NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
16 N.C. J.L. & TECH. ON. 202 (2015)

INSTASEARCH:
FIXING FOURTH AMENDMENT JURISPRUDENCE AS APPLIED TO INSTAGRAM AND OTHER CYBERSPACE DATA STORAGE PROVIDERS

Adam Charles Maas*

Under the Supreme Court's Fourth Amendment jurisprudence, the constitutional privacy protections that many Americans take for granted are non-existent in cyberspace because of the third-party doctrine, which was born decades before the popular adoption of cyberspace social networks and data storage services. When someone in America posts a picture on Instagram or updates a status on Facebook, regardless of the enabled privacy settings, the Supreme Court has determined that the Fourth Amendment does not protect that information from unreasonable search or seizure. However, Americans do in fact have reasonable expectations of privacy when using cyberspace services like Instagram, Facebook, Google Drive, and Dropbox. Therefore, the courts should adopt a new test for discerning reasonable expectations of privacy that better balances the public interest in effective law enforcement with the actual reasonable privacy expectations of individuals.

I. INTRODUCTION

Instagram[1] is one of the largest social networks in the world, and it is growing quickly.[2] As of December 2014, 300 million

* Adam Maas is a law student at the University of North Carolina School of Law. He thanks everyone on the staff of the N.C. Journal of Law and Technology, and specifically his editors, Kyle Evans, Kelly Morris, Nic Turza, and Matthew Spangler for all of their help and advice. He also thanks Professor Joseph Kennedy for helping him to understand the third-party doctrine and for being so generous with his time. Finally, Adam would like to thank all of the third parties in his life for maintaining his confidences when the Fourth Amendment does not require them to do so.

people actively used the service daily, which is 100 million more than did so less than one year prior.[3] Instagram's owner, Facebook,[4] has grown over ten years from a small social network that Mark Zuckerberg operated out of his dorm room to a global phenomenon with over one billion users.[5] As a result of the increased usage—by both law-abiding citizens and criminals—of these and other Internet services that store massive amounts of user data,[6] law enforcement has increasingly sought access to this user-generated information to facilitate criminal investigations. *United States v. Gatson*[7] provides a good example.

In *Gatson*, police officers created a fake Instagram account through which they requested[8] that Daniel Gatson—a suspect in a burglary investigation—grant them access to his pictures.[9] Gatson complied without knowing that police operated the account. Some of the pictures featured Gatson with cash and jewelry that police

---

[1] Instagram is a social networking site that allows users to share pictures. For more information, see INSTAGRAM, http://www.instagram.com (last visited Jan. 9, 2015).

[2] Alice Truong, *How Instagram Overtook Twitter in Users – In One Chart*, QUARTZ (Dec. 10, 2014), http://qz.com/309908/how-instagram-overtook-twitter-in-users-in-one-chart/.

[3] *Id.*

[4] Facebook bought Instagram in 2012. Kashmir Hill, *10 Reasons Why Facebook Bought Instagram*, FORBES (April 11, 2012, 5:00 PM), http://www.forbes.com/sites/kashmirhill/2012/04/11/ten-reasons-why-facebook-bought-instagram/.

[5] Jemima Kiss, *Facebook's 10th Birthday: From College Dorm to 1.23 Billion Users*, THE GUARDIAN (Feb. 4, 2014), http://www.theguardian.com/technology/2014/feb/04/facebook-10-years-mark-zuckerberg.

[6] Facebook alone has been reported to process over 500TB of data every day. Donna Tam, *Facebook Processes More Than 500 TB of Data Daily*, CNET (Aug. 22, 2012), http://www.cnet.com/news/facebook-processes-more-than-500-tb-of-data-daily/.

[7] No. 13-705, 2014 WL 7182275 (D.N.J. Dec. 16, 2014).

[8] Instagram users have the option either to allow any other users to view their photographs at all times or to require each user that wishes to view their photographs be specifically granted permission by them. *See How Do I Set My Photos and Videos to Private So That Only Approved Followers Can See Them?*, INSTAGRAM, https://help.instagram.com/448523408565555 (last visited Jan. 10, 2015).

[9] *See Gatson*, 2014 WL 7182275, at *22.

believed had been stolen in a string of burglaries.[10] The police did not have a warrant to create a false account and use it to gain access to Gatson's data, but the United States District Court for the District of New Jersey nonetheless allowed the evidence because it found that Gatson had consented[11] to the search when he accepted the police account's request to view his photos.[12]

As more of daily American life takes place on social media services like Instagram and Facebook and more data is stored online with services like Dropbox and Google Drive, the intersections between those services and criminal investigations will become more frequent and significant.[13] This Recent Development examines the relationship between the Fourth Amendment and government searches of data stored on these sites. The third-party doctrine is essential in cyberspace because some warrantless searches are necessary to facilitate successful law enforcement in that arena, but modifications are needed with respect to specific cyberspace platforms. This balancing would protect the reasonable privacy expectations of users while not unduly infringing upon effective law enforcement practices.

For services whose primary function is the sharing of data, a search should require a warrant if the search technique would constitute a breach of a website's Terms of Service ("TOS"). Such a search should require a warrant because a reasonable person would expect privacy in information obtainable only by breaking

---

[10] *Id*.

[11] The consent of the defendant will allow the warrant requirement to be waived. *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 218 ("It is equally well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent.").

[12] *Gatson*, 2014 WL 7182275, at *22.

[13] Dropbox is a cloud storage service that allows users to upload their files and then access them from any internet-enabled device. For more information about Dropbox, see DROPBOX, https://www.dropbox.com/ (last visited Feb. 18, 2015). Google Drive is a cloud storage service that allows users to upload their files and then access them from any internet-enabled device. For more information about Google Drive, see *Google Drive*, WEBOPEDIA, http://www.webopedia.com/TERM/G/google_drive.html (last visited Feb. 18, 2015).

the law or by violating established community norms.[14] In the case of services whose primary function is data storage, courts should maintain the third-party doctrine but create an evidentiary privilege between users and the service with a specific exception for evidence of criminal activity discovered through prescribed means.[15]

Part II discusses the evolution of Fourth Amendment jurisprudence and the third-party doctrine in the face of technological advancement. Part III explains both the weaknesses of the third-party doctrine and why, despite those weaknesses, the doctrine should not be discarded entirely. Part IV suggests a solution in order to reconcile the legitimate privacy concerns of citizens in cyberspace with the need for effective law enforcement in a world with technology well beyond the imaginations of the drafters of the Fourth Amendment.

II. FOURTH AMENDMENT LAW AND CYBERSPACE

Courts developed the third-party doctrine before the creation of the Internet. The doctrine was necessary to preserve the police practice of using informants or undercover agents to investigate suspects prior to having the probable cause necessary to justify a search or arrest warrant because informants and covert police officers are third parties to the information they observe.[16] Currently, the doctrine exempts any data stored in cyberspace from Fourth Amendment protection.[17] However, the Supreme Court has indicated in recent decisions in *Riley v. California*[18] and *United States v.*

---

[14] For more information regarding the possibility that breaking a website's Terms of Service agreement might be illegal see Kerr, *infra* note 107 and accompanying text.

[15] *See infra* Part IV.A. (describing in detail these authorized means).

[16] *See* On Lee v. United States, 343 U.S. 747, 756 (1952) ("Society can ill afford to throw away the evidence produced by the falling out, jealousies, and quarrels of those who live by outwitting the law. Certainly no one would foreclose the turning of state's evidence by denizens of the underworld. No good reason of public policy occurs to us why the Government should be deprived of the benefit of On Lee's admissions because he made them to a confidante of shady character.").

