2016

What's In The Box? Re-Conceptualizing Computers as Containers, Metadata as Contents of that Container, and Applying Fourth Amendment Protections

Christopher Michels
Michigan State Law Review

Follow this and additional works at: https://digitalcommons.wcl.american.edu/clp

Part of the Computer Law Commons, Criminal Law Commons, and the Fourth Amendment Commons

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/clp/vol3/iss2/2

This Article is brought to you for free and open access by Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in Criminal Law Practitioner by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
WHAT'S IN THE BOX?

RE-CONCEPTUALIZING COMPUTERS AS CONTAINERS, METADATA AS CONTENTS OF THAT CONTAINER, AND APPLYING FOURTH AMENDMENT PROTECTIONS

Christopher Michels
INTRODUCTION

In 1967, the United States Supreme Court handed down its watershed decision in *Katz v. United States*, establishing the principle that the Fourth Amendment protects people from government searches without a warrant in places where a person has "exhibited an actual (subjective) expectation of privacy," and that expectation is "reasonable." That same year, researchers at the Advanced Research Projects Agency met with representatives of the Department of Defense to discuss possible computer protocols that could be used to share data over long-distance using computers. Little did the Justices in *Katz* know, these computer protocols would soon revolutionize society's concept of privacy as they developed into what is today recognized as the Internet.

Every day, nearly three billion people throughout the world connect to the Internet to share and collect data. In 2013, over 74% of people in the United States used the Internet in their household. In addition, by 2014, 64% of adults in the United States had a smartphone capable of accessing the Internet. Explaining the importance of using the Internet has become a lesson in the obvious. While much of the use of the Internet is innocuous, the Internet is also commonly used for several insidious purposes, namely, for furthering crimes. The Government has an interest in monitoring these nefarious acts and, if needed, using information gathered from this monitoring to obtain an arrest warrant or to use as evidence in a criminal trial.

Unique Fourth Amendment implications are raised when the Government wants to monitor what persons do on the Internet because the Internet is not a tangible place that can be observed using traditional police tactics, but is instead a system of shared data that exists in a complex system of servers, routers, and client computers. One of the key functions of the Internet has been its ability to remember what the user has previously done. Through the use of "cookies" web browsers save the sites their user visits: Gmail saves a record of the e-mails users send, Facebook records when a person

---

2 U.S. Const. amend. IV. ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .").
3 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
5 *Id.*
8 *Smartphone*, Oxford Dictionaries, http://www.oxford-dictionaries.com/us/definition/american_english/smartphone (last visited Apr. 10, 2016) (defining smartphones as "a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications").
12 *See infra Section I.C.*
13 *See infra* notes 119-122 and accompanying text.
views a picture, Netflix can recommend shows and movies based on what users have previously watched, and the list goes on.

This information is collectively referred to as “metadata” because it is data regarding the data a user accesses on the Internet. While private companies normally store this metadata, the National Security Administration has recently been attempting to store metadata of American Internet users. This storage of computer metadata has drawn criticism from privacy advocates and the public because of the potentials for abuse.

This metadata is already stored en masse by private companies. This storage is not out of a benevolent desire to make using the Internet convenient, but because this data is valuable to advertisers who buy the metadata and use it to make Internet advertisements more targeted to the individual viewing the advertisement. While these advertisements can be distracting, the general consensus among Internet users is that targeted advertisements are an inevitable, and perhaps even necessary, price for the use of the Internet.

The question thus arises as to whether there is a reasonable expectation of privacy for things people do on the Internet. People accept that advertisers may see what they look at on the Internet, but they also do not generally want individuals or the government monitoring their whereabouts on the Internet. This dichotomy strains the traditional Katz analysis of a reasonable expectation of privacy. This Note attempts to alleviate that strain by reconceptualizing a computer as a container and metadata as information that is stored in that container.

---

15 Facebook Data Use Policy: Cookies, Pixels and Other Similar Technologies, Facebook, https://www.facebook.com/about/privacy/cookies [last visited Apr. 10, 2016].
17 See infra Part I.C for a discussion on how these technologies work.
18 The term “metadata” is also used to describe data about use of a cellular phone. See infra Part I.C.
21 See infra notes 143-148 and accompanying text.
23 See Olivier Sylvain, Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance, 49 Wake Forest L. Rev. 485, 490-91 (2014) (discussing that advertisers will see individual’s activities on the Internet).
24 Id.
By applying the Fourth Amendment protections for containers, the analysis for metadata affords clear protections to computer metadata from warrantless government searches.27

Part I of this Note discusses the background and development of Fourth Amendment protection against warrantless searches as well as the development of the Internet and the use of metadata.28 Part II describes the current circuit split and outlines the different applications of Fourth Amendment protections to metadata and the Internet.29 Part III analyzes the split and the shortcomings of current Fourth Amendment applications to metadata.30 Part IV proposes and discusses a new analytical framework for Fourth Amendment application by suggesting that computers are containers and metadata is the content of that container.31

I. TECHNOLOGY AND THE FOURTH AMENDMENT

Before analyzing how the Fourth Amendment protects computers, it is important to look at how Fourth Amendment protection against unreasonable searches has evolved along with technology. First, it is important to examine how the Supreme Court analysis of the Fourth Amendment has evolved with technology.32 Second, it is important to examine how Fourth Amendment protections extend to unreasonable searches of containers.33 Finally, a background on how the Internet works is needed to understand current problems with applying the Fourth Amendment to current technologies.34

A. Reasonable Expectations of Privacy and Warrantless Searches

The modern application of the Fourth Amendment to warrantless searches began with *Katz v. United States*.35 In *Katz*, the Supreme Court first acknowledged the Fourth Amendment "protects people and not places."36 Justice Harlan articulated the two-prong test for when a search is unreasonable: "[F]irst, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"37

The *Katz* doctrine has received criticism for its lack of any bright-line rule, especially when it is applied to new technology.38 Further, courts seem to interpret the reasonable expectation of privacy prong of *Katz* as based heavily on property law.39 What the courts view as "reasonable" is often at odds with what the legislature or most people want to be considered private.40

This reliance on principles of property law for Fourth Amendment protection is readily apparent in the majority opinion of the

---

27 See infra Part IV.
28 See infra Part I.
29 See infra Part II.
30 See infra Part III.
31 See infra Part IV.
32 See infra Section I.A.
33 See infra Section I.B.
34 See infra Section I.C.
36 Id. at 351.
37 Id. at 361 (Harlan, J., concurring); see also United States v. Jones, 132 S. Ct. 945, 950 (2012) (noting that the Supreme Court applied Justice Harlan's analysis from *Katz*).
39 Kerr, supra note 38, at 815-27.
40 Id. at 838.
recent decision of United States v. Jones. The majority relied heavily on the pre-Katz "physical intrusion" or "trespass" doctrine of Fourth Amendment protection. In Jones, the Court also acknowledged that Katz extended Fourth Amendment protections beyond common-law trespasses. One such extension exists for when the government uses technology "not in general public use" in order to view a constitutionally protected area that is not in plain view. These protected areas are any area in which a person has placed his or her effects and has "manifested an expectation that the contents would remain free from public examination." Protected areas are not static, but can move with the person and remain protected because "the Fourth Amendment protects people, not places." One such protected area is in an opaque container that a person controls.

B. Reasonable Expectations of Privacy and Containers

The general rule for searches under the Fourth Amendment is that "in cases where the securing of a warrant is reasonably practicable, it must be used." The Supreme Court has recognized a general protection for objects a person keeps within the curtilage of his or her own property. This protection also extends to hotel rooms and rental storage lockers that are kept outside of the home. Unless the object is in plain view from outside the curtilage, the object is protected from warrantless police searches. Plain view does not necessarily equate to visibility with the naked eye, but to objects that are visible using technology that is available for "general public use."

However, once a person leaves the curtilage of her home, the objects she carries with her do not necessarily receive the same protection as they would in the home. The reasoning behind this distinction is that obtaining a war-

---

42 Id. at 949 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted."). See also, Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013) (holding that the use of a drug-sniffing dog within the curtilage of the defendant’s home without a warrant was a physical intrusion and was unconstitutional).
43 Jones, 132 S. Ct. at 952. ("The Katz reasonable-expectation-of-privacy test has added to, not substituted for, the common-law trespassory test."). See also United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) ("[W]hen the government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment . . .").
44 Kyllo v. United States, 533 U.S. 27, 29-30, 40 (2001) (noting the police used, without a warrant, a thermal imager to detect infrared radiation emitting from heat lamps used to grow marijuana inside the defendant’s house.
46 Katz v. United States, 389 U.S. at 351.
47 See generally Chadwick, 433 U.S. 1.

