Boston College Law Review

Volume 59 | Issue 3 Article 7

3-26-2018

"A Search Is a Search": Scanning a Credit, Debit, or Gift Card Is a Search Under the Fourth Amendment

John A. LeBlanc
Boston College Law School, john.leblanc.2@bc.edu

"A SEARCH IS A SEARCH": SCANNING A CREDIT, DEBIT, OR GIFT CARD IS A SEARCH UNDER THE FOURTH AMENDMENT

Abstract: On May 18, 2017, the U.S. Court of Appeals for the First Circuit, in *United States v. Hillaire*, joined the Fifth, Sixth, and Eighth circuits in holding that the government's act of scanning the magnetic stripes of lawfully seized credit, debit, or gift cards to access the information encoded therein is not a search within the meaning of the Fourth Amendment. In each case, the courts concluded that an individual is precluded from claiming a reasonable expectation of privacy in the electronic information encoded on a card's magnetic stripe. This Note provides an overview of how Fourth Amendment jurisprudence has evolved in light of advances in technology and introduces the current standard by which courts determine whether governmental conduct amounts to a Fourth Amendment search. This Note goes on to argue that both existing precedent on Fourth Amendment search determinations and the technological realities of the modern world should allow an individual to claim a reasonable expectation of privacy in this information. Accordingly, scanning the magnetic stripe of a card to access its encoded information should be considered a Fourth Amendment search.

INTRODUCTION

Millions of Americans fall victim to acts of identity theft each year.[1] In 2016 alone, the number of identity theft victims totaled an estimated 15.4 million Americans.[2] Notably, many of these crimes involved the theft of credit card account information.[3] Once stolen, credit or debit card account infor-

[1] *See Identity Theft and Data Security*, FED. TRADE COMM'N., https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security [https://perma.cc/4AGJ-6SBF] (illustrating the frequency of identity theft complaints each year)*; see also Facts + Statistics: Identity Theft and Crime*, INS. INFO. INSTIT., http://www.iii.org/fact-statistic/identity-theft-and-cybercrime [https://perma.cc/X74J-R9MY] (reporting recent identity theft crime statistics); Martyn Williams, *One in Every 14 Americans Fell Victim to Identity Theft Last Year*, PCWORLD (Sept. 27, 2015, 12:18 PM), http://www.pcworld.com/article/2986810/security/identity-theft-hit-7-of-us-population-last-year.html [https://perma.cc/6AQ4-6SBP] (describing 2014 identity theft statistics).

[2] Herb Weisbaum, *Identity Fraud Hits Record Number of Americans in 2016*, NBC NEWS (Feb. 2, 2017, 7:21 AM), https://www.nbcnews.com/business/consumer/identity-fraud-hits-record-number-americans-2016-n715756 [https://perma.cc/P7FC-HJKK] (describing a recent study performed by Javelin Strategy & Research that determined how many Americans were victims of identity theft in 2016).

[3] *Id.* Identity thieves routinely gain access to consumer account information by hacking or otherwise breaching the consumer financial records of large businesses. *See* Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUT. & HIGH

mation can be used in a variety of ways to inflict substantial pecuniary harm on the account holder.[4] One method that perpetrators use to exploit stolen account information involves re-encoding the magnetic stripes of existing or counterfeit credit, debit, or gift cards (collectively, "cards") with the stolen account information.[5] Once the magnetic stripe on the back of any such card is re-encoded with stolen account information, the card can be used to make purchases that will in turn be charged to the victim's account.[6]

Typically, the front and back of a card is embossed with the card holder's first and last name, the card number, the expiration date, and the card security

