to information possessed by a communication service provider in which users have no expectations of privacy. However, encrypted, password-protected data stored in a user's account likely would not be exposed during the course of a normal audit.

The U.S. Court of Appeals for the Ninth Circuit created a more easily satisfied two part test to determine whether a private party could be restrained under the Fourth Amendment, asking: "(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends."[203] If applied to the programs similar to the NSA Terrorist Surveillance Program, then collusive companies likely would be restricted as a state actor under this test. Additionally, the aforementioned volunteer hacker-vigilante scenarios conceivably could satisfy both prongs. Moreover, this test could safeguard adequately the rights of users of Google's Gmail and similar services and prevent them from becoming the backbone of a warrantless digital dragnet.

The state action doctrine is one possible avenue by which a person can enforce Fourth Amendment protections against third parties. The incredible surveillance powers possessed by communication providers exceed, replace, and complement the exclusive traditional powers of law enforcement entities. Therefore, this concept should be applied along with factors of entwinement and the Ninth Circuit's two prong test to determine whether or not private searches are state actions. The Fourth Amendment should restrain private searches by communication service providers when content-data is turned over to the government.

[202] United States v. Blocker, 104 F.3d 720, 727 (5th Cir. 1997).
[203] United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).

VIII. CONCLUSION

The Fourth Amendment must be applied to online communications to withstand and adapt to modern citizen behavior. The voluntary and secret disclosure of personal user information by third party telecommunication companies during the NSA Warrantless Surveillance incident demonstrates the potential privacy implications for citizens entrusting storage of their documents and effects to cloud computing companies. Hackers and private parties are a much greater threat to information security than the law enforcement regimes of democratically elected governments. However, as public-private partnerships increase out of necessity, constitutional protections should follow so that traditional rights are not evaded by way of outsourcing digital searches to volunteer private entities.

Left unrestricted, private entities might build erroneous character profiles improperly targeting innocent people due to trigger words used in online documents or web searches. The goal of Internet-era Fourth Amendment jurisprudence must not be to thwart investigations but rather to prevent fishing expeditions. It is important not to impede the efforts of law enforcement officials to solve crimes or prevent terrorist attacks. For this, a digital false friend exists. Law enforcement officials can still retrieve instant messages, emails, and shared documents from the person in whom the suspect confides or through the traditional warrant process. Undercover agents still can befriend suspects or laypersons online as a means of following and developing investigative leads. Moreover, online data still can be accessed without prior notice for national security investigations utilizing the FISA regime.

Citizens should enjoy a reasonable expectation of privacy from unwarranted government intrusion in their password-protected digital documents and effects repositories even in the cloud. Federal courts should distinguish the traditional third party doctrine analogy from the anonymous and automated role played by a communication service provider. Moreover, the state action doctrine should be expanded to permit constitutional rights to restrict searches conducted by communication service providers. This would prevent TOS agreements from trumping reasonable expectations of privacy. In the mean time, Congress should update the Electronic Communication Privacy Act to protect and recognize the digital documents and effects that have functionally replicated and replaced those mentioned in the text

of the Fourth Amendment.

The stakes of not adapting the protections of the Fourth Amendment to modern realities will increase as interconnected databases, cross-referencing technologies, and the prevalence of cloud computing expand. Future research should examine the potential national security problems posed if foreign companies purchase domestic communication service providers and obtain access to the vast amounts of data held by American corporations and regulated by American laws. Export controls placed on the sale of the data itself or even restrictions on server locations should be examined in light of the legal and privacy implications of recent hacking incidents and the privacy expectations analyzed in this research. Ultimately, legal regimes must continue to evolve with technology to reduce uncertainty and ambiguity for citizens and service providers alike.