49 Jardines, 133 S. Ct. at 1409.
51 See United States v. Karo, 468 U.S. 705, 721 n. 6 (1984) (noting that defendants “surely . . . had a reasonable expectation of privacy in their own storage locker.”). But see United States v. Lnu, 544 F.3d 361 (1st Cir. 2008) (holding that a defendant did not have a reasonable expectation of privacy in a rented storage unit after he failed to pay rent for several months).
52 Compare Oliver v. United States, 466 U.S. 170 (1984) (holding that police searching an open field is not an unreasonable search), and California v. Ciraolo, 476 U.S. 207 (1986) (holding that it was not unreasonable for police officers to survey a house from aircraft over 500 feet above the defendant’s house because they were in “within public navigable airspace” and “from this point they were able to observe plants readily discernible to the naked eye as marijuana”), with Jardines, 133 S. Ct. 1409 (holding that a search was unreasonable when evidence was found by a drug-sniffing dog while within the defendant’s curtilage without a warrant).
rant for searching a movable object is impractical. However, these objects are not without protection. The Fourth Amendment generally provides protection to the possessor of every container that conceals its contents from plain view because there is a reasonable expectation of privacy of objects contained within opaque containers. This protection from searches only extends to the person who is the actual controller of the container.

The first case to recognize Fourth Amendment protection of containers outside

55 Id. at 154 ("[T]he guaranty of freedom from unreasonable searches and seizures by the Fourth Amendment has been construed, practically since the beginning of the government, as recognizing a necessary difference between a search of a store, dwelling house, or other structure in respect of which a proper official warrant readily may be obtained and a search of a ship, motor boat, wagon, or automobile for contraband goods, where it is not practicable to secure a warrant, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.").

56 See United States v. Chadwick, 433 U.S. 1, 7 (1977), abrogated by California v. Acevedo, 500 U.S. 565, 580 (1991) ("The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained"). See also Bond v. United States, 529 U.S. 334 (2000) (holding that the physical manipulation of a person's bag by a law enforcement officer was an unreasonable search).

57 Robbins v. California, 435 U.S. 420, 427 (1981) plurality opinion) ("[U]nless the container is such that its contents may be said to be in plain view, those contents are fully protected by the Fourth Amendment."). But see United States v. Ross, 456 U.S. 798, 824 (1982) (overruling Robbins in the context of searching an automobile and holding that the scope of a warrantless search of an automobile "is defined by the object of the search and the places in which there is probable cause to believe that [contraband] may be found."); Acevedo, at 580 ("The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.").

58 Rakas v. Illinois, 439 U.S. 128, 155-56 (1978) (holding that passengers do not have legitimate expectation of privacy in the glove compartment or area under the seat of a car in which they were merely passengers and have no standing to challenge evidence found through searching these areas).

the home was Ex Parte Jackson, which recognized the Fourth Amendment protection from warrantless searches of all containers delivered in the mail. This long-standing precedent bars the government from opening without a warrant any sealed container that is sent in the mail. Even if the mail was delivered to the wrong recipient, the protection from warrantless searches continues. However, if the package is damaged or opened by a third party so that the contents are in plain view, the Fourth Amendment protection dissipates.

The Fourth Amendment has also generally extended to opaque, portable containers. The Court has defined a container as "any object capable of holding another object."

For example, in United States v. Chadwick, the defendant was transporting a 200-pound footlocker when the police, suspecting it contained marijuana, searched the container without a warrant. The Supreme Court held this search unconstitutional. The Court explained that the defendant had the same reasonable expec-

59 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household.").

60 Id. However, if the government does have a valid warrant, they may open the package searching for contraband, then reseal it and deliver the package to its intended recipient. Illinois v. Andreas, 463 U.S. 765, 771 (1983).

61 See Walter v. United States, 447 U.S. 649 (1980) (holding that the FBI cannot remove film from a container without a warrant and view it when the package had been delivered to the wrong person).


65 Chadwick, 433 U.S. at 4.

66 Id. at 15-16.
tation of privacy in placing items in a locked footlocker as if he would have kept the items in his home.67

The Fourth Amendment protection similarly extends to unreasonable searches of opaque lens containers,68 purses,69 filing cabinets,70 and briefcases.71 No protection, however, exists for containers that have a "single purpose," such as a kit of burglar tools or a gun case, which "by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance."72

Fourth Amendment protection from warrantless searches extends beyond mere visual inspection of containers.73 In Bond v. United States, the Supreme Court examined a case in which an officer examined the exterior of a person's luggage by squeezing the outside of the bag and noticing the contours of a "brick" of amphetamines.74 The Court determined this was an unconstitutional search,75 reasoning that even though a person expects her luggage will be touched and handled by other persons, there is no reasonable expectation that the container would be handled in an "exploratory manner."76

However, there are several exceptions to the warrant requirement.77 The number of exceptions has grown so much that it has led one Justice to comment that the warrant requirement has "become so riddled with exceptions that it [is] basically unrecognizable."78 For example, exceptions exist for searching closed containers for when the container had been thrown away,79 when searching containers "incident to arrest,"80 when conducted during an automobile search,81 when part of a border search,82 when part of an administrative search of regulated businesses,83 when there are exigent circumstances for the search,84 when part of an inventory search,85 when the search is of children at school,86 and when the search was conducted in objectively reasonable reliance on binding appellate precedent.87 Even with so many exceptions, any warrantless search cannot extend in scope beyond what the officer had probable cause to search.88

---

67 Id. at 11 ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination. No less than one who locks the doors of his home against intruders, one who safeguards his personal possessions in this manner is due the protection of the Fourth Amendment Warrant Clause.").

68 United States v. Donnes, 947 F.2d 1430, 1438 (10th Cir. 1991).

69 United States v. Monclavo-Cruz, 662 F.2d 1285, 1287 (9th Cir. 1981).


71 United States v. Freire, 710 F.2d 1515, 1519 (11th Cir. 1983) ("Few places outside one's home justify a greater expectation of privacy than does the briefcase.").

72 Arkansas v. Sanders, 442 U.S. 753, 764 n.13 (1979) abrogated on other grounds by California v. Acevedo, 500 U.S. 565 (1991). But see United States v. Gust, 405 F.3d 797 (9th Cir. 2005) (holding a gun case was a constitutionally protected container because it was not readily identifiable as a gun case).


74 Id. at 335.

75 Id. at 339.

76 See generally Craig M. Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468 (1985) (listing exceptions to the Fourth Amendment).

77 Acevedo, 500 U.S. at 582-583 (Scalia, J., concurring).


79 O'Connor v. Ortega, 496 U.S. 209 (1990) (holding that police officers may search an arrestee's person and area "within his immediate control").


---

78 Id.
Yet another, more far-reaching exception is the third-party doctrine. The doctrine was first introduced to hold evidence that was gathered by government informants whom the defendant had confided in constitutionally admissible, such as an associate who is wearing a recording device or an undercover agent. The basic rationale was put forward in Katz when the Court acknowledged that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." This information, while only revealed to one person, is the same as revealing the information to the public because the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrong doing will not reveal it."

The third-party doctrine extended beyond things confided to actual people to include records stored in the course of business, such as bank records and automated telephone pen registers. Pen registers are automated mechanical devices used by telephone companies that recorded the numbers a person dials on a telephone. Pen registers were used by telephone companies for the purposes of checking billing operations, detecting fraud and preventing violations of law.

The Supreme Court in Smith v. Maryland reasoned that accessing these pen register records without a warrant is reasonable since there is no reasonable expectation of privacy in the phone numbers dialed by a person. The Court also noted that no property interest of the defendant was violated since the pen registers were installed on the phone company’s property. While expanding the third-party doctrine to automated pen registers, the Court was cautious to point out the "limited capabilities" of the pen register since pen registers do not reveal any of the contents of the communication.

While the third-party doctrine is still controlling law, as technology advances, the third-party doctrine has drawn heavy criticism. Several states’ courts have backed away from the third-party doctrine or outright abandoned it. In addition, one Justice of the Su-

---

98 442 U.S. at 742.
99 Id. at 741.
100 Id. at 742.
102 Stephen E. Henderson, Learning from 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, 376 (2006) (finding that eleven states had rejected the federal third-party doctrine and ten more have possibly rejected it).
Supreme Court has openly called into question the validity of the third-party doctrine in the digital age.\footnote{United States v. Jones, 132 S. Ct. 945, 957 (2013) (Sotomayor, J., concurring) ("It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information 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.")}. This distaste for the third-party doctrine likely draws heavily on the copious amount of information people give out to third parties online and how little of that information they actually expect humans to access.\footnote{Id. ("People reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."). See also Sylvain, supra note 23 (stating that consumers are of two minds when it comes to sharing information, one being that consumers are subjectively concerned with privacy, the other that we are willing to share personal information with Internet service providers); Matthew Tokson, Automation and the Fourth Amendment, 96 Iowa L. Rev. 581, 616-17 (2011) (arguing that the third-party doctrine should apply if the information is "observed" by an actual person, not just an automated process).}

C. The Internet and Metadata

To fully understand the intricacies of privacy expectations in the digital era, it is important to take a step back and describe exactly what the Internet is and how the computers people use every day interact with the Internet. According to the U.S. Census Bureau in 2014, 78.9% of all United States households have a computer at home, with 94.8% of those homes using their computer to connect to the Internet.\footnote{United States Census Bureau, Computer & Internet Trends in America, United States Census Bureau (Oct. 28, 2014), http://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf.} In addition, 70.6% of individuals 25–34 years of age use smartphones.\footnote{Id.; Smartphone, supra note 8 (defining smartphones as "a mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, internet access, and an operating system capable of running downloaded applications.")}. Smartphones have become such a ubiquitous part of Americans’ daily lives that the Supreme Court has noted "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."\footnote{Riley v. California, 134 S. Ct. 2473, 2484 (2014).} While the Internet is used at a nearly universal level, how exactly it works is rarely explained.