---

TECH. L.J. 375, 378–79 (2009) (listing large chain retailers that suffered data breaches that exposed consumer debit and credit card account information to identity thieves and explaining how the compromised information is used to commit fraud). These types of large scale breaches are often highly publicized. *See, e.g.*, Kara Brandeisky, *Anthem Health Insurance Was Hacked. Here's What Customers Need to Know*, MONEY (Feb. 5, 2015), http://time.com/money/3697026/anthem-data-breach-social-security/ [https://perma.cc/N896-3A6A] (detailing the hack of approximately 80 million Anthem Health Insurance customers); *CVS Alerts Photo Site Users After Confirming July Data Breach*, NBC NEWS (Sept. 11, 2015, 5:47 PM), http://www.nbcnews.com/tech/security/cvs-alerts-photo-site-users-after-confirming-july-data-breach-n426126 [https://perma.cc/M2PU-UJEV] (describing the data breaches that exposed the financial information of CVS Health-Corp, Rite-Aid, Costco, and Wal-Mart Canada customers); Gregory Wallace, *Target Credit Card Hack: What You Need to Know*, CNN (Dec. 23, 2013, 11:43 AM), http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/ [https://perma.cc/RYH4-9MT5] (recounting how the information of over 40 million credit and debit card accounts were stolen from Target Corporation).

[4] *See* Olivia DeGennaro, *How Thieves Can Access Your Credit Card Information Without Ever Touching Your Card*, NBC RENO (July 27, 2016), http://mynews4.com/news/local/how-thieves-can-access-your-credit-card-information-without-ever-touching-your-card [https://perma.cc/3XXX-JANC] (describing the consequences associated with having one's credit card information stolen); *Identity Theft & Credit Card Fraud—How to Protect Yourself*, WALL STREET J., http://guides.wsj.com/personal-finance/credit/how-to-protect-yourself-from-identity-theft/ [https://perma.cc/GZT8-JSGC] (explaining that the risks associated with the exposure of one's credit card account information may include a thief opening new accounts, taking out loans in the victim's name, or using the information to make purchases); Theresa Payton, *What Really Happens After Your Credit Card Is Stolen*, ABC NEWS (Sept. 20, 2014, 6:26 AM), http://abcnews.go.com/Business/credit-card-stolen/story?id=25633648 [https://perma.cc/TRR5-2B6U] (explaining how identity thieves can use stolen credit card account information to sell the information to other criminals, use the information to make purchases, re-encode the account information onto fraudulent cards, or make purchases and then sell the items for cash). *But see* Peretti, *supra* note 3, at 379) (describing how a victim's monetary liability due to unauthorized credit or debit card use may be limited by federal law).

[5] United States v. Turner, 839 F.3d 429, 435 (5th Cir. 2016) (describing the need for a specific piece of equipment to re-encode the magnetic stripe of a credit card); Jay S. Albanese, *Fraud: The Characteristic Crime of the Twenty-First Century*, *in* INTELLECTUAL PROPERTY THEFT AND FRAUD: COMBATING PIRACY 1, 6 (Jay S. Albanese ed., 2007) (describing the process of re-encoding a credit or debit card with stolen account information); Byron Acohido & Jon Swartz, *Thieves Turn Simple Strip into Cutting-Edge Tool*, USA TODAY (July 31, 2007, 11:57 PM), http://usatoday30.usatoday.com/tech/news/computersecurity/infotheft/2007-07-31-gift-cards_N.htm [https://perma.cc/N292-FZNX] (discussing the method by which identity thieves re-encode the magnetic stripe of gift cards with stolen credit card account information by using a "'magstripe reader-writer'").

[6] *See* United States v. Alabi, 943 F. Supp. 2d 1201, 1212 (D. N.M. 2013) (explaining that when a fraudulent card is used, the purchase or withdrawal will be charged to the victim's account).

code ("CSC code").[7] The same information will ordinarily be encoded on the magnetic stripe of the card as well.[8] A card's magnetic stripe, however, can be manually re-encoded to store other information, such as a victim's stolen card number.[9] Because a fraudulent card appears authentic on its face, its fraudulence typically cannot be recognized by anyone, including government officials, unless and until it is scanned by a magnetic card reader.[10] Once scanned, the government is able to compare the information embossed on the front and back of the seized card with the electronic information encoded on the card's magnetic stripe.[11] If the two sets of information differ, the card may be deemed fraudulent.[12]

As this method of identity theft has become more prevalent over the last several years, courts have increasingly been tasked with answering the critical question of whether or not the government's act of scanning a seized card is a search within the meaning of the Fourth Amendment.[13] Within the last three years, each in a case of first impression, the U.S. Courts of Appeals for the First, Fifth, Sixth, and Eighth Circuits have held that it is not a search.[14] Indeed, every federal court to have addressed the issue has ruled that scanning a card is not a Fourth Amendment search.[15]

---

[7] United States v. Bah, 794 F.3d 617, 623 (6th Cir. 2015), *cert. denied sub nom.* Harvey v. United States, 136 S. Ct. 561 (2015); *see also Turner*, 839 F.3d at 435 (describing electronic information contained within the magnetic stripe of gift cards); United States v. DE L'Isle, 825 F.3d 426, 430 (8th Cir. 2016) (same).