[17] The reader should remember that even though the Constitution does not provide protection, Congress could draft laws to do so. For information about such laws, see *infra* note 58 and accompanying text.

[18] 134 S. Ct. 2473 (2014).

Jones [19] that there may be some changes brewing in Fourth Amendment jurisprudence with respect to cyberspace.

A. *Origins of the Third-Party Doctrine*

The third-party doctrine refers to the Supreme Court's determination that people do not have a reasonable expectation of privacy in information that they disclose to others.[20] The doctrine originated with the Supreme Court's decision in *On Lee v. United States*.[21] In that case, the defendant was an opium dealer operating under the cover of his laundry business, and he made incriminating statements to a person who he believed was his friend.[22] Unfortunately for Lee, his friend had become a police informant and was wearing a wire.[23] The police did not obtain a warrant before sending in the informant to talk with Lee.[24] At trial, Lee made the argument that the fact that the wire was attached to a person as opposed to an object in his laundry did not mean that the government had not conducted an unwarranted search of his business when it sent the informant onto his private property.[25] The Court disagreed and ruled that because the person wearing the wire was a participant in the conversation with whom the defendant had voluntarily shared information, with or without the wire, no search subject to Fourth Amendment protection had occurred.[26] The Court also reasoned that the informant could have heard the same conversation had he been eavesdropping outside the window, which at the time was not considered a search because it was not a physical trespass.[27]

---

[19] 132 S. Ct. 945 (2012).

[20] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–29 (2006) (providing a general description of the third-party doctrine).

[21] 343 U.S. 747, 756 (1952); *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567 (2009) (beginning the discussion of the history of the third-party doctrine with *On Lee*).

[22] *On Lee*, 343 U.S. at 749.

[23] *Id.*

[24] *See id.* at 751.

[25] *See id.* at 751–52 (rejecting defendant's argument that stated a trespass had occurred and therefore there was an illegal search).

[26] *See id.* at 754 (rejecting the argument that eavesdropping on a conversation with the "connivance of one of the parties" constitutes an unreasonable search).

[27] *Id.*

The Court discarded the strict trespass standard in Fourth Amendment jurisprudence—whereby a physical trespass was a necessary condition for a search—in *Katz v. United States*.[28] Instead the Court declared "the Fourth Amendment protects people" and not "simply areas."[29] A now-famous concurrence written by Justice Harlan set up the modern test to determine if a search protected by the Fourth Amendment has occurred.[30] The first prong of the test requires that a person have a subjective expectation of privacy, and the second prong requires the expectation to be one that "society is prepared to recognize as 'reasonable.'"[31] The *Katz* test would have allowed future courts to determine that a person who shares information with a bank, a friend, or any other third party has a reasonable expectation—under certain circumstances defined by the Court—that the information will remain private as to everyone else other than that third party.[32] However, the Court rejected the extension of reasonable expectations of privacy to third parties in *United States v. White*[33] and held categorically that people do not have a reasonable expectation of privacy in information divulged to a third person.[34] The Court later extended the third-party doctrine to businesses, such as banks and phone companies, which hold client information.[35]

---

[28] 389 U.S. 347 (1967). Although *Katz* removed physical trespass as a necessary condition of Fourth Amendment searches, the Supreme Court in *Jones* revived the idea that physical trespass can be a sufficient condition for a search. According to the *Jones* majority, Katz augmented the trespass doctrine by removing the "strictness" of the test rather than abandoning the test entirely as some had believed. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012).

[29] *Katz*, 389 U.S. at 353.

[30] *See* Kerr, *supra* note 21, at 568.

[31] *Katz*, 389 U.S. at 361.

[32] Importantly, this may have foreclosed the use of undercover informants because if the court ruled that people have a reasonable expectation of privacy with respect to outsiders in conversations held in private, many undercover informants would be prevented from sharing information gained from such conversations at a trial.

[33] 401 U.S. 745 (1971).

[34] *Id*. at 749.

[35] *See generally* Couch v. United States, 409 U.S. 322 (1973) (finding that records held by a defendant's accountant were not subject to a reasonable expectation of privacy and therefore not protected by the Fourth Amendment);

For Fourth Amendment purposes, Instagram is like a phone company or a bank. When a user posts a picture on his Instagram account, other users are able to view it on Instagram, and the employees of Instagram can also see it even if the account is entirely private as to other users.[36] Therefore, the poster has disclosed the photo to a third party in the same way that he would disclose dialed phone numbers to a phone company or account numbers to a bank. Consequently, the Internet seemingly offers users no protection from warrantless searches because most information uploaded in cyberspace is accessible by the operators of whichever platform is used to store the data.[37] There are, however, reasons to believe that the Supreme Court is on the verge of making some changes to its Fourth Amendment jurisprudence and might even be ready to abandon the third-party doctrine altogether.[38]

B. *Wavering on the Third-Party Doctrine in* Riley v. California *and* United States v. Jones

Recent Supreme Court opinions in *Riley v. California*[39] and *United States v. Jones*[40] have created doubt that the third-party

---

see also United States v Miller, 425 U.S. 435 (1976) (finding bank account records to be unprotected by the Fourth Amendment); Smith v. Maryland, 442 U.S. 735 (1979) (finding that data—recorded by pen registers—held by phone companies regarding the numbers dialed from a particular phone was not subject to Fourth Amendment protection).

[36] *See Privacy Policy*, INSTAGRAM, https://instagram.com/about/legal/privacy/#section1 (last visited Feb. 28, 2015) (explaining that Instagram collects and monitors data posted by users to the service).

[37] For an exception to this rule, see *infra* note 104 and accompanying text describing services that do not observe or hold user data.

[38] For more information on the abandonment of the third-party doctrine with respect to data stored in cyberspace (such as Instagram photos), see Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (Sept. 11, 2014), http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud ("*Riley* suggests that the Court is ready to find that cloud-based data receive Fourth Amendment protection, and that cloud users do not waive a reasonable expectation of privacy in every file they save simply because storage is moving to the cloud."). *But see* Kerr, *supra* note 21 (arguing that the third party doctrine should be kept because it is simple and predictable in its application as well as being necessary to find modern crime).

[39] 134 S. Ct. 2473 (2014).

doctrine will continue to operate as it has in the past, especially where cyberspace data is concerned. In *Jones*, the police suspected that the defendant was trafficking in narcotics and installed, without a warrant,[41] a very small GPS tracking device on his car while it was parked in a public parking lot.[42] Police then observed and recorded the movements of the defendant's vehicle for four weeks using the GPS tracker they had installed on the car.[43] In response to a pretrial motion, the United States District Court for the District of Columbia ruled that the police did not need a warrant to place the GPS tracker on the car and monitor its travels because no search had occurred excepting the period when the car was parked inside of a garage.[44] The Supreme Court previously held that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and the District Court accordingly supported its decision with that reasoning.[45] The majority opinion in *Jones* did not reach the issue of reasonable privacy expectations,[46] but in a concurring opinion, Justice Sotomayor raised questions regarding the reasonableness of the third-party doctrine in the modern world writing that:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the

---

[40] 132 S. Ct. 945 (2012).

[41] The police had obtained a warrant to use the device in the District of Columbia for ten days, but they installed the device on the eleventh day while the car was parked in Maryland. *Id*. at 948.

[42] *Id*. at 948.

[43] *Id*.

[44] *Id*.

[45] *Id.* (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

[46] The majority in *Jones* avoided the third-party issue by finding in favor of the defendant because the placing of the tracking device on the defendant's car was a trespass and therefore required a warrant. *Jones*, 132 U.S. at 950 ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas it enumerates. *Katz* did not repudiate that understanding.").

> phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[47]

Although the majority in *Jones* did not rule on the basis of reasonable privacy expectations, neither did it dismiss the idea that a persistent four-week-long observation of an automobile driving around could violate the driver's reasonable expectations of privacy.[48] However, under the third-party doctrine, the Court should hold that any driving activity observable by others in public has been willfully disclosed to third parties and is therefore not subject to a reasonable privacy expectation.[49]

In *Riley*, the police stopped the defendant for a traffic violation and arrested him on weapons charges after conducting an inventory search of his impounded car.[50] After the arrest, the police

---

[47] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

[48] *Id*. at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

[49] The flaw in this reasoning is that unlike government surveillance, no one person on the street would observe every movement of a car for days or weeks at a time. Additionally, the people in public—who individually may have observed a particular car for only a few seconds—would never spontaneously gather together for the purpose of compiling an account of any one car's travels over a long period of time. Therefore, it is often reasonable for someone driving in public to expect that his journey in aggregate will remain private.

[50] *Riley v. California*, 134 S. Ct. 2473, 2480 (2014). An inventory search is a search done for the purpose of collecting and securing property in a car that has been seized. It is not an investigative search, but the Court has ruled generally that evidence of a crime found during such a search does not require probable cause or a warrant to be used at trial. *See e.g.*, South Dakota v. Opperman, 428

conducted a warrantless search of his person incident to the arrest and discovered a smartphone.[51] The police searched the smartphone and found incriminating photographic evidence tying Riley to a shooting that had occurred a few weeks prior.[52] The Supreme Court ruled that police must obtain a warrant under these circumstances to search a phone incident to an arrest.[53]

Considering how many people now use smartphones in their daily lives, *Riley* is an important decision.[54] The Court reasoned that if all of the information that could be stored in a mobile phone would receive robust privacy protections if it were stored in the home—where it would have been stored prior to the invention of smartphones—the Fourth Amendment protections should not be reduced simply because that information is now located all in one place on a smartphone.[55] If anything, that fact supports providing *more* privacy protection because the information accessible through a smartphone is greater than that which any person can store in one place in hard copy, and it is "qualitatively different" from information typically stored in hard copy.[56] A search of a

---

U.S. 364 (1976) ("The decisions of [the Supreme Court of the United States] point unmistakably to the conclusion reached by both federal and state courts that inventories pursuant to standard police procedures are reasonable.").

[51] *Riley*, 134 S. Ct. at 2480.

[52] *Id*. at 2481.

[53] *Id*. at 2495.

[54] Around 160 million Americans own a smartphone. *Smartphone Penetration Now at Two-Thirds of the US Mobile Market*, MARKETINGCHARTS (Mar. 10, 2014), http://www.marketingcharts.com/online/smartphone-penetration-now-at-two-thirds-of-the-us-mobile-market-41248/; *see also* Ben Dickinson, *How the Internet, Social Media, and Smartphones Are Dividing And Conquering Our Consciousness*, ELLE (Oct. 11, 2013), http://www.elle.com/life-love/society-career/social-media-smartphones-influence-on-our-lives (describing the effects of pervasive use, particularly among young people, of modern technology and noting particularly that "[n]early 20 percent of smartphone owners ages 18 to 34 report having used their phones while having sex").

[55] *Riley*, 134 S. Ct. at 2495 ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

[56] *Id*. at 2490 ("Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An internet search and browsing history, for example, can be found on

person's phone can reveal his tastes, interests, medical problems, travel habits, and a host of other personal information that before would never have been found in one place in a person's house or especially on his person.

The questions raised, both explicitly and implicitly, by the Court's analysis in *Riley* have implications for cyberspace data storage beyond mobile phones, which are only one method of accessing cyberspace. If accessing a suspect's phone without a warrant and thereby exposing much of his private life to government scrutiny is a grave violation of the Fourth Amendment, then going directly to the holders of the information accessible through the mobile phone—such as e-mail services or cloud storage providers—is as well. Concurring in *Riley*, Justice Alito recognized that the Fourth Amendment raised these issues, but rather than suggesting a re-assessment of the manner in which the *Katz* test had been applied to cyberspace, Justice Alito preferred that the issue be left to the legislature.[57]

Regardless of the solution proposed, at least some Supreme Court justices have recognized potential problems created by the collision of the third-party doctrine with advancing technology and the ever-increasing prevalence of that technology in the lives of Americans. Despite these difficulties, however, it would be unwise to throw out the doctrine entirely.

III. THE THIRD-PARTY DOCTRINE IS PROBLEMATIC BUT NECESSARY IN CYBERSPACE

Under a strict application of the third-party doctrine as it currently exists, the search of the defendant's Instagram account in *Gatson* would have been constitutional without a search warrant.

---

an Internet-enabled phone could reveal an individual's private interests or concerns.").

[57] *See id*. at 2497 (Alito, J., concurring) ("In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.").

Even if the police had not obtained consent from the defendant for the search, they could have—without showing probable cause—obtained a court order requiring Instagram to grant access to Gatson's account and avoided any Fourth Amendment violations because those pictures had been shared with Instagram itself, which is a third party.[58] This result is counter-factual with respect to people's actual reasonable privacy expectations.

A. *Flaws in the Third-Party Doctrine as Applied to Cyberspace*

The third-party doctrine is flawed because it does not reflect reasonable privacy expectations in cyberspace. As discussed above, the defendant's data in *Gatson* would not have been entitled to constitutional protection even if the defendant had not "consented" to sharing his photos with the police. Justice Sotomayor's concurrence in *Jones* questions the logic behind this and similar applications of the third-party doctrine.[59] People do in fact have reasonable expectations of privacy in information that is known to others. The average American would probably be surprised if he found out that when he sent an e-mail to his girlfriend or posted a photograph to his Instagram account—access to which he had deliberately restricted by allowing only people whom he had

[58] The police would have to comply with current federal law protecting online data, but those protections are less than would be provided by the Fourth Amendment. Under current U.S. law, the government may access data stored for more than 180 days if it can offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703. This is a lower standard than the Fourth Amendment probable cause standard requires to justify searches. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 37 (1968) (Douglas, J., dissenting) (objecting to the use of reasonable suspicion to justify cursory searches because that standard does not provide as much protection from unreasonable searches and seizures as does probable cause). Like any law, Congress can rescind these protections at its whim. The experience of 9/11 has shown that Congress, when frightened, can move remarkably quickly in restricting the liberties and privacy rights of its citizens.

[59] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

specifically approved to see his photos—that he had forfeited reasonable expectations of privacy in that e-mail or that picture.[60]

The third-party doctrine is flawed also because it relies on expectations of privacy, and those expectations may not be constant. For example, in the wake of Edward Snowden's revelations regarding National Security Administration ("NSA") surveillance programs and the reporting of Glenn Greenwald in *The Guardian*, Americans arguably no longer have a reasonable expectation of privacy in their online conduct because they have been warned that the NSA is watching.[61] By this logic, any American government that wants to infringe on privacy rights[62] has only to inform the public that it no longer has any privacy in cyberspace, and the public's reasonable expectations will vanish along with its rights.[63]

---

[60] *See* John Horrigan, *Use of Cloud Computing Applications and Services*, PEW RESEARCH (Sept. 12, 2008), http://www.pewinternet.org/2008/09/12/use-of-cloud-computing-applications-and-services/ (reporting on a poll finding that 90% of Internet users would be very concerned if their online files were sold to other companies and over 60% would be either very concerned or somewhat concerned if their files were given to law enforcement agencies upon request).