To begin, the Internet is not so much a place as much as it is a thing. When two or more computers are connected and share data, they create a network or an "internet."\footnote{In re DoubleClick Inc. Privacy Lit., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001).} The "Internet" is the name given to the large infrastructure of these connections.\footnote{Id. ("The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables and routers through which data is shared online.").} This data and information contained within the Internet is most commonly found on the platform known as the World Wide Web.\footnote{Id. ("The [World Wide] Web is data: a vast collection of documents containing text, visual images, audio clips and other information media that is accessed through the Internet.").}

There is also an important distinction between the Internet and the way users access the Internet.\footnote{Id. ("The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables and routers through which data is shared online.").} Every computer that is connected to the Internet is part of a network that is usually created and maintained by a private company known as an Internet Service Provider or ISP who connects the computer's network to the larger network of networks that is the Internet.\footnote{Jeff Tyson, How Internet Infrastructure Works, How Stuff Works, http://web.stanford.edu/class/msande91s/www-spr04/readings/week1/Howstuffworks.htm. (last visited Apr. 10, 2016).} Every machine that connects to the Internet has a unique identifying number, called an Internet Protocol Address or an IP
Address. This number is present regardless of whether the computer is a "client" computer, which requests data, or is a "server," which provides data.

These servers can take up a large physical space. The reason for their colossal size is due to the fact that the servers often need to store an immense amount of data. This data includes the content that is found on the Internet, as well as data regarding the access to that content. This data regarding the access to data is called "metadata.”

Metadata is often cumulated using a computer program known as a "cookie," which tracks an Internet user's actions. Popular computer servers, such as Facebook and Google, use these cookies to track their users' actions. By tracking a user's activities online, companies are able to aggregate and sell the metadata to advertisers, who are able to take the metadata and target advertisements based on what the individual user has been looking at online. It is possible to access the Internet without having some cookies tracking one's movements by using a web browser's privacy mode, or by using data encryption. However, it is extremely difficult to eliminate all cookies, as any activity online will bring more cook-

113 Id.
114 Id. ("A server has a static IP address that does not change very often. A home machine that is dialing up through a modem, on the other hand, typically has an IP address assigned by the ISP every time you dial in. That IP address is unique for your session—it may be different the next time you dial in. This way, an ISP only needs one IP address for each modem it supports, rather than one for each customer.").
116 Jeffrey Dean & Sanjay Ghemawat, MapReduce: Simplified Data Processing on Large Clusters, 51 Comms. ACM 113, 3 (2008) (stating in 2008, Google was processing over twenty petabytes (a petabyte is 1000 terabytes or 10 bytes to the 15th power) of data per day).
117 See infra notes 143-148 and accompanying text.
119 Id. (noting that Google maintains hundreds of thousands of servers, located in data centers ranging from a warehouse in Iowa, a converted paper mill in Finland, and other large spaces.).
120 See infra notes 143-148 and accompanying text.
121 Id. ("A server has a static IP address that does not change very often. A home machine that is dialing up through a modem, on the other hand, typically has an IP address assigned by the ISP every time you dial in. That IP address is unique for your session—it may be different the next time you dial in. This way, an ISP only needs one IP address for each modem it supports, rather than one for each customer.").
122 Id.
123 Google Support Forum, Google, https://support.google.com/chrome/answer/95464?hl=en. (last visited Apr. 10, 2016) (For example, Google Chrome has an "incognito mode." In this browser, Google will not save cookies, however the information that is gathered by websites a person accessed can still be saved by that server).
124 See Jeffrey Rosen, The Unwanted Gaze 173-78 (2000) (discussing how encryption works and services that provide online encryption).
ies, and if cookies are disabled, many websites will not function properly.\textsuperscript{125}

Metadata from computers is similar to the metadata that is stored by phone service providers.\textsuperscript{126} The term \textit{metadata} is used to refer to both data regarding phone usage and data regarding computer usage.\textsuperscript{127} While differences exist between the two, both fall within the same federal statutory definition under the Stored Communications Act (SCA).\textsuperscript{128} Metadata reveals similar information for both cell phones and computer usage.\textsuperscript{129} For example, metadata accrued when using e-mail services will include the sender's and recipient's e-mail addresses, the unique IP address of the sender, the date and time the e-mail was sent, and whether the e-mail made it to the recipient.\textsuperscript{130}

\textsuperscript{125} See Mozilla Support: Disable Third-party Cookies in Firefox to Stop Some Types of Tracking by Advertisers; Mozilla, https://support.mozilla.org/en-US/kb/disable-third-party-cookies (last visited Apr. 10, 2016) (stating that many e-mail services will not work without third-party cookies).

\textsuperscript{126} Guardian, supra note 118.

\textsuperscript{127} Id.

\textsuperscript{128} See 18 U.S.C. § 2703(c)(A)(B) (2009) ("[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity . . . obtains a warrant . . . [or] obtains a court order . . . "). (emphasis added). 18 U.S.C. § 2510(13) (2015) (defining electronic communication services as "any service which provides to users thereof the ability to send . . . electronic communications."); 18 U.S.C. § 2510(12) (2015) (defining electronic communication as "any transfer of . . . signals . . . sounds . . . or data . . . of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photoptical system that affects interstate or foreign commerce."). See also \textit{United States v. Perrine}, 518 F.3d 1196, 1199-1201 (10th Cir. 2008) (stating computer metadata falls within the Electronic Communications Privacy Act); \textit{In re Application of the U.S. for Historical Cell Site Data}, 724 F.3d 600, 607 (5th Cir. 2013) (stating cell phone metadata falls within the Stored Communications Act).\textsuperscript{129} See supra note 126.

\textsuperscript{129} Id.


\textsuperscript{130} Sylvain, supra note 23, at 493.


\textsuperscript{130} Id.

\textsuperscript{131} Id.

\textsuperscript{132} Id.

\textsuperscript{133} Id.

\textsuperscript{134} Id.

\textsuperscript{135} Id.

\textsuperscript{136} Id.

\textsuperscript{137} Id.
you browse (69%), and the time of day you are online (50%). 138

On the other hand, a majority of people (59%) do not believe it is possible to be completely anonymous online. 139 In addition, Internet users appear to give up their reasonable expectation of privacy by accepting clickwrapped contracts during the user’s online use. 140 Accepting a contract is important for many courts’ analysis of whether any expectation of privacy is reasonable. 141 Scholars have argued that these contracts give away privacy rights without the individual even knowing they are doing it, because people “agree” to the terms of use without reviewing them. 142

For example, by using Google’s services, a person is agreeing to Google’s “Terms of Service,” which allows them to collect the following information: 143 search queries, IP addresses, cookies, actual location information (such as GPS signals sent by a mobile device), and personal information (such as names, e-mail addresses, telephone numbers or credit card information given to Google). 144 Google also reserves the right to share information if it has a good-faith belief the disclosure is reasonably necessary to “meet any applicable law, regulation, legal process or enforceable government request.” 145

One possible explanation for why people simultaneously believe that they are revealing information while still keeping the information private is because of the infinitesimal likelihood that any actual person will see that information. 146 The processing and storage of the vast amount of metadata is automated out of efficiency. 147 For example, online bookstore Amazon lists the “Automatic Information” that it stores and the software it uses to gather and analyze the metadata. 148 It is the gathering and aggregation of metadata that makes the Internet possible. 149 However, to what extent metadata is protected from government searches is a question that has not yet been clearly answered.

138 Id. This information falls within the definition of metadata. See supra note 132.
139 Raine, et al., supra note 135.
141 See, e.g., City of Ontario, Cal. v. Quon, 560 U.S. 746, 763-65 (2010) (determining that even if there is an expectation of privacy in text messages, a contract between the plaintiff and his governmental employer made a search of plaintiff’s cell phone reasonable); United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding that a remote search of defendant’s work computer did not violate the Fourth Amendment because of a contract with the employer that allowed the employer to audit his computer).
142 Crowther, supra note 140, at 354.
143 Google Terms of Service, Google, http://www.google.com/intl/en/policies/terms/ [last visited Apr. 10, 2016]. (“By using our Services, you agree that Google can use such data in accordance with our privacy policies.”).
144 Google Privacy Policy, supra note 120.
145 Id.
146 See Teksonnory test.rson of the use of their services f privacy), , supra note 104, at 604-09.
147 Id. at 603 (“ISPs . . . automatically collect and process enormous amounts of data about users’ web-surfing habits. ISPs maintain logs of the IP addresses of each website a user visits as well as the volume of data transmitted to and from the user: Some service providers even monitor and retain the address of each individual page a user visits. Many affiliated groups of websites collect the URLs of each page a user sees within their group. These service providers and website networks then automatically use this information to target advertisements to the individual user, or sell the information to third-party advertisers for the same purpose.”).
II. CURRENT PROTECTIONS FOR COMPUTER DATA AND METADATA

With the rise of the Internet, computers and cell phones are becoming an important part of everyday life. The problem for courts in analyzing Fourth Amendment protections is that the use of these devices creates metadata, which contains information that does not fit neatly into any category of current Fourth Amendment protections.