[8] *Bah*, 794 F.3d at 623; *see also Turner*, 839 F.3d at 435; *DE L'Isle*, 825 F.3d at 430.

[9] *Alabi*, 943 F. Supp. 2d at 1212 (detailing trial testimony that explained that by using a specific device, identity thieves are able to re-encode the magnetic stripes of fraudulent cards with a victim's actual account information).

[10] *See Turner*, 839 F.3d at 431–32 (describing how the seized cards were revealed to be fraudulent only upon scanning them); *DE L'Isle*, 825 F.3d at 429 (explaining that charges were brought only after scans of the confiscated cards revealed them to be fraudulent).

[11] *See Turner*, 839 F.3d at 431–32; *DE L'Isle*, 825 F.3d at 429; *see also Bah*, 794 F.3d at 623; *Alabi*, 943 F. Supp. 2d at 1212.

[12] *See Bah*, 794 F.3d at 623 (chronicling how the suspects were arrested after scans of seized cards revealed the account information encoded on the magnetic stripes to be different from the account information embossed on the front of the cards); *see also Turner*, 839 F.3d at 431–32 (describing how the seized cards were revealed to be fraudulent only upon scanning them); *DE L'Isle*, 825 F.3d at 429 (explaining that charges were brought only after scans of the confiscated cards revealed them to be fraudulent).

[13] *See, e.g.*, *Turner*, 839 F.3d at 431; *DE L'Isle*, 825 F.3d at 430; *Bah*, 794 F.3d at 621; *Alabi*, 943 F. Supp. 2d at 1207.

[14] *See* United States v. Hillaire, 857 F.3d 128, 130 (1st Cir. 2017); *Turner*, 839 F.3d at 431; *DE L'Isle*, 825 F.3d at 430; *Bah*, 794 F.3d at 621.

[15] *See, e.g.*, *Hillaire*, 857 F.3d at 130; *Turner*, 839 F.3d at 431; *DE L'Isle*, 825 F.3d at 430; *Bah*, 794 F.3d at 621; United States v. DE L'Isle, No. 4:14-CR-3089, 2014 WL 5431349, at *4 (D. Neb. Oct. 24, 2014); *Alabi*, 943 F. Supp. 2d at 1207; Report and Recommendation on Defendant's Motion to Suppress, United States v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *10 (S.D. Fla. Oct. 24, 2009).

This Note will discuss how these recent decisions have analyzed the Fourth Amendment implications of scanning the magnetic stripe of a card to access the electronic data encoded therein.[16] Part I provides an overview of how Fourth Amendment jurisprudence has evolved in light of advances in technology and introduces the current standard that courts use to determine whether governmental conduct amounts to a Fourth Amendment search.[17] This part goes on to introduce the U.S. Courts of Appeals' recent foray into the constitutionality of scanning cards without a warrant.[18] Part II examines the reasoning underlying the Sixth, Eighth, and Fifth Circuits' conclusions that these scans are not Fourth Amendment searches.[19] Part III argues that, notwithstanding what the circuits have held in recent years, scanning the magnetic stripe of a lawfully seized card should be considered a search under the Fourth Amendment.[20]

I. THE FOURTH AMENDMENT'S ADAPTION TO THE MODERN WORLD

The Fourth Amendment of the U.S. Constitution ensures that American citizens are protected from unreasonable searches and seizures by the government.[21] The Amendment reigns in governmental conduct and seeks to safeguard privacy interests.[22] Accordingly, a court's initial determination of whether or not governmental conduct amounts to a Fourth Amendment search is de-

---

[16] *See infra* notes 95–150 and accompanying text.