[61] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order?guni=Article:in%20body%20link (reporting on a leaked secret order from the FISA court authorizing the unlimited collection of call metadata from Verizon Wireless customers over a three-month period); *see also* Glenn Greenwald, Laura Poitras & Ewen MacAskill, *Edward Snowden: US Surveillance 'Not Something I'm Willing to Live Under'*, THE GUARDIAN (July 8, 2013, 2:22 PM), http://www.theguardian.com/world/2013/jul/08/edward-snowden-surveillance-excess-interview (discussing the revelations of Edward Snowden in an interview with Glenn Greenwald, which include the existence of a program called "Boundless Informant").

[62] The motives behind such infringement need not be nefarious in order to be dangerous:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Olmstead v. U.S., 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).

[63] *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., concurring) ("More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define

The Court's response to this argument has been to suggest that in such a circumstance, a "normative inquiry would be proper" to ascertain reasonable privacy expectations.[64] However, it is unclear which fact patterns would trigger a normative inquiry.[65] Also unclear is how such an inquiry would proceed and why privacy expectations are not always evaluated using such an inquiry.[66]

The third-party doctrine is vulnerable to criticism for reasons beyond its counter-factual premise. In the case of Instagram users, if the doctrine accurately reflects privacy expectations, those expectations are arbitrary and illogical. Suppose that Charles has a collection of photographs that he has taken, and he has printed them on glossy photography paper. If Charles keeps the photographs in his desk drawer in his room, the police must obtain a search warrant to search his desk and to view the pictures because the pictures are in his home. Charles has a reasonable expectation of privacy in items not revealed to the public but kept in his home.[67] Even if Charles allows some of his family and friends to see his pictures, the police would not be allowed to then break into his home without a warrant to get a look at the photographs for themselves.[68] However, despite Charles' efforts, a nosy member of his family would be able to discover the pictures if that person looked in his desk drawer.

---

the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications.").

[64] *Id*. at 740 n.5.

[65] The Court held that such an inquiry would be triggered when an individual's subjective expectations had been shaped by "influences alien to well-recognized Fourth Amendment freedoms." *Id*. That reasoning simply begs the question "which expectations are alien to the Fourth Amendment?," which puts the analysis right back where it started.

[66] *See Smith*, 442 U.S. at 750 (Marshall, J., concurring) ("The Court is willing to concede only that, in some circumstances, a further 'normative inquiry would be proper.' No meaningful effort is made to explain what those circumstances might be, or why this case is not among them.").

[67] *See* Katz v. United States, 389 U.S. 347, 351 (1967).

[68] The police would be allowed to ask the friends or family members what they had seen without first obtaining a warrant because the friends and family are third parties.

On the contrary, if Charles uploads his photos to Instagram with the maximum privacy settings enabled rather than printing and placing them in his desk drawer, he has now forfeited Fourth Amendment protection of those pictures because the police can view them without being required to obtain a warrant.[69] In reality, Charles has not relinquished his reasonable expectations of privacy in his photographs. If anything, he has more reason to expect his pictures will remain private when they are on Instagram than he does if he has them in his desk. A nosy family member or friend can access Charles' pictures without his consent by opening his desk drawer. However, viewing them on Instagram without consent would require hacking into Charles' account or correctly guessing his password assuming he has his privacy settings enabled.[70] In this case, the justification of the third-party doctrine and its purported reasonable expectations are either at odds with Charles' *actual* reasonable expectations of privacy, or Charles' privacy expectations are arbitrarily derived.

These questionable results required by the application of the third-party doctrine to cyberspace have caused some commentators to call for the end of the third-party doctrine and consequently full Fourth Amendment protection for data stored online. For many of the reasons discussed above, Ryan Watzel argues that the Supreme Court's decision in *Riley*—and its supporting logic—is a signal that the third-party doctrine does not have long to live.[71]

---

[69] Statutes may also provide privacy protections. *See supra* note 58 and accompanying text.

[70] Instagram can view the pictures that Charles has posted, but Charles has a legal agreement with them that those pictures will not be distributed to those people he does not authorize. *See Thank You, and We're Listening*, INSTAGRAM, http://blog.instagram.com/post/38252135408/thank-you-and-were-listening (last visited Jan. 24, 2015).

[71] *See* Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (Sept. 11, 2014), http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud ("*Riley* suggests that the Court is ready to find that cloud-based data receive Fourth Amendment protection, and that cloud users do not waive a reasonable expectation of privacy in every file they save simply because storage is moving to the cloud.").

B. *The Necessity of the Third-Party Doctrine*

Despite the issues with the third-party doctrine, there are good reasons not to abandon it entirely because the doctrine is functionally necessary and doctrinally defensible. The respected computer law expert Professor Orin Kerr makes this argument in his defense of the third-party doctrine.[72] Kerr offers a general defense of the third-party doctrine, and this section examines and modifies that defense specifically to cyberspace data storage. Kerr defends the third-party doctrine on two fronts. First, despite its logical inconsistencies, the doctrine provides clarity and predictability to law enforcement. Second, the world is becoming too dangerous with the advance of technology to eliminate the third-party doctrine.

The third-party doctrine provides clarity and simplicity to the law because it judges whether or not a Fourth Amendment search has occurred based on the location of the item to be searched.[73] Kerr illustrates this point using a letter,[74] but his example applies to e-mail as well.[75]

If Harry sends an e-mail to Sally, Harry has a reasonable expectation of privacy in that e-mail while it is in his possession and while it is in transit to Sally.[76] If an agent of the government opens the e-mail before it arrives in Sally's inbox, that examination will be classified as a search, and the message will be subject to Fourth Amendment protections.[77] Once the e-mail arrives in Sally's inbox, it becomes the property of Sally, and then *Sally's* privacy expectations govern the search rules regarding the message.[78] This is also true of every other e-mail in Sally's inbox.[79]

---

[72] Kerr, *supra* note 21.

[73] *See id.* at 580.

[74] *Id*. at 582.

[75] *See id*. Note that there are important differences between e-mail and traditional letters with respect to transmission that are not directly relevant to this discussion.

[76] *Id*.

[77] Similarly, the police would not be permitted to board a mail truck and conduct warrantless searches on every letter in the truck that had yet to be delivered.

[78] *See* Kerr, *supra* note 21, at 582.

If the police were to gain Sally's consent to search her computer and discovered the e-mail from Harry, that e-mail message would be searchable because Sally consented to the search, and the third-party doctrine nullifies any privacy interest that Harry had in the e-mail when he disclosed the contents to Sally, a third party.[80]

Examination of this scenario in the absence of the third-party doctrine reveals the importance of the doctrine to efficient and effective law enforcement. Harry sends an e-mail to Sally just as before, and just as before, Sally consents to a police search of her computer. The police discover the message from Harry, and they open the e-mail and find pornographic images of children. With or without the third-party doctrine, Sally is in a great deal of trouble because she consented to the search. However, in the absence of the third-party doctrine, Harry can now claim Fourth Amendment protection for his e-mail and ask the court to exclude the e-mail evidence because he has a reasonable expectation of privacy in his communications with his friends, and the police search was warrantless. Even though Sally consented to a search of her computer, Harry did not consent to a search of his e-mail message. The precise relationship between Harry and Sally would further complicate the analysis. If Harry and Sally are close friends or lovers, then Harry's expectations of privacy in information divulged to Sally are probably reasonable, and the evidence must be excluded. However, if the two recently met or only have an arms-length relationship, then perhaps Harry's expectations are not reasonable, and no warrant is needed. As can be seen from this example, the exclusionary rule—the enforcement mechanism of the Fourth Amendment—would require police conducting a search of Sally's computer to search only the files that had originated with Sally at least until a full investigation of her relationship with Harry could be conducted.[81] The consequences of any mistake

---

[79] *Id*.