Under the Stored Communications Act (SCA), the government may obtain from Internet Service Providers (ISPs) or telephone companies any metadata of a user by obtaining a court order. This court order does not require a showing of probable cause, but only a “specific and articulable showing that there was reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation.”

The Supreme Court has yet to address the issue of whether warrantless searches of metadata are constitutional. Without any guidance from the Supreme Court, circuit courts have diverged widely in the constitutionality of searching either computer or phone metadata without a warrant and relied on a range of rationales. Cases discussing telephone metadata provide a useful comparison for computer metadata, since both types of metadata fall within the same federal statute. Circuits fall into three categories: (1) holding warrantless inspections of data and metadata under the SCA are unconstitutional because there is a reasonable expectation of privacy in that information; (2) holding warrantless inspections of metadata constitutional because metadata falls under the third-party doctrine or is analogous to a pen register; and (3) holding that warrantless inspection of metadata is not per se unconstitutional, but that magistrate judges have discretion to require a showing of probable cause.

A. Warrantless Searches under the Stored Communications Act Are Unconstitutional

The first court to attack the constitutionality of warrantless searches under the SCA was the Sixth Circuit in United States v. Warshak. In Warshak, the government obtained 27,000 of the defendant’s private e-mails from his ISP without a warrant. The case did not directly implicate Fourth Amendment protection of metadata, but the protection of contents on the Internet, which in this case were the defen-
fendant’s e-mail.\textsuperscript{162} The Sixth Circuit held that there is a reasonable expectation of privacy in e-mails because they are the digital equivalent of letters.\textsuperscript{163}

In analyzing the relationship between the ISP and e-mails, the court treated the ISP not as a third party, but as an “intermediary” that had the ability to access the data, but did not diminish the reasonable expectation of privacy in that data.\textsuperscript{164} The court concluded that section 2703(d) of the SCA, allowing the government to obtain e-mails from ISPs without a warrant, was unconstitutional.\textsuperscript{165}

In 2014, a panel from the Eleventh Circuit held unconstitutional the same provision of the SCA as applied to the warrantless searches of cell phone metadata in the case of \textit{United States v. Davis}.\textsuperscript{166} In \textit{Davis}, the government obtained information from the defendant’s cell-phone service provider that showed the defendant had placed and received cell-phone calls in close proximity to the locations of the robberies for which he was charged.\textsuperscript{167} This cell site location information is a form of telephony metadata.\textsuperscript{168} In striking down the law, the Eleventh Circuit relied heavily on the Supreme Court’s decision in \textit{United States v. Jones}\textsuperscript{169} and determined that tracking a person’s movements via cell phone was turning a person’s private whereabouts into a public event.\textsuperscript{170} The Eleventh Circuit pointed out that metadata regarding the location of a cell phone did not fall within the third-party exception.\textsuperscript{171} The court relied on reasoning from a case from the Third Circuit that stated that a cell-phone user is not voluntarily revealing her location to the phone company, even when placing a call.\textsuperscript{172} Moreover, even if the user is willingly giving metadata, the user is unaware the information will be stored.\textsuperscript{173}

\textbf{This opinion was later vacated en banc.}\textsuperscript{174} The en banc 11th Circuit determined that obtaining cell site location information from the service provider without a warrant was not a violation of the Fourth Amendment because the information was a “business record” similar to the bank records from \textit{Miller} or the pen reg-

\textsuperscript{162} \textit{Id.} at 288 ("The government may not compel a commercial ISP to turn over the contents of a subscriber’s emails without first obtaining a warrant based on probable cause.") (emphasis added).

\textsuperscript{163} \textit{Id.} at 285-86 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . . Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age."). \textit{But see United States v. Lifshitz}, 369 F.3d 173, 193 (2d Cir. 2004) (concluding that the Fourth Amendment protects against searches of a probationer’s home computers and e-mails, but that the ‘special needs’ of the probation system are sufficient to justify conditioning [defendant’s] probation upon his agreement to submit to computer monitoring.").

\textsuperscript{164} \textit{Id.} at 286-87. ("As an initial matter, it must be observed that the mere \textit{ability} of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. . . . Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country").

\textsuperscript{165} \textit{Id.} at 288.

\textsuperscript{166} 754 F.3d 1205, 1213, \textit{vacated}, 573 Fed.Appx. 925 (11th Cir 2014) (mem.).

\textsuperscript{167} \textit{Id.} at 1209-10.

\textsuperscript{168} \textit{See supra} note 127.

\textsuperscript{169} 132 S. Ct. 945 (2012).

\textsuperscript{170} \textit{Davis}, 754 F.3d at 1216.

\textsuperscript{171} \textit{Id.} at 1216-17.

\textsuperscript{172} \textit{Id.} at 1217 ("[W]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed, and there is no indication to the user that making that call will also locate the caller.") (quoting \textit{In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t}, 620 F.3d 304, 317 (3d Cir. 2010)).

\textsuperscript{173} \textit{Davis}, 754 F.3d at 1217.

\textsuperscript{174} \textit{United States v. Davis}, 573 Fed.Appx. 925 (11th Cir. 2014) (mem.).
ister from Smith. The majority emphasized the importance that the metadata was a form of “non-content evidence” created for use by a third party. However, this ruling only applied to cell site location metadata and no other forms of metadata.

In dissent, two judges echoed the sentiments of the original panel’s ruling and argued the majority’s reason could “allow the government warrantless access to not only where we are at any given time, but also to whom we send e-mails, our search histories, our online dating and shopping records, and by logical extension, our entire online personas.” The dissent latched onto the ambiguous line between content and non-content evidence.

A divided Fourth Circuit, in a similar case involving the warrantless obtaining of cell phone metadata, disagreed with the en banc Eleventh Circuit in United States v. Graham. Relying on the Supreme Court’s decisions from Kelo and Kyllo, the Eleventh Circuit held that the warrantless obtaining of cell site location information, a form of metadata, is unconstitutional because it could “allow the government to place an individual and her personal property—specifically, her cell phone—at the person’s home and other private locations at specific points in time.” Furthermore, the court relied concurrences of Riley and Jones, the Fourth Circuit held that obtaining cell phone locations was the form of long term tracking and dragnet-style surveillance of a person’s movements that is an unreasonable search.

B. Metadata Under the Third-Party Doctrine and Pen Registers

The Fourth Circuit’s decision in Graham contrasts with an earlier Fourth Circuit decision in an unpublished opinion from 2000 that held there is no reasonable expectation of privacy of any information, including metadata, shared with Internet service providers. While not explicitly reciting the third-party exception, the court pointed to a lack of a reasonable expectation of privacy because the defendant “entered into an agreement to obtain Internet access from [his ISP and] he knowingly revealed his name, address, credit card number, and telephone number to [the ISP] and its employees.”

In 2001, the Sixth Circuit echoed this sentiment and determined that computer users do not have a reasonable expectation of privacy in metadata relating to “their subscriber information because they have conveyed it to another person—the system operator.” This subscriber information was metadata that included the names, addresses, birthdates, and passwords of subscribers to an online bulletin board. The court equated subscriber infor-

---

175 United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc).
176 Id. at 511.
177 Id. at 505 (calling the ruling “narrow”).
178 Id. at 533 (Martin, J., dissenting).
179 Id. at 537 (Martin, J., dissenting). But see, Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005, 1019-20 (2010) (articulating that the content/non-content distinction can be a viable way to structure Fourth Amendment protections).
180 796 F.3d 322, 355-56 (4th Cir. 2015) vacated for re-hearing en banc, 624 Fed. Appx. 75 (mem.).
181 Id. at 346.
182 Id. at 347-49.
184 Hambrick, 55 F. Supp. 2d at 508.
185 Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001).
186 Id. This subscriber information is similar to information Google gathers from its users, which Google will only share with the user’s consent or if they have a “good-faith belief that . . . disclosure of the information is reasonably necessary to . . . meet any applicable law, regulation, legal process or enforceable governmental request.” Google Privacy Policy, supra note 120.
formation to bank records and pointed to the Supreme Court ruling that there is no reasonable expectation of privacy in bank records. By 2010, the Sixth Circuit formed a distinction between metadata regarding subscriber information from the metadata created when sending e-mails.

The Ninth Circuit in 2007 addressed the warrantless inspections of metadata and found them to be functionally equivalent to pen registers. The court looked in particular at metadata displaying the "to/from" addresses of [defendant’s] e-mail messages, the Internet protocol ("IP") addresses of the websites that he visited[,] and the total volume of information transmitted to or from his account. The court equated the surveillance of this metadata to surveillance of the physical mail. The court treated e-mail as contents of mail and all the metadata as information transmitted to a third party, the ISP, similar to the address on the outside of a package.

The Tenth Circuit joined in a similar line of reasoning when looking at whether there is a reasonable expectation of privacy in Internet subscriber information. In that case, Pennsylvania law enforcement obtained, via court order, the subscriber information from Yahoo!, from which they were able to determine each day in which the defendant had logged into his account from his home computer. The court determined there was no reasonable expectation of privacy in subscription information because it had been revealed to a third party; namely the ISP. Similar to all the circuits in this category, the Tenth Circuit relied on the third-party doctrine and found no reasonable expectation of privacy in metadata.