[17] *See infra* notes 21–90 and accompanying text.

[18] *See infra* notes 91–94 and accompanying text.

[19] *See infra* notes 95–150 and accompanying text. Although the First Circuit in *Hillaire* concluded that scanning a card was not a search, the court did not provide its own reasoning or otherwise thoroughly analyze the issue. *Hillaire*, 857 F.3d at 130. Instead, the court simply quoted the reasoning of the *Bah* and *DE L'Isle* courts in a brief footnote. *Id.* at 130 n.3. The only other First Circuit decision addressing this issue similarly did not include a thoroughly detailed reasoning behind the decision. *See* United States v. Ramdihall, 859 F.3d 80, 95 (1st Cir. 2017) (holding that the appellant had waived any argument that scanning seized credit cards amounted to a Fourth Amendment search because the appellant did not assert that he had a reasonable expectation of privacy in the encoded information on appeal). Accordingly, only the opinions of the Fifth, Sixth, and Eighth Circuits will be analyzed in this Note. *See infra* notes 106–137 (analyzing the *Bah*, *DE L'Isle*, and *Turner* decisions).

[20] *See infra* notes 151–213 and accompanying text. As with Part II of this Note, the First Circuit's decision in *Hillaire* will not be analyzed in Part III. *See supra* note 19.

[21] 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, and no warrants shall issue, but upon probable cause . . . ."); *see* Riley v. California, 134 S. Ct. 2473, 2482–83 (2014) (summarizing Fourth Amendment jurisprudence); Katz v. United States, 389 U.S. 347, 350–51 (1967) (discussing the scope of what is protected by the Fourth Amendment); John Potapchuk, Note, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1412–13 (2016) (discussing the scope of Fourth Amendment protections).

[22] *See* Schneider v. Smith, 390 U.S. 17, 25 (1968) (noting that the Bill of Rights was created as a way to "take government off the backs of people"); Camara v. Mun. Court of City & Cty. of S.F., 387 U.S. 523, 528 (1967) (noting that the "basic purpose" of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by governmental officials").

terminative of whether or not the full weight of the Amendment's protections will apply.[23]

Although Fourth Amendment searches were first thought to occur only when the government physically trespassed onto "a constitutionally protected area," advancements in technology over the latter half of the twentieth century forced the U.S. Supreme Court to revisit that approach.[24] Section A discusses the origins and evolution of Fourth Amendment search determinations.[25] Section B provides an overview of specific instances where courts consistently hold that governmental conduct does not amount to a Fourth Amendment search.[26] Section C discusses the U.S. Supreme Court's 2014 decision in *Riley v. California*, which addressed privacy interests that arise with certain digital storage devices under the Fourth Amendment.[27] This section goes on to introduce the U.S. Courts' of Appeals recent foray into the constitutionality of scanning cards without a warrant.[28]

A. One Size Does Not Fit All: The Origins and Evolution of Fourth Amendment Search Determinations

As with each of the first ten amendments to the U.S. Constitution, the Founders constructed the Fourth Amendment to protect against the abusive governmental overreach that colonial Americans were subjected to prior to the American Revolution.[29] In order to guard against this type of governmental

---

[23] *See* Allison M. Lucier, *You Can Judge a Container by Its Cover: The Single-Purpose Container Exception and the Fourth Amendment*, 76 U. CHI. L. REV. 1809, 1811 (2009) (describing how courts adjudicate Fourth Amendment disputes).

[24] *See* United States v. Jones, 565 U.S. 400, 404–06, 408 (2012) (citing United States v. Knotts, 460 U.S. 276, 286 (1983)) (explaining the evolution of the U.S. Supreme Court's approach to Fourth Amendment search determinations); *Katz*, 389 U.S. at 358–59 (adopting a new approach to determining whether a search had occurred under the Fourth Amendment); *see also infra* notes 138–150 and accompanying text (describing *Katz*'s adoption of a new approach to Fourth Amendment search determinations).

[25] *See infra* notes 29–51 and accompanying text.

[26] *See infra* notes 52–79 and accompanying text.

[27] *See infra* notes 80–90 and accompanying text.

[28] *See infra* notes 91–94 and accompanying text.