[80] *Id*.

[81] *See* Weeks v. U.S., 232 U.S. 383, 398 (1914) (holding that letters seized in violation of the defendant's Constitutional rights should have been returned to him and not used as evidence against him at trial); *see also* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (incorporating the exclusionary rule to the states).

would be the loss of potentially critical evidence of criminal activity.[82]

According to Kerr, without the third-party doctrine, "information should retain a history."[83] The police would need to determine the history of every piece of information to be searched before conducting the search in order to determine whose expectations of privacy applied to each particular piece of information. Even after making that determination, the work of figuring out whether or not that person's privacy expectations were reasonable would still be left to do.

The pace of technological change creates an additional problem. One of the most controversial third-party doctrine cases was the pen register case, *Smith v. Maryland*.[84] This case allowed the police to obtain metadata[85] about phone calls—specifically the numbers called from a particular phone—without a warrant.[86] People might have considered the numbers that they were dialing to be a private matter in the 1970s when the Supreme Court decided the case.[87] However, in modern times, anyone a person calls who has a mobile phone—or caller ID on a landline phone—knows from which phone number the call is coming before he answers.[88] This advance in technology has changed the expectations of privacy that people reasonably hold in phone numbers, especially given that

---

[82] *See Weeks*, 232 U.S. at 398.

[83] Kerr, *supra* note 21, at 582.

[84] 442 U.S. 735 (1979).

[85] Metadata is information regarding an item, such as a phone call or an electronic file, that is about the item but does not deal directly with the content of the item. Metadata about a phone call would include the number dialed, the duration of the call, and the location from which the call was placed. For more information about metadata, see *Metadata*, TECHTERMS.COM, http://www.techterms.com/definition/metadata (last visited Jan. 14, 2015).

[86] *See Smith*, 442 U.S. at 745–46.

[87] The dissenting justices certainly did. *Id*. at 748 (Stewart, J., dissenting) ("Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called.").

[88] The exception would be numbers that are deliberately blocked from identification programs and generally appear as "unknown."

telemarketers are constantly calling people who have never divulged their phone number to the entities making those calls.[89] Now the courts not only must define privacy expectations for various technologies,[90] but they must also re-evaluate those decisions every decade or so to determine whether or not reasonable expectations have changed.

The third-party doctrine avoids all of these decisions and complications because a third party is a third party no matter which technology a suspect uses to transmit information to that entity. Some scholars have suggested that one way to cure the ambiguity inherent in a unilateral repeal of the third-party doctrine would be to simply require a warrant obtained after a showing of probable cause for nearly every search that occurs in cyberspace per the Fourth Amendment's warrant clause.[91] The weakness of this approach is that the technology available to criminals to carry out and conceal their crimes is now more sophisticated, and the potential consequences of those crimes are much greater than they were when the Fourth Amendment was ratified in the 18th century.

Modern criminals are capable of much more damaging activities than a bank robbery or even a series of murders.[92] They

---

[89] Americans must submit their phone numbers to a list to get telemarketers to leave them alone. *See National Do Not Call Registry*, FED. TRADE COMM'N, https://www.donotcall.gov/confirm/conf.aspx (last visited Jan. 14, 2015) (providing a means to verify if you have properly registered your phone number for the do not call list, which in theory prevents telemarketers from making unsolicited calls to that number).

[90] Examples of such technology include e-mail, cloud storage, cybershopping purchasing history, browsing history, financial transactions using online services such as PayPal, etc.

[91] *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1302–03 (2004) (arguing that standards, such as mere reasonableness, justifying searches that are lower than the probable cause threshold have been inadequate protections against unreasonable searches and seizures).

[92] *See* Andrew Roman, *September 11, 2001—As It Happened—The South Tower Attack*, YOUTUBE (Aug. 30, 2007), https://www.youtube.com/watch?v=1lKZqqSI9-s (showing a series of newscasts at the time of the attack on Tower 2 of the World Trade Center); *see also Nerve Gas Attack on Tokyo Subway*, HISTORY, http://www.history.com/this-day-in-history/nerve-gas-attack-on-tokyo-subway (last visited

engage in sophisticated organized crime.[93] In order to implement their designs, they use technology that is much more effective and difficult to combat than were single-shot muskets and couriers on horseback.[94] Privacy and security are on opposite ends of a sliding scale, and the following example illustrates that a total abandonment of the third-party doctrine might tip the balance too far in one direction and expose the fact that there is such a thing as too much privacy.

Suppose Sven is using Instagram[95] to run a criminal syndicate that specializes in contract killings. His syndicate has a privacy-protected Instagram account and gives access only to prospective contractors and clients. When a client wants a job done, Sven posts a picture of the target on the syndicate's account. He then sends a text message[96] to one of his contractors with a code indicating which picture is the target and a password to the Instagram account. After the contractor completes the job, Sven deletes the picture. He might also deactivate the account as an extra precaution. In this scenario, the police are entirely reliant on the cooperation of Instagram to conduct an investigation because a magistrate is highly unlikely to find that the government has probable cause to search the account without any voluntary cooperation on the part of Sven's associates. Police might have confidence that Sven is a criminal mastermind and have corresponding suspicions of his involvement with professional killings, but such a general suspicion is insufficient to obtain a

---

Feb. 13, 2015) (describing the sarin gas attack on the Tokyo subway system in 1995 by members of the religious cult, Aum Shinrikyo).

[93] *See* Chris Matthews, *Fortune 5: The Biggest Organized Crime Groups in the World*, FORBES (Sept. 14, 2014, 6:00 AM), http://fortune.com/2014/09/14/biggest-organized-crime-groups-in-the-world/ (detailing the five largest organized criminal operations in the world).

[94] *See* Robert Lemos, *Report: Cybercrime Costs US $12.7M a Year*, ARS TECHNICA (Oct. 17, 2014, 11:05 AM), http://arstechnica.com/security/2014/10/report-cybercrime-costs-us-12-7m-a-year/ (reporting on the costs, primarily to energy and financial companies, of cybercrime attacks).

[95] An analogous example can be created with any data storage platform (Facebook, Dropbox, Google Drive, etc.).

[96] Text messages are conveyed through third parties such as telecommunications companies.

warrant. By conducting operations exclusively through third parties in which Sven has a reasonable expectation of privacy—perhaps all syndicate members swore a blood oath to remain loyal—he can conduct his business with near-impunity.[97] The consequences are even graver in the example of terrorist activities. For these reasons, the third-party doctrine is probably necessary for the safety of modern society.[98]

IV. BALANCING THE THIRD-PARTY DOCTRINE WITH REASONABLE PRIVACY EXPECTATIONS IN CYBERSPACE

While the third-party doctrine has problems as it relates to the actual privacy expectations of Americans in their daily lives, there are good reasons to believe that eliminating the doctrine entirely would make law enforcement in the modern world increasingly difficult or almost impossible in some cases. Therefore, there must be a compromise, as always, between security and privacy. In cyberspace, this compromise would be best made on a

[97] It is likely that Instagram, and other platforms that rely on public relations to make millions of dollars a year, would not long allow Sven's activities to go on and would cooperate voluntarily with law enforcement. Google currently does so with respect to child pornography detected in Gmail. *See* Hayley Tsukayama, *How Closely is Google Really Reading Your E-mail?*, WASH POST (Aug. 4, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/04/how-closely-is-google-really-reading-your-e-mail/.