C. Magistrate Judge Discretion

The Third Circuit currently stands alone in determining that it is in the discretion of the magistrate judges, who grant the court order compelling metadata from a cell phone service or ISP, as to whether probable cause is necess-

187 Id. (citing United States v. Miller, 425 U.S. 435 (1976)).
188 United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (en banc) ("T[he] mere ability of a third-party intermediary to access the contents of communication cannot be sufficient to extinguish a reasonable expectation of privacy."). See also Warshak v. United States 490 F.3d 455, 472 (6th Cir. 2007) ("Guest v. Leis did not hold that the mere use of an intermediary such as an ISP to send or receive e-mails amounted to a waiver of a legitimate expectation of privacy.").
189 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) ("We conclude that the surveillance techniques [that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account] are constitutionally indistinguishable from the use of a pen register that the Court approved in Smith."). (referring to Smith v. Maryland, 442 U.S. 735 (1979) (holding pen registers constitutional); But see In re Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx] Internet Serv. Account/User Name [xxxxxx@ xxx.com], 396 F.Supp.2d 45 (D. Mass. 2005) (holding that a pen register cannot extend to content).
190 Id. at 504. This information falls within the definition of metadata. Supra note 127.
191 Id. at 511 ("The government’s surveillance of e-mail addresses . . . may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.").
192 Id. ("E-mail, like physical mail, has an outside address ‘visible’ to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. . . . The contents may deserve Fourth Amendment protection, but the address and size of the package do not."). But see Kerr, supra note 179, 1017-19 (arguing to replace this type of distinction).
193 United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (citing cases).
194 Id. at 1199.
195 Id. at 1204-05. The court also pointed out that the defendant had peer-to-peer software on his computer which allowed other computers access to files on his computer which "additionally vitiates any expectation of privacy he might have in his computer and its contents." Id.
196 Id.
sary to obtain the metadata. 197 The court pointed out that the government did not seek the contents of any electronic communication, but metadata regarding the cell site location. 198 The court nonetheless deferred to the magistrate judge’s ruling that cell phone metadata could be the functional equivalent of a tracking device, which would require a showing of probable cause. 199 The court relied heavily on the legislative history of the SCA in giving discretion to magistrate judges on whether probable cause should be required to compel a company to provide the government with a customer’s metadata. 200

The concurrence added an alternative reasoning for why a magistrate judge could turn down a court order compelling disclosing metadata. 201 The concurrence reasoned that using cell-phone metadata could allow the government to track a user’s location within his home and that doing so without a warrant would be an unreasonable search. 202 The current circuit split as to whether the Fourth Amendment protects metadata shows the need for a unified analytical framework for distinguishing when there is a reasonable expectation of privacy in metadata. 203 Some circuits hold that an ISP’s or cell phone service provider’s ability to access a user’s metadata is enough, under the third-party doctrine, to defeat a reasonable expectation of privacy. 204 Others circuits hold that access alone is not enough to view metadata without a warrant, 205 or at least not enough to view metadata that shows the location of an individual. 206 The main source of conflict comes from when a defendant’s expectation of privacy can be considered “reasonable.”

III. SHORTCOMINGS OF CURRENT PROTECTIONS OF METADATA

Scholars have argued that the Katz test of a “reasonable expectation of privacy” will progressively get less workable as technology progresses since the courts lack the intricate knowledge of new technologies and the third-party doctrine will put the court in a difficult position. 207 This position appears to be closing in when applying Katz and the reasonable expectation of privacy to computer and

197 In re Application of the U. S. for an Order Directing a Provider of Elect. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 319 (3d Cir. 2010) (“Because (SCA § 2703) as presently written gives the [magistrate judge] the option to require a warrant showing probable cause, we are unwilling to remove that option . . . .”).
198 Id. at 306 (“The Government does not . . . seek disclosure of the contents ofwire or electronic communications. Instead, the Government seeks what is referred to in the statute as ‘a record or other information pertaining to a subscriber to or customer of such service’ . . . .”).
199 Id. at 310-11 (“The [magistrate judge] held that . . . the government must show probable cause because a cell phone . . . cell phone location information . . . make[s] a cell phone act like a tracking device.”).
200 Id. at 313-14.
201 Id. at 320 (Tashima, J., concurrence) (“[T]he magistrate may refuse to issue [a court order compelling metadata disclosure] only if she finds that the government failed to present specific and articulable facts sufficient to meet the standard under 28 U.S.C. § 2703(d) or, alternatively, finds that the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user’s location within the interior or curtilage of his home.”).
202 Id. (citing Kyllo v. United States, 533 U.S. 27, 35-36 (2001)).
203 See Sylvain, supra note 23, at 523 (concluding that the “Fourth Amendment doctrine today has nothing to offer in the way of privacy protection when even courts are uncertain about how to define public expectation as a descriptive matter.”).
204 Supra Section II.B. See also, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (holding similarly).
205 Supra Section II.A.
206 Supra Section II.C.
207 See generally Sylvain, supra note 23 (discussing the failure to establish a clear reasonable expectation of privacy in a digital context).
208 Crowther, supra note 140.
cell phone metadata.⁹⁹ All three categories of courts tend to have the same flaw; namely, they all lack a clear conception of what metadata has a reasonable expectation of privacy and what does not.²¹⁰

The first group of circuits²¹¹ only addressed a narrow category of metadata. The Sixth Circuit in Warshak dealt with the acquiring of only the content of e-mail.²¹² The court left open the possibility that non-content metadata, such as IP addresses, subject lines of e-mails, and other forms of metadata do not get protection.²¹³ The Fourth Circuit in Graham did draw a distinction between information that was voluntarily conveyed to a third party and metadata that was not.²¹⁴ However, the case dealt only with cell site information, leaving questions about computer metadata unanswered.²¹⁵ Similarly, the panel in the Eleventh Circuit in Davis dealt only with cell phone location.²¹⁶ If the rationales regarding telephone metadata from the Fourth Circuit and the panel from the Eleventh Circuit extend to computer metadata, it could support Fourth Amendment protection for metadata that reveals a user’s location or that is automatically generated, such as a person’s IP address.²¹⁷

The first category of circuits also tends to gloss over the third-party doctrine in its analysis.²¹⁸ The Sixth Circuit does attempt to vitiate the applicability of the third-party doctrine by referring to an e-mail server as an “intermediary” and not a third party.²¹⁹ Similarly, the Fifth Circuit treats cell phone companies as intermediaries who are entrusted with users’ location information that is not intended “to be open to inspection of others.”²²⁰ The Eleventh Circuit panel in Davis addressed the third-party doctrine in the context of cell-phone location and determined that a cell-phone company was not a third party because the only metadata that a person voluntarily shares with a phone company “is the number that is dialed.”²²¹ Neither the Eleventh Circuit panel nor the Fifth Circuit address what would happen to the reasonable expectation of privacy if access to a person’s location, via GPS location, becomes part of the

²⁹⁹ See generally Sylvain, supra note 23.
²¹⁰ See Crowther, supra note 140, at 358-63 (providing examples of "where the traditional reasonable expectation of privacy standard has failed in digital contexts and where the courts have yet to clearly define boundaries.").
²¹¹ Supra Section IIA.
²¹² United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010) (en banc).
²¹³ Id. at 286. "[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails." (emphasis added). See also Kerr, supra note 179, at 1019-31 (arguing that content of Internet communications is protected by the Fourth Amendment but non-content metadata is not).
²¹⁴ United States v. Graham, 796 F.3d 332, 376-77 (4th Cir. 2015).
²¹⁵ Id. See also United States v. Bynum, 604 F.3d 161, 162-63 (4th Cir. 2010) (holding there was no unreasonable search when police acquired a defendant’s Yahoo! account information without a warrant).
²¹⁶ See United States v. Davis, 754 F.3d 1205, 1208 (11th Cir. 2014).