[29] *See Schneider*, 390 U.S. at 25 (describing the purpose of the Bill of Rights); *Camara*, 387 U.S. at 528 (describing the purpose of the Fourth Amendment); Nelson v. County of Los Angeles, 362 U.S. 1, 10 (1960) (Black, J., dissenting) (noting that the Bill of Rights was created "to protect individual liberty against governmental procedures that the Framers thought should not be used"). The Fourth Amendment was a direct response to the Founders' contempt for the British soldiers' habit of "rummaging" through colonial homes and businesses without justification to do so. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); *see Riley*, 134 S. Ct. at 2494 (explaining that the impetus for the Fourth Amendment was the displeasure the colonial Americans had with the British government's utilization of "writs of assistance" to authorize "unrestrained search[es] for evidence of criminal activity"); Stanford v. Texas, 379 U.S. 476, 481–82 (1965) (describing the origins of the Fourth Amendment and noting that it was "most immediately the product of contemporary revulsion against a regime of writs of assistance" that empowered investigators with "blanket authority to search where

conduct, when a Fourth Amendment search is deemed to have occurred, the Fourth Amendment requires the government to prove that the search was reasonable.[30] To meet this threshold of reasonableness, the government is typically required to obtain a search warrant.[31] In the absence of a warrant, however, a Fourth Amendment search may still be reasonable if the search falls within one of the several exceptions to the warrant requirement.[32]

In most cases, when an object or item is lawfully seized by the government, the government need not concern itself with any further Fourth Amendment protections.[33] As the Fifth Circuit has articulated, this is the case for objects such as firearms.[34] Once seized, the government may examine the weap-

---

they pleased"); Boyd v. United States, 116 U.S. 616, 624–65 (1886) (quoting early colonial opinions on writs of assistance).

[30] U.S. CONST. amend. IV; *Camara*, 387 U.S. at 528 (noting that the Fourth Amendment "safeguard[s] the privacy and security of individuals against arbitrary invasions by governmental officials"); Lucier, *supra* note 23, at 1809 (noting that "the Fourth Amendment requires that all searches be reasonable").

[31] Lucier, *supra* note 23, at 1809; *see Riley*, 134 S. Ct. at 2482 (finding that "[o]ur cases have determined that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant'") (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)); Mincey v. Arizona, 437 U.S. 385, 393–94 (1978) (finding that "warrants are generally required to search a person's home or his person"); *Coolidge*, 403 U.S. at 454–55 (explaining that in general, searches performed by law enforcement without the prior authorization of a judge are violative of the Fourth Amendment). *But see* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 318 (2012) (explaining that courts may also deem a warrantless search to be reasonable if the government's interest in searching the object "outweigh[s]" the individual's privacy interest in the object being searched).

[32] *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (explaining that the warrant requirement has exceptions); Flippo v. West Virginia, 528 U.S. 11, 13 (1999) (noting that searches performed without a warrant are "invalid unless [they] fall[] within one of the narrow and well-delineated exceptions to the warrant requirement"); *Katz*, 389 U.S. at 357 (describing "[s]earches conducted outside the judicial process, without prior approval by judge or magistrate" as "*per se* unreasonable under the Fourth Amendment" unless they fall within a recognized exception to the warrant requirement); *see also* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.1(b) (5th ed. 2012) (describing exceptions to the warrant requirement); Alexander Porter, Note, *"Time Works Changes": Modernizing Fourth Amendment Law to Protect Cell Site Location Information*, 57 B.C. L. REV. 1781, 1786 (2016) (explaining the existence of exceptions to the warrant requirement). Notable exceptions to the warrant requirement include searches or seizures that are consented to by the individual whose person or property is subject to the search, searches conducted incident to a lawful arrest, or when evidence is in plain view of law enforcement. *See* John M.A. DiPippa, *Is the Fourth Amendment Obsolete? Restating the Fourth Amendment in Functional Terms*, 22 GONZ. L. REV. 483, 487 n.20 (1987) (listing the exceptions to the warrant requirement). Given the rights that are at stake when a warrant is not required, each exception is narrowly tailored and subject to careful analysis. *See, e.g.*, Texas v. Brown, 460 U.S. 730, 736–38 (1983) (describing the threshold for determining whether a warrant exception exists for evidence in plain view of law enforcement); Schneckloth v. Bustamonte, 412 U.S. 218, 230–33 (1973) (discussing the standard for determining whether the consent exception to the warrant requirement was met)*; infra* note 85 and accompanying text (discussing the search incident to arrest exception of the warrant requirement).