[98] There is a movement in the wake of Edward Snowden's NSA spying revelations to increasingly use encrypted programs to transmit data. *See* David Kravets, *Citing Encryption, FBI Lobbying To Keep Phone Metadata Spying Powers*, ARS TECHNICA (Feb. 25, 2015), http://arstechnica.com/tech-policy/2015/02/citing-encryption-fbi-lobbying-to-keep-phone-metadata-spying-powers/ (discussing efforts by the FBI and some lawmakers to maintain section 215 of the Patriot Act that allows warrantless bulk metadata collection between overseas and domestic callers in order to compensate for the increasing use of encryption in communications). There are also services—like Mark Cuban's Cyber Dust—that never store customer data on any server in addition to using data encryption to protect messages in transit. CYBER DUST, https://www.cyberdust.com/ (last visited Feb. 25, 2015). These technologies and services may make the third-party doctrine a nullity in cyberspace because even if the government can compel a third party to give up information on a user without probable cause or a warrant, if the third party either does not have any information or cannot access the information because it is encrypted, warrants are immaterial.

platform-by-platform basis. Currently, the law treats as the same Dropbox, Google Drive, Instagram, Facebook, and all other cyberspace locations because they are third parties with which users have consented to share information. Therefore, users have waived their reasonable expectations of privacy in data stored with those services. In order to balance the necessity of the third-party doctrine in some contexts with people's actual reasonable privacy expectations, the doctrine should be maintained and modified for some cyberspace platforms but eliminated with respect to others.

Services that store data in cyberspace should be divided into two categories.[99] The first category is sites whose primary purpose is data storage and that involve little or no social interaction or sharing of content between users. Examples in this category include Dropbox, SpiderOak, and Google Drive.[100] The second category is services whose primary purpose is to share information with others. Examples in this category include Instagram, Twitter, and Facebook. The third-party doctrine should remain fully applicable to the first category of services because users rarely, if ever, share information on those services with strangers, and therefore, eliminating the third-party doctrine would make criminal investigations involving these services difficult, if not impossible, to conduct. However, the third-party doctrine should no longer apply to services in the second category because law enforcement already has opportunities to gain information without a warrant—as it did in *Gatson*—and therefore a more accurate reflection of the reasonable privacy expectations of citizens using those services would not unduly jeopardize effective law enforcement. In the

[99] This division is based on the premise that intellectual consistency is less important in this area than is striking a pragmatic balance between the interests of privacy and effective law enforcement. Based on the concurrence of Justice Sotomayor in *Jones*, it can be well argued that the third-party doctrine should not apply in cyberspace anymore, particularly in the case of pure data storage services like Dropbox. Justice Sotomayor's concurrence is discussed in greater detail Part II (B) *supra*.

[100] In each of these examples, there is some sharing possible, but that is not the primary purpose of the services. Many people use their Google Drive accounts to store information without sharing that information with anyone. On the contrary, relatively few people use Facebook, Instagram, or Twitter without sharing information.

absence of the third-party doctrine, the government could no longer compel a service such as Facebook to allow access to a user's account without courts classifying such access as a search under the Fourth Amendment and requiring a warrant supported by probable cause. With respect to this second category, courts should evaluate the reasonable privacy expectations of users of a particular service using the service's TOS agreement in order to judge whether or not police have conducted a search for Fourth Amendment purposes.

A. *An Evidentiary Privilege Between Users and Service Providers*

The privacy expectations of users of services like Dropbox that customers primarily use for data storage should not be entirely disregarded. The more difficult the task is for the government to obtain information, the more reasonable the privacy expectations of the users become. Therefore, a paradox of the third-party doctrine is that the more reasonable the privacy expectations of users are the more dangerous is full acknowledgement of those expectations. Holding the third-party doctrine inapplicable to such services would make criminal investigations too difficult.[101] As a compromise, the courts should create an evidentiary privilege between users and cyberspace data storage services like Dropbox whose primary function is data storage. Jacob Small has described such a privilege in detail.[102] The privilege would protect information so long as:

> (1) a sufficient level of privacy has been maintained, (2) the documents have not been shared with a party outside of the privileged relationship, (3) the contract establishing the relationship is consistent with a subjective expectation that the documents will be private, and (4) the user, not the provider, is asserting the privilege.[103]

---

[101] These difficulties are discussed in Part III (B) *supra*.

[102] *See* Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. C. R. L.J. 255, 267 (2013).

[103] *Id*. at 279.

However, in order to allow law enforcement to continue functioning effectively in cyberspace, there should be an exception to the privilege for information that is evidence of criminal activity.

If the police have suspicion falling short of the probable cause required to get a Fourth Amendment warrant that a specific user's account contains evidence of specific criminal conduct, they would be able to ask the service if the user's account contains such evidence. If it does, the police would be able to obtain a warrant based on that affirmation, and the privilege would be void. If not, the service would answer the inquiry in the negative, and the search would end without revealing any of the user's data to anyone who did not already have access to it.[104] This proposed evidentiary privilege thus would prevent the government from conducting dragnet searches of user accounts without any particularized showing of cause or suspicion but would not allow users to hide evidence of suspected criminal activity with impunity.

B. *Violations of Terms of Service Should Require a Warrant*

With respect to services that are social in nature, the Supreme Court should determine that the Fourth Amendment is activated if the government wants to obtain information through means that would constitute a breach of a particular website's TOS if a non-government actor employed the same means.[105] In those cases,

---

[104] There are sites that explicitly promise not to cooperate with law enforcement and indeed prevent themselves from being able to cooperate with law enforcement by encrypting users' data without storing the users' passwords. Therefore, if the police ask for access to a user's account, the service literally is unable to comply. See SPIDEROAK, *Law Enforcement*, https://spideroak.com/law_enforcement/ (last visited Feb. 14, 2015) (explaining that the only data that SpiderOak has access to is metadata regarding the creation of a user's account).

[105] This "non-government user" qualification is important so that services do not accommodate government intrusion into their Terms of Service. It is true that if a site writes warrantless searches into its Terms of Service, users could take their business elsewhere. However, some services, such as Facebook, have such market power and leverage that the consumer is not in a good bargaining position because there are no close substitutes for Facebook. Facebook is a comprehensive service whereas services like Instagram and Twitter specialize in sharing pictures or brief thoughts respectively. Facebook is larger than any other social network by a wide margin, and even Google has failed to adequately

the government should have to obtain a warrant supported by probable cause before conducting the search. Furthermore, the government should be prohibited from conducting warrantless searches in which it assumes the identity of a person known to the target user regardless of whether or not such conduct is permitted by the TOS. To not do so would make a mockery of the notion of consent and potentially create an Orwellian nightmare.[106]

Under this TOS test, if the government violates a cyberspace service's TOS as they would be applied to the average user, then the government must obtain a search warrant supported by probable cause pursuant to the Fourth Amendment in order to conduct the search.[107] This standard serves two important purposes. First, it is clear. All of the cyberspace services discussed in this article have TOS agreements that define the norms of acceptable conduct while using the service, and when these terms are changed, services generally notify all users. Courts will have an easy task of deciding whether or not a given government action constituted a Fourth Amendment search because simply reading the contemporaneous TOS will resolve the inquiry.

---

compete with it. *See* Steve Faktor, *What Killed Google+ And What Can Save It*, Forbes (May 1, 2014, 1:18 PM), http://www.forbes.com/sites/stevefaktor/2014/05/01/what-killed-google-and-what-will-save-it/3/ (explaining why Google+ failed to become a successful rival to Facebook).