²¹⁷ Graham, 796 F.3d at 358 ("Like a user of web-based email who intends to maintain the privacy of her messages, however, there is nothing the typical cell phone user can do to hide information about her location from her service provider."). See also Tokson, supra note 133, at 2131-36 (arguing that search terms and IP addresses are content similar to e-mails).
²¹⁸ Warshak, 631 F.3d at 287 ("We recognize that our conclusion may be attacked in light of the Supreme Court’s decision in United States v. Miller ...."); United States v. Graham, 796 F.3d 332, at 378. (Motz, J., dissenting) (arguing that the third party doctrine should apply to metadata).
²¹⁹ Warshak, 631 F.3d at 287. See also Patricia L. Bellia & Susan Freiwald, Fourth Amendment Protection for Stored E-Mail, 2008 U. Chi. Legal F. 121 (arguing that ISPs are not third parties under existing precedent).
²²⁰ Graham, 796 F.3d at 358.
²²¹ Davis v. United States, 754 F.3d 1205, 1217 vacated 573 Fed.Appx. 925 (11th Cir. 2014) (mem.).
contract for using a cell phone or Internet service.²²²

The rationales of the second group of circuits²²³ rely heavily on cases from the 1970s, namely Miller²²⁴ and Smith.²²⁵ These courts seem to commit the folly of “contend[ing] that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”²²² While the information was gathered from individuals’ home computers, none of the circuits discuss the technology’s “general public use” requirement set forth in Kyllo for when viewing inside a person’s curtilage.²²⁷ Some scholars have argued that these circuits’ rationales are drawn from judges’ relative lack of experience in the context of swiftly evolving digital technologies.²²⁸

Additionally, the rationales of courts in the second category seem to strain the third-party doctrine to a great extent.²²⁹ Many activities done on the Internet are not knowingly exposed to the public or confined to third parties since these third parties are not persons, but automated machines.²³⁰ Treating these automated machines as functionally equivalent to pen registers looks past critical dicta from Smith where the Court acknowledges the “limited capabilities” of the pen register,²³¹ which points out that pen registers were not even capable of indicating if the call was even completed.²³² Metadata reveals far more information than a pen register could reveal.²³³

The rationale of the third group²³⁴ strikes a middle ground between the first and second groups. By giving deference to magistrate judges, the court some shows flexibility in determining which metadata is protected and which is not.²³⁵ The problem with this deference is that this will lead to inconsistent rulings on the same types of metadata based on which magistrate judge is making the ruling.²³⁶ Additionally, the reasoning that allows magistrate judge discretion in requiring a heightened showing of probable cause may not be on firm statutory grounds.²³⁷

²²² See Crowther, supra note 140, at 353-55 (arguing that contracts greatly affects the reasonable expectation of privacy). For an example of a contract that has a clause allowing for tracking GPS location, see Google Privacy Policy, supra note 120 (“When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device.”). See also City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010) (holding that an employment contract affects the reasonable expectation of privacy in messages sent from a work pager).
²²³ Supra Section II.B.
²²⁷ See, e.g., United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008) (stating that the police were able to track the sending of illegal content sent from defendant’s computer to inside his house).
²²⁸ Kerr, supra note 38, at 875-76 (“Judges struggle to understand even the basic facts of [digital] technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension.”); Crowther, supra note 142, at 356 (“[H]ow can a judge with no technological background grasp the intricacies of an IP address that allows substantial tracking of individuals online, and at the same time gauge how much privacy society feels it is giving up by going online?”).
²²⁹ See Tokson, supra note 104, at 588-601.
²³⁰ Id.
²³² Id. at 736 n. 1.
²³³ See supra note 130-132 and accompanying text.
²³⁴ Supra Section II.C.
²³⁵ Id.
²³⁶ See Kerr, supra note 179, at 1029 (stating every Internet application generates its own data and the line between protected data and non-protected data is difficult to establish.”).
²³⁷ See In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 606-07 (5th Cir. 2013) (arguing that the Third Circuit’s analysis allowing discretion ignores the intervening “shall” in 28 U.S.C. § 2703(d)).
With a circuit split on whether there is a reasonable expectation of privacy in metadata, a simplified analytical framework is needed to determine when metadata is protected from search. As the use of computers becomes more prevalent, it becomes imperative to create established protections for metadata. The next Part seeks to establish this framework.

IV. CONTAINER LAW AND METADATA

Courts should consider computers as a container, treat all metadata as contents stored within computers, and apply the same Fourth Amendment protections for metadata as for other contents of containers. By treating computers as containers, a person’s reasonable expectation of privacy in metadata is shaped by how they use ISPs and a clear line is established between what metadata is protected and what metadata is not. Courts can address computers kept within the home and computers used outside the home, i.e. smartphones, and applying container law, find identical Fourth Amendment protections for metadata.

A. Computers and Smartphones as Containers

The Supreme Court defines a container as “any object capable of holding another object” and both computers and phones fit squarely within the definition of an opaque container. Both are portable and could potentially contain objects that a person wishes to keep from public view. The Supreme Court has already recognized that modern cell phones are a container that hold a person’s “privacies of life” and deserves Fourth Amendment protection. Computers follow similarly since they contain vast amounts of information and smartphones are already considered “minicomputers.”

Furthermore, computers are implicitly referred to as containers in the Stored Communications Act. Section 2703(b) requires disclosure of contents of electronic communication that are “held or maintained” by a provider of “remote computer service.” Part (c) of that section applies to the disclosure of “other information pertaining to a subscriber or customer of such service” that the computer service provider maintains. Both the contents of electronic communications and information are stored by ISPs in massive computer servers. While their contents are electronic data and are not physically tangible, the Supreme Court has recognized that data is still an object that can be contained in a computer or cell phone. Since computers and cell phones are containers, all of their contents should receive similar protection.

B. Metadata as Contents

Computers contain not only data, but also metadata. Scholars have articulated there is a distinction between metadata that is “content” and metadata which in non-con-
tent "transactional data." However, the line between metadata that could be considered content and metadata that could be considered transactional is blurred and difficult to find. IP addresses and search queries are metadata that fall around the hazy line. By treating all metadata as contents of a computer similar to data, the analysis avoids finding this difficult distinction and recognizes that metadata is contained the same as data.

1. Internet Servers as Rented Space

Treating metadata as contents in a container then moves the analysis of whether there is a reasonable expectation of privacy to who has a possessory interest in the container so that it has protection from unreasonable searches. The easy answer would be the ISP who owns the server. Yet that ISP did not create the metadata and has no interest in any particular metadata created by any one individual. The ISP’s interest is in aggregating the metadata and selling it to advertisers. Often, larger Internet companies will remove any metadata that could be used to identify a particularized individual.

A possessory interest is shared between the ISP and the creator of the metadata, the user of the computer. This makes the storage of the metadata akin to a rental storage unit. The user allows, consciously or not, their metadata to be stored within third-party servers, via third-party cookies, in order to use the Internet effectively. In exchange for the use of the storage, the user agrees, via contract, to allow the ISP to sell its aggregated metadata. Part of this agreement is the understanding that the operators, and not users, have standing to challenge searches.

---

251 See, Tokson, supra note 133, at 2123-26 (arguing the distinction of information as either content or non-content is “perhaps the most important determinant of the constitutional and statutory protection which that information receives.”); Kerr, supra note 192, at 1019-22 (formulating a distinction between content and non-content metadata); Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J.L. & Pol’y 211, 279-80 (2006) (arguing that transaction data should be constitutionally protected).

252 See Kerr, supra note 192, at 1029-30 (“Every different Internet application generates its own data, and lines must be drawn to distinguish content from non-content for each. Some cases are difficult”).

253 Tokson, supra note 133, at 2109-10.

254 See id., at 2126-32 (stating that e-mails and the transmission of website data are sent using “packets of digitalized information” which includes content as well as metadata). But see Kerr, supra note 192, at 1021-22 (arguing the “fact that content and non-content information are actually jumbled together as packets shouldn’t matter”).


256 See, e.g., Brian I. Simon, The Tangled Web We Weave: The Internet and Standing Under the Fourth Amendment, 21 Nova L. Rev. 941, 968 (1997) (arguing only system
user's metadata is handled by automated machines and the user's activities on the Internet will not be viewed by a person who could identify the user.264

Treating the servers as rental storage is similar to the Sixth Circuit's reasoning that an e-mail service provider is an "intermediary" and avoids implicating the third-party doctrine in establishing Fourth Amendment protection.265 This reasoning could be expanded to protect all Internet services and not just e-mail.266 E-mails are easy to conceptualize as sending data and content since they are similar to ordinary mail.267 However, using any Internet service is a similar sending and receiving of data.268 For example, typing in a search query on Google is sending data from the user, i.e., the requested search terms.269 Google's server receives the data and then sends data, i.e., the search results, and links to other web pages back to the user.270 Google's servers then store all the metadata.271

Computer servers are far different than the third parties that were originally envisioned by the Court in Katz.272 The Court in Katz excluded from protection what persons "knowingly expose[s] to the public"273 and things shared with an individual274 or even a machine, such as a pen register.275 The Supreme Court was cautious to point out these limited capabilities of the pen register.276 While a computer server is an automated machine and has been equated to a pen register by some courts,277 a computer server reveals far more information than a pen register.278 Because of the similarities between computers and other containers, the Fourth Amendment protections of containers should be instructive on how metadata is protected from unreasonable searches.


Using metadata created from this exchange of data, ISPs and advertisers can follow the user's activities online.279 By accessing metadata from these companies, the government could also see a person's movements online by seeing what websites a person accessed, when she accessed those websites, who she e-mailed, and other information gathered by

---

264 See supra notes 146-148.
265 United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010) (en banc). See also Bellia & Freiwald, supra note 219 (stating ISPs are not third parties).
266 See, e.g., Tokson, supra note 133, at 2131-32 (arguing that all Internet communication is similar to sending an e-mail).
267 Id. at 286. (referring to e-mail as the "technological scion of tangible mail").
268 See Tyson, supra note 112. ("All of the machines on the Internet are either servers or clients. . . . When you connect to [a website] to read a page, you are a user sitting at a client's machine. You are accessing the [website's] server. The server machine finds the page you requested and sends it to you.").
269 See Tokson, supra note 133, at 2134 (referring to search queries as "content" which receives Fourth Amendment protection); See also In re Application of the U.S. of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp.2d 45, 49-50 (D. Mass. 2005) (excluding from a warrant all metadata that contains search queries).
270 Tyson, supra note 112.
271 See supra note 116.
272 Growther, supra note 140, at 366 ("The third party doctrine was established prior to the digital age, and its advocates could not have fully contemplated society's heavy reliance on digitally stored information."). See also United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (arguing that the Court should reconsider the third-party doctrine because "it 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").
276 Id. at 742.
277 E.g., United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).
278 See supra notes 129-133.
279 See supra note 22.
third-party cookies. The Supreme Court has been wary of letting the government track the activities of a person without a warrant, especially when those movements are within a person’s home. The activities of a person online should be even more protected when the use of the Internet is within the curtilage of the home, which about 75% of Americans have a computer at home that they use to connect to the Internet. By allowing the government to view metadata of a computer, it would allow the government to peer within the curtilage and see what a person is doing within the privacy of his or her home. By examining metadata, the government is in essence viewing a container within the home, something that already has a reasonable expectation of privacy.