[106] We might already be there. Smart TVs made by Samsung have the ability to record conversation and transmit that data to a third-party where it is stored for an unknown period of time. This data, divulged with warning to consumers via a privacy agreement, would likely not be subject to Fourth Amendment protection under the third-party doctrine. Therefore, anyone purchasing a smart TV with this capability is basically placing a government listening device in his home. *See Not in Front of the Telly: Warning Over 'Listening' TV,* BBC (Feb. 9, 2015, 6:20 AM), http://www.bbc.com/news/technology-31296188.

[107] It is possible that violating a website's TOS could be illegal under the Computer Fraud and Abuse Act ("CFAA"). *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1583 (2010) (noting that although the court in *United States v. Drew* did not find a TOS violation to be illegal under the CFAA because such a ruling would have clearly given the CFAA an unconstitutionally broad sweep, "the basic strategy in Drew can be repeated in other cases that are less clear. . . . The courts now must use vagueness arguments to chisel away at the edifice of the CFAA until the resulting scope of the statute is both relatively clear and relatively narrow.").

The second purpose is that such a rule would truly reflect the reasonable privacy expectations of users. A user can reasonably expect other users to follow the TOS of the site he or she is using because those terms are enforced by negative incentives. Although many users do not diligently read the TOS of each website with which they engage, they do generally follow them. For example, Facebook famously has a policy preventing the use of a false identity.[108] To comply with Facebook's TOS, users must use their real legal names. Some users do not, but the vast majority of users do.[109] Other services, such as Twitter and Google+, do not have such a requirement, and as a result, many more anonymous accounts are on those sites than on Facebook. Posting nude photos on Facebook or Instagram is impermissible,[110] but Twitter allows those pictures. Consequently, many pornography-related accounts are on Twitter with far less, if any, on Facebook. Therefore, if making an account with a name that does not match the legal name

---

[108] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited Feb. 15, 2015) ("Facebook users provide their real names and information, and we need your help to keep it that way."). Apparently some users do not wish to be helpful. *See* Eric Ravenscraft, *How to Use a Fake Name on Facebook Without Getting Flagged*, LIFEHACKER (Sept. 22, 2014, 10:00 AM), http://lifehacker.com/how-to-use-a-fake-name-on-facebook-without-getting-flag-1637644101 (explaining how Facebook users can use a fake name without detection and subsequent account suspension).

[109] Facebook is diligent about enforcing this policy but is also willing to make accommodation in certain circumstances. *See* Reed Albergotti, *Facebook Changes Real-Name Policy After Uproar From Drag Queens*, THE WALL ST. J. (Oct. 2, 2014, 3:31 AM), http://www.wsj.com/articles/facebook-changes-real-name-policy-after-uproar-from-drag-queens-1412223040 (reporting that Facebook will allow drag queens to use their stage names on their Facebook pages after several drag queens protested the suspension of their accounts for violating Facebooks policy requiring users to use their real names on for their profiles). *But see* Steve Dent, *Native Americans Still Battling Facebook Over 'Real Name' Policy*, ENGADGET (Feb. 17, 2015), http://www.engadget.com/2015/02/17/facebook-native-american-real-names/ (telling the story of American Indians trying unsuccessfully to use their tribal names instead of their legal names for their Facebook accounts).

[110] For Facebook's terms, see FACEBOOK, *supra* note 108. For Instagram's terms, see *Terms of Use*, INSTAGRAM, https://help.instagram.com/478745558852511 (last visited Feb. 15, 2015) ("You may not post . . . pornographic or sexually suggestive photos or other content via the Service.").

of the account's creator is a TOS violation, then a user can reasonably expect that he is actually interacting with the person with whom he thinks he is interacting. Under those circumstances, the government could still create false accounts in the hopes of tricking suspects into divulging information to it, but it would have to obtain a search warrant supported by probable cause to do so. On the other hand, if the TOS allow for such false accounts, then the users of that site are on notice of that fact and do not have the same reasonable privacy expectations. Accordingly, the government could use false accounts on that particular site without obtaining warrants. The application of the TOS test will vary depending on the terms of each particular service.

In the case of Instagram, the Fourth Amendment should protect user data, such as that of Daniel Gatson, when the user has chosen to make his account "private" and require specific consent for another user to be able to view his pictures. If the pictures are publicly available, then police can view them like anyone else without violating reasonable privacy expectations. Users must take affirmative steps to ensure their photos are not viewable by the public, and this action evidences a reasonable expectation of privacy.[111] Unfortunately for Gatson, the TOS test would not have helped him because he consented to revealing his information to an account that the police happened to operate. Arguably, Gatson consented to revealing his photos to another account generally but would not have done so had he known that the police operated the account. The argument that his consent was nullified by the deception has been made before and rejected by the Court.[112]

In addition to precedential obligations, a finding that the use of informants or undercover police agents constitutes a Fourth Amendment search would cripple the government's ability to

---

[111] *Controlling Your Visibility*, INSTAGRAM, https://help.instagram.com/116024195217477/ (last visited Jan. 12, 2015) (explaining the procedure for making an Instagram account private).

[112] *See, e.g.*, Hoffa v. United States, 385 U.S. 293 (1966) (rejecting the argument that a defendant's consent is vitiated when he believes he is speaking to someone who is not an agent of the government but is, in fact, an agent of the government).

investigate and prosecute organized crime.[113] Even without the third-party doctrine, the result in *Gatson* would stand under the TOS test. Any user could have created an account under a false name to gain access to Gatson's photos without violating Instagram's TOS. Therefore, when the police did so, they did not infringe on Gatson's reasonable privacy expectations. The police conducted no search, and consequently no warrant was needed. However, the result would have been different had Gatson chosen to post his incriminating photos on Facebook.

Under the TOS test, Daniel Gatson would have had greater reasonable expectations of privacy on Facebook than he had on Instagram because the TOS of Facebook do not permit users to create accounts with names other than their own.[114] If police created a Facebook account using a name other than that of the officers creating the account, they would be in violation of Facebook's TOS and would need a Fourth Amendment warrant to conduct that search.

Instagram, Google+, Twitter, and other similar services allow their users to create anonymous profiles and accounts. As a result, as in *Gatson*, the police could trick a defendant into revealing information by using an account with a false name. This result is proper in light of the precedent set by the Court in cases involving undercover agents and informants and because people do not reasonably expect that strangers are never affiliated with law enforcement.[115] A requirement that law enforcement officers always

---

[113] *See id*. at 315 (Warren, J., dissenting) ("There are some situations where the law could not adequately be enforced without the employment of some guile or misrepresentation of identity. A law enforcement officer performing his official duties cannot be required always to be in uniform or to wear his badge of authority on the lapel of his civilian clothing. Nor need he be required in all situations to proclaim himself an arm of the law. It blinks the realities of sophisticated, modern-day criminal activity and legitimate law enforcement practices to argue the contrary.").

[114] *See* FACEBOOK, *supra* note 108. The exception to this might be if the police were a drag queen police force. *See* Albergotti, *supra* note 109 and accompanying text.

[115] *See, e.g.*, *Hoffa*, 385 U.S. at 293 (rejecting the argument that a defendant's consent is vitiated when he believes he is speaking to someone who is not an agent of the government but is, in fact, an agent of the government).

reveal their identity in the absence of a warrant would cripple their investigative effectiveness. However, allowing the police to impersonate specific real people that are known to their targets is an entirely different matter.

C. *Government Impersonation of Actual Persons*

The courts should draw a line between the police creating an undercover account based on a fictitious personality and the police creating an undercover account impersonating someone who exists and is known to the targeted user. If the police are allowed to impersonate the acquaintances, friends, and family members of investigative targets for the purposes of tricking potential defendants into consenting to searches and forfeiting their privacy rights, then fears of a totalitarian chilling effect on free expression as Justice Douglas expressed in his *White* dissent could come to fruition:

> [M]ust everyone live in fear that every word he speaks may be transmitted or recorded and later repeated to the entire world? I can imagine nothing that has a more chilling effect on people speaking their minds and expressing their views on important matters. The advocates of that regime should spend some time in totalitarian countries and learn firsthand the kind of regime they are creating here.[116]

Such a ruling would also make a mockery of the notion of consent. It is one thing to tell a secret to a trusted friend who subsequently reveals the information to the police or to grant access to a strange Instagram account knowing full well that you are disclosing information to a stranger. Those risks are inherent in interactions with other people, as the Court has held on many occasions.[117] It is another thing entirely to believe you are telling your mother something when you are actually conversing with a government agent. To say that a person who thinks he is speaking with his mother due to deception—not his own negligence—

---

[116] United States v. White, 401 U.S. 745, 764–65 (1971) (Douglas, J., dissenting).

[117] *See Hoffa*, 385 U.S. at 413 ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

consented to tell an impersonator information meant for his mother is unreasonable.[118] A finding that such deception does not constitute a search would require anyone who wanted to keep his affairs private from the government to create an elaborate system of identity checks to feel truly safe in the confidences he wishes others to keep. People reasonably expect that they do not live in a country where those measures are necessary.

Although the Supreme Court has yet to weigh in on this tactic, the Drug Enforcement Administration ("DEA") has already tried it.[119] The DEA arrested Sondra Prince because they suspected that she was involved in a conspiracy to distribute drugs.[120] During her arrest, the DEA seized pictures from her phone. Later, an agent used those pictures to create a fake Facebook profile.[121] The agent—through the fake profile—subsequently "friended" at least eleven people during an investigation into a New York drug ring.[122] During the course of the investigation, the agent posted messages from the account such as, "I miss Hovie," Prince's suspected

---

[118] In analogous circumstances pertaining to rape, many courts have unfortunately disagreed. *See, e.g.*, Suliveres v. Commonwealth, 449 Mass. 112, 118 (2007) (finding defendant not guilty of rape when he impersonated the accuser's boyfriend in order to have sex with her because "[f]raudulently obtaining consent to sexual intercourse does not constitute rape."). However, some states have passed statutes to arrive at a more just outcome in cases where rapists impersonate a victim's lover in order to engage in sexual intercourse with him or her. *See* CAL. PENAL CODE § 261(a) (2013) (listing as a circumstance constituting rape: "[w]here a person submits under the belief that the person committing the act is someone known to the victim other than the accused, and this belief is induced by any artifice, pretense, or concealment practiced by the accused, with intent to induce the belief."); *see also* TENN. CODE ANN. § 39-13-503 (2014) (listing as a circumstance constituting rape: "[t]he sexual penetration is accomplished by fraud.").

[119] *See* Terrence McCoy, *DEA Created a Fake Facebook Profile in This Woman's Name Using Seized Pics – Then Impersonated Her*, WASH. POST (Oct. 7, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/10/07/dea-created-a-fake-facebook-profile-in-this-womans-name-using-seized-pics-then-impersonated-her/ (telling the story of Sondra Prince (aka Sanda Arquiett), whom the DEA impersonated on Facebook in order to get information from her family and friends).

[120] *Id*.

[121] *Id*.

[122] *Id*.

boyfriend.[123] Prince eventually discovered the false account and sued the DEA.[124] The lawsuit settled in 2015 for $134,000, but the DEA admitted no wrongdoing.[125] Even if the DEA had obtained Prince's pictures through legitimate means, and impersonating other people was not against Facebook's TOS, the Fourth Amendment should protect citizens from such tactics.[126] The harm of allowing the government to impersonate an actual person known to the suspect is also apparent—and perhaps more chilling to the average law-abiding citizen—in an example outside the context of a specific criminal investigation.

The practice of two strangers meeting for the first time and then "friending" each other on Facebook afterwards has become common. Suppose that Ricardo has been saying and posting things online that are critical of the current U.S. government. Government agents begin to track Ricardo's social habits and in the process discover that he has recently joined the Oily Wrapper Cigar Club.[127] The agents discover that a man named Jimmy is also a member of the club, and playing the hunch that Ricardo and Jimmy have recently met, the agents make a Facebook profile for Jimmy and send a friend request to Ricardo. Ricardo, reasonably expecting that the friend request really comes from Jimmy, accepts it. In one sense, Ricardo has now consented to sharing any personal information on his Facebook with the police.[128] However,

---

[123] *Id.*

[124] *Id.*

[125] *See* Lisa Vaas, *Fake Facebook Account Case Settled With DEA Who Admits No Wrongdoing*, NAKED SECURITY (Jan. 23, 2015), https://nakedsecurity.sophos.com/2015/01/23/fake-facebook-account-case-settled-with-dea-who-admits-no-wrongdoing/.

[126] Facebook has complained to the DEA about this behavior and demanded that they stop because impersonating people on Facebook violates their TOS for everyone, including the government. *See Facebook Tells DEA: Stop Impersonating Users*, CNN MONEY, http://money.cnn.com/2014/10/20/technology/security/facebook-dea/ (last visited Feb. 26, 2015).

[127] To my knowledge such a place does not exist, and if it does, my use of its name is purely coincidental.

[128] This sense is the same dubious sense that a woman who has sex with a stranger who she believes to be her husband has consented to sex with that stranger and is not being raped.

Ricardo believes he is sharing that information with a new friend.[129] This conduct differs from that of a person who thinks he is sharing information with one stranger, but the recipient turns out to be a different stranger. If police could permissibly impersonate the close friends and family members of their targets, society would feel much less open and free.

The TOS test and categorical ban on warrantless impersonation of specific, actual people will allow users of cyberspace data sharing services some measure of reasonable Fourth Amendment protections but will not unduly hinder the effective investigation of crime.

V. CONCLUSION

Instagram, Facebook, Dropbox, and other third-party data storage services are becoming more important to Americans in their daily lives with each passing year. The Fourth Amendment should protect the reasonable privacy expectations of users of these services because diminishing the privacy rights of citizens simply because the means of communication and information storage are changing is arbitrary and illogical.

In the case of services like Dropbox and Google Drive—whose primary function is to store data for users with minimal or non-existent sharing functionality—the third-party doctrine should remain in full effect. To do otherwise would greatly endanger the public and unreasonably hinder law enforcement. However, there are few places where a person's actual privacy expectations are more reasonable than in information stored in a password-protected Dropbox account. Therefore, an evidentiary privilege is needed to ensure that law enforcement has access only to evidence of criminal activity and nothing else unless it has been granted a search warrant under the Fourth Amendment.

With respect to cyberspace data stored with services like Instagram and Facebook—whose primary purpose is the sharing of

[129] In order to avoid this mistake in the future, Ricardo will need to get in the habit of giving people he meets for the first time a piece of personal information that he can later ask them about to confirm their identities.

data—people can reasonably expect that other users adhere to the TOS. Therefore, users can reasonably expect that the government will follow the same rules. If the government does not, its efforts should be considered a search under the Fourth Amendment, and a warrant obtained upon a showing of probable cause should be required. Under any circumstances, when the police impersonate an actual person known to a target with the design to obtain information from that target, that conduct should be permissible only with a valid search warrant obtained by showing probable cause under the Fourth Amendment. Adopting these changes will allow the third-party doctrine—which is probably necessary to effectively prosecute crime in the 21st century—to adequately protect modern reasonable privacy expectations without unduly sacrificing the public good achieved through effective law enforcement.