A warrantless search can also be seen as a trespass onto a person’s curtilage. Even without a physical entering of land, the governmental official is able to trespass onto the curtilage by using technology not within general public use. ISPs and Internet advertisers have the ability to extract and analyze metadata; however, the general public does not use these technologies.

In addition to the trespass in viewing the contents of a computer, there is a popular expectation of privacy in metadata held within a computer. There is a difference between what people think is anonymous and private online and what people think ought to be private. People expect, and are often willing, to reveal information to ISPs that they want to keep private from the government or other individuals. But this willingness does not dispel a person’s reasonable expectation of privacy results under the Katz analysis since that information is not being exposed to the public, but is being added to, not substituted for, the common-law trespassory test.”

See supra notes 119-125 and accompanying text.

See, e.g., United States v. Jones, 132 S. Ct. 945, 957 (Alito, J., concurring) (finding that using a GPS tracker on defendant’s vehicle without a warrant for four weeks was an unreasonable search); United States v. Karo, 468 U.S. 705 (1984) (holding that tracking to the inside of a defendant’s house was an unreasonable search).

File, supra note 105.

Compare United States v. Perrine, 518 F.3d 1196, 1199-1200 (2008) (upholding the constitutionality of using a court order to obtain metadata that disclosed the dates defendant had logged onto a Yahoo! account from his house), with United States v. Karo, 468 U.S. 705, 715 (1984) (excluding evidence gathered when “the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house.”). See also In re Application of the U. S. for an Order Directing a Provider of Elect. Commun’n Service to Disclose Records to the Gov’t, 620 F.3d 304, 320 (3d Cir. 2010) (Tashima, J., concurring) (holding that telephony metadata is protected because it allows the police to see a user’s location within the curtilage of their home).

See Karo, 468 U.S. 705.

Jones, 132 S. Ct. at 952 (majority opinion of Scalia, J.) (holding that for Fourth Amendment protection from unreasonable searches, the reasonable expectation of privacy test has been “added to, not substituted for, the common-law trespassory test.”); Id. at 955 (Sotomayor, J., concurring) (stating the trespassory test is the “irreducible constitutional minimum.”).

Kyllo v. United States, 533 U.S. 27, 40 (2001). See also Florida v. Jardines, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring) (stating that a drug detecting dog was a device not in general public use when used to explore within the curtilage of the home).

For example, Google requires vast amounts of computer memory to process their data. See Dean, supra note 116. This processing can require large physical spaces. See supra note 96. In comparison, thermal imaging cameras, which the Court in Kyllo determined were not in general public use, are now commercially available at less than $300. Daniel Terdiman, Heat Seeker: Meet the Thermal-Imaging Camera You Can Afford, Cnet, (Sept. 25, 2014, 9:00 AM), http://www.cnet.com/news/heat-seaker-thermal-imaging-camera-for-the-masses/ (stating that, for example, Google requires vast amounts of computer memory to process their data); See Dean, supra note 116 (noting that this processing can require large physical spaces); See supra note 96 (holding thermal imaging cameras, which the Court in Kyllo determined were not in general public use, are now commercially available at less than $300).

See supra notes 135-138 and text accompanying.

Raine, et. al., supra note 135.

Sylvain, supra note 23, at 492.
shared with automated machines.\textsuperscript{291} Furthermore, several popular Internet services make explicit in their terms of service that a user’s metadata will remain anonymous or aggregated if accessed by a third party.\textsuperscript{292}

3. Container Law and Smartphones

Even when a computer is not held within the curtilage, such as a smartphone, it still receives the same high level of Fourth Amendment protection that an opaque container would.\textsuperscript{293} Opaque containers are free from unreasonable governmental searches.\textsuperscript{294} The physical viewing of the data on a person’s smartphone by a police officer without a warrant or probable cause is already unconstitutional.\textsuperscript{295} The viewing of metadata without a warrant would also be similarly unconstitutional since metadata can reveal many of the same privacies of life that content data can.\textsuperscript{296} For example, metadata can reveal whom the person emails,\textsuperscript{297} the number of times and the durations of time spent on websites,\textsuperscript{298} and the person’s actual location.\textsuperscript{299}

Viewing metadata of a smartphone is also a nonvisual inspection of a container in an “exploratory manner.”\textsuperscript{300} Just like an officer who squeezes a bag to inspect its contents, inspecting the metadata of a smartphone reveals the contents of that smartphone without actually opening the phone and visually inspecting it.\textsuperscript{301} Metadata, by its definition, reveals information about the data contained in the computer.\textsuperscript{302} Since the content stored on the smartphone is protected,\textsuperscript{303} all information about that content should be similarly protected.\textsuperscript{304}

Even when the metadata is stored in an external source such as a computer server, the metadata is the contents of the smartphone that the person is keeping out of public view.\textsuperscript{305} Similar to using telephony metadata without a warrant to track a person’s whereabouts, viewing the metadata of a person’s smartphone tracks a person’s use of their phone and converts a seemingly private event into a public one.\textsuperscript{306} Similar to computers held within the home or briefcases carried on the person, smartphones

\begin{itemize}
  \item \textsuperscript{291} Tokson, supra note 104, at 632-36.
  \item \textsuperscript{292} See, e.g., Google Privacy Policy, supra note 120 (stating Google “may share aggregated, non-personally identifiable information publicly and with our partners—like publishers, advertisers or connected sites.”); Netflix Privacy Policy, supra note 16. (stating Netflix “may provide analysis of and information from or about our users in the aggregate or otherwise in anonymous form to partners, Service Providers and other third parties.”).
  \item \textsuperscript{293} Riley v. California, 134 S. Ct. 2473, 2489 (2014) (the amount of information a person carries in their phone is similar to having to “drag[ging] behind them a trunk of the sort held to require a warrant in Chadwick”); (citing United States v. Chadwick, 433 U.S. 1 (1977)).
  \item \textsuperscript{294} Robbins v. California, 453 U.S. 420, 427 (1981) (plurality opinion) (“[U]nless the container is such that its contents may be said to be in plain view, those contents are fully protected by the Fourth Amendment.”).
  \item \textsuperscript{295} Riley, 134 S. Ct. at 2495.
  \item \textsuperscript{296} See Richards, supra note 257, at 417 (noting that aggregated metadata can reveal personal information).
  \item \textsuperscript{297} E.g., United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (en banc).
  \item \textsuperscript{298} Contra United States v. Perrine, 518 F.3d 1196, 1199 (10th Cir. 2008).
  \item \textsuperscript{299} See, e.g., Google Privacy Policy, supra note 120 (“When you use a location-enabled Google service, we may collect and process information about your actual location. We use various technologies to determine location, IP address, GPS, and other sensors...”). See also United States v. Davis, 754 F.3d 1205 (11th Cir. 2014) (holding that obtaining a customer’s location using metadata obtained via court order is unconstitutional).
  \item \textsuperscript{300} See Bond v. United States, 529 U.S. 334 (2000).
  \item \textsuperscript{301} See id.
  \item \textsuperscript{302} See supra note 126.
  \item \textsuperscript{303} Riley v. California, 134 S. Ct. 2473 (2014).
  \item \textsuperscript{304} See Tokson, supra note 133, at 2170-71 (metadata that reveals the underlying content of Internet communications should be treated as the same as content).
  \item \textsuperscript{305} See Brenner, supra note 251, at 257-59.
  \item \textsuperscript{306} See Davis, 754 F.3d at 1216.
\end{itemize}
should be treated as containers. Conceptualizing both smartphones and computers will simplify the protections the Fourth Amendment provides.

C. Benefits of Container Framework

The benefits of using a presented analytic framework is two-fold. First, it gives clear Fourth Amendment protections for metadata in current technologies. Second, it provides a clear framework to analyze Fourth Amendment protections of future technologies.

1. Current Technologies

With container law guiding the Fourth Amendment protections of computers and phones, it simplifies the analysis for what metadata is protected under the Fourth Amendment. Treating computers as containers shifts the focus away from whether there is a reasonable expectation of privacy in evolving digital technologies, which many judges struggle with. By treating computers as containers, judges can begin to conceptualize warrantless viewing metadata as a trespass, either by using technology not in public use to look into a person’s curtilage or by viewing the contents of a personal computer in an exploratory manner. By treating viewing metadata as a trespass, it creates the default rule that there is a reasonable expectation of privacy in a person’s metadata.

Additionally, analyzing computers as containers avoids difficulties with the third-party doctrine. Courts and scholars have suggested several ways around the third-party doctrine in looking at digital privacy. By treating computers as containers, metadata gathered by ISPs and stored on servers is not treated as being revealed to a third party, but as being stored on the server under a contractual arrangement, analogous to a rented storage unit. These contracts can then alter a person’s reasonable expectation of privacy.

Because the metadata is being stored by a private party, the user’s reasonable expectation of privacy in metadata can be altered primarily based on the privacy agreements between the Internet user and the ISP. Because servers are automated machines, the metadata would be presumed to be protected as being reasonably private. If the server’s privacy agreement states that a user’s metadata will be held anonymously or will be shared only in aggregated form, such as Google’s Privacy

---

307 See supra Subsection IV.B.3.
308 See infra Subsection IV.C.1.
309 See infra Subsection IV.C.2.
310 See Crowther, supra note 140, at 356-57.
311 See supra Subsections IV.B.2-IV.B.3.
312 See United States v. Jones, 132 S. Ct. 945, 952 (2012) (“The Katz reasonable-expectation-of-privacy test has added to, not substituted for, the common-law trespassory test.”).
313 See, e.g., United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010) (en banc) (referring to ISPs as “intermediaries” and distinguishing them from the third-party doctrine); United States v. Graham, 796 F.3d 332, 333 (4th Cir. 2015) (stating that cell phone users do not “convey” their metadata to their service provider). See also, Brenner, supra note 251, at 266-68 (stating that transaction metadata is protected because of the “shared privacy” interest between users and ISPs).
314 See generally, Bellia & Freiwald, supra note 219.
316 See Crowther, supra note 140, at 353-55 (noting that terms of agreement alter a user’s reasonable expectation of privacy).
317 See Tokson, supra note 104, at 638.
318 See supra note 121 for examples.
Policy, then that metadata will be reasonably considered private, and thus protected from unreasonable searches. Conversely, if the ISP’s terms of use make clear that the metadata is not private, there would be no reasonable expectation of privacy.

This analytic framework is different than the ones currently being employed by circuit courts because it recognizes the realities of how privacy on the Internet works. The analysis, like the first category of courts, would find Fourth Amendment protections for contents stored communications. The analysis differs from the first category because it acknowledges that there is more than a privacy interest in e-mail contents and in cell phone location, but that the warrantless viewing of metadata is actually a trespass by viewing inside the person’s computer or phone.

The analysis differs from the second category of circuit courts by not using tenuous analogies of treating computer servers as persons or pen registers under the third-party doctrine. It instead treats metadata as stored within a container that the ISP and the user have a shared interest in because they have a contractual agreement akin to rental storage. The analysis recognizes that the government cannot view inside this container using technology not in general public use or view inside in any exploratory manner without a showing the search is reasonable.

Finally, the analysis differs from the third category of courts by avoiding difficult questions as to what metadata is content and what is not. The analysis treats all metadata as content since metadata is contained within a computer just like any other content that is protected. Fourth Amendment protections would not be based on magistrate discretion, but would apply to metadata that the ISP and the user have agreed is private. In addition to having implications on Fourth Amendment protection for current technologies, the same rationales can apply to future technologies.

2. Future Technologies

While it is difficult to predict how future technologies will affect the reasonable expectation of privacy, it is clear that computers and the Internet will play a crucial role in determining privacy expectation. With technology rapidly changing, a clear line of analysis for reasonable expectations of privacy will be needed. Scholars have articulated a need for legislative initiative in clearly defining privacy interests in technologies. Additionally, as Justice Sotomayor has noted, “A legislative body is well situated to gauge changing public attitudes, to

319 Google Privacy Policy, supra note 120.
320 Supra Section II.A.
321 See Crowther, supra note 142, at 357 (“judges’ technological inexperience and misunderstandings threaten to further undermine digital privacy interests.”).
322 See United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (en banc) (finding SCA 2703(d) unconstitutional in the context of e-mails); United States v. Davis, 754 F.3d 1205, 1217 (finding SCA 2703(d) unconstitutional in the context of cell phone location information).
323 Supra Subsection IV.B.2-IV.B.3.
324 Supra Section II.B.
325 See Kerr, supra note 38, at 875-76 (“Judges struggle to understand even the basic facts of [digital] technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension.”).
326 Supra Subsection IV.B.1.
draw detailed lines, and to balance privacy and public safety in a comprehensive way.\footnote{United States v. Jones, 132 S. Ct. 945, 964 (2012) (Sotomayor, J., concurring).} While a legislative scheme is preferable, if the legislature is unwilling or incapable of keeping up with technological changes, treating computers as containers will provide a useful base to analyze future technologies.

In addition, applying Fourth Amendment protections of containers to new technologies will have practical benefits. By treating a user’s metadata as shared by user and the ISP, it will discourage users from hiding or eliminating their metadata in order to feel anonymous online.\footnote{Id. (Fifty-nine percent of Americans do not believe it is possible to be completely anonymous online); Mozilla, supra note 125 (stating it is possible to access the Internet without accumulating metadata, however it then becomes difficult to use many Internet services, such as e-mail).} While it is currently difficult to use the Internet without creating metadata,\footnote{See Rosen, supra note 124, at 196-224 (arguing the importance of anonymity online); Raine et al., supra note 135 (Forty-one percent of Internet users already take steps to disable or remove cookies from their computer).} future technologies may make anonymous Internet use practical.\footnote{See Rosen, supra note 124, at 198-200.} Avoiding anonymous use on the Internet has a two-fold advantage.

First, accumulating, aggregating, and selling metadata is how many successful Internet companies operate.\footnote{See, e.g., United States v. Lifshitz, 369 F.3d 173, 193 (7th Cir. 2004) (searching the defendant’s computer without a warrant was reasonable since the defendant was on probation and part of the agreement was to allow monitoring).} By recognizing metadata as being private content within a user’s computer, users could be more willing to accumulate metadata and share it with ISPs.\footnote{Rosen, supra note 124, 174 (one encryption service “destroys all documents and logs on its central server within twenty-four hours, to avoid subpoenas.”).} The sharing of metadata will help improve the economy by improving the online market-place.\footnote{See Even, supra note 149 (stating that the market for analyzing metadata is expected to grow to $16.9 billion in 2015).} When users have a privacy interest in their metadata, they will they be more willing to share more of their metadata.\footnote{See Kerr, supra note 192, at 1029-31. (arguing that there exists Fourth Amendment protections for content on the Internet but they can be waived if shared publicly).}

Second, if persons do not accumulate metadata, the information it reveals could not be viewed by the government in the event it is the product of a reasonable search.\footnote{Rosen, supra note 124, 174 (one encryption service “destroys all documents and logs on its central server within twenty-four hours, to avoid subpoenas.”).} The government will not be able to view the metadata because it simply would not exist.\footnote{See, e.g., California v. Ciraolo, 476 U.S. 207, 209 (1986) (defendant kept marijuana plants in his house).} Similar to how persons maintain incriminating material within their property,\footnote{See Rosen, supra note 124, at 173-78.} treating metadata as contained within a personal computer will lead persons to accumulate metadata that could be useful to prosecute them. Treating metadata as something exposed to the public would lead criminals to be more protective of their metadata and destroy useful evidence.

D. Shortcomings of Analytical Framework

Treating metadata as contained within a computer does not address the issue of contents that are shared with other individuals using the Internet.\footnote{See supra notes 22-23.} For example, using container law would not address the reasonable expectation of privacy for contents stored using
“cloud computing” or using peer-to-peer file sharing. The third-party doctrine would have more of an impact on shared content than on metadata. However, content could still be protected under a similar framework if the server that the content is on maintains a clear privacy policy as to who may view the content.

Additionally, the analytical framework may become unworkable if technology that is used to access and analyze metadata becomes in general public use or if people no longer believe things done on the Internet should be private. As technology changes, the reasonable expectation of privacy using technology will likely change as well. This change could lead to inconsistent rulings similar to those currently splitting lower courts. However, this inconsistency is more a product of the varying applications of the third-party doctrine and the reasonable expectation of privacy test. Using container law as a guide simplifies the courts’ analysis of whether there is a reasonable expectation of privacy by using well-established concepts of Fourth Amendment jurisprudence.

**CONCLUSION**

The Internet started out as computer protocols and has evolved into an entire digital world. It has revolutionized the world and altered American’s concepts of privacy. Courts have the problem of reflecting these changing concepts of privacy when they apply Fourth Amendment protections to metadata. By treating computers as containers under the Fourth Amendment and the metadata as content contained within those containers, a simplified analysis can be used to establish Fourth Amendment protections for metadata.

A computer may be just a box, but the contents of that box are often very private. In order to protect those intimate contents, all contents have to be protected equally. Exposing a person’s metadata may turn their computer into a Pandora’s box and reveal all their secrets, to terrifying effect.
ABOUT THE AUTHOR

Christopher Michels is a 2016 graduate of the Michigan State University College of Law. He was an associate editor of the Michigan State Law Review as well as the champion of the Chicago Bar Association’s Moot Court Competition. He would like to thank Prof. Catherine Grosso for her guidance as well as his editors, Kent Spark and Benjamin Krinke.