[33] *Turner*, 839 F.3d at 434 (noting that "[o]nce seized, most items do not give rise to a separate Fourth Amendment search inquiry").

[34] *Id.*

on without infringing on any privacy interests because the only privacy interest at stake is in the weapon itself.[35] Other objects or items that are lawfully seized, however, may retain Fourth Amendment protections over their contents when such contents are not visible to the naked eye.[36] For example, an individual retains Fourth Amendment protections in the contents of a seized wallet or suitcase.[37] For a search of these seized items to be reasonable under the Fourth Amendment, the government is typically required to either obtain a warrant or prove that the search falls within one of the exceptions to the warrant requirement.[38] This is true even of certain objects that contain digital data.[39]

Given the limitations that the Fourth Amendment's reasonableness requirement imposes on the government, a reviewing court's threshold determination of whether or not a Fourth Amendment search occurred is critical to each case.[40] Because the driving force behind the Fourth Amendment was the fear of physical trespass by the government, Fourth Amendment search determinations traditionally focused on whether or not the government had physically encroached upon a person or place.[41] As technology evolved, however,

---

[35] *See id.* (describing that "[t]he evidentiary value" of an object like a firearm lies "i[n] the object itself, so seizing them is all law enforcement needs to do").

[36] *Id.*; *see also* United States v. Place, 462 U.S. 696, 700–01 (1983) (discussing privacy interests in the contents of objects that contain other items); United States v. Ross, 456 U.S. 798, 822–23 (1982) (noting that the Fourth Amendment protects containers that "conceal[] [their] contents from plain view"). One exception to this rule is when the object is a "single-purpose container." *See* United States v. Eschweiler, 745 F.2d 435, 440 (7th Cir. 1984) (holding that a privacy interest does not exist in the contents of a container when the nature of said contents can be determined just by looking at the container); Lucier, *supra* note 23, at 1817–19 (describing single-purpose containers and compiling relevant case law on the issue). The contents of these containers are apparent just by looking at the container itself and therefore do not give rise to a separate privacy interest. *Eschweiler*, 745 F.2d at 440.

[37] *See Turner*, 839 F.3d at 434 (describing separate privacy interests in contents of a suitcase); United States v. Rivera-Padilla, 365 F. App'x 343, 345–46 (3d Cir. 2010) (holding a warrantless search of a closed wallet to be an unreasonable search under the Fourth Amendment).

[38] *Turner*, 839 F.3d at 434.

[39] *Id.*; *see also Riley*, 134 S. Ct. at 2489–90 (holding a warrantless search of a cell phone to be unreasonable under the Fourth Amendment).

[40] *See* Lucier, *supra* note 23, at 1811 (noting that "[a]s a threshold question, courts must first determine whether a 'search' or 'seizure' occurred").

[41] *See* Olmstead v. United States, 277 U.S. 438, 461–65 (1928) (holding that because there was no physical trespass, there was no Fourth Amendment search); *see also Jones*, 565 U.S. at 404–06 (discussing the U.S. Supreme Court's history of interpreting the Fourth Amendment to protect against "government trespass upon areas ('persons, houses, papers, and effects') [the Fourth Amendment] enumerates"); Kyllo v. United States, 533 U.S. 27, 31–32 (2001) (describing the traditional approach to Fourth Amendment search determinations until the mid-twentieth century); *Turner*, 839 F.3d at 434 (discussing how the Fourth Amendment is typically violated when "the government physically intrudes on a constitutionally protected area"); Lawrence Rosenthal, *The Court After Scalia: Fourth Amendment Jurisprudence at a Crossroads*, SCOTUSBLOG (Sept. 9, 2016, 5:31 PM), http://www.scotusblog.com/2016/09/the-court-after-scalia-fourth-amendment-jurisprudence-at-a-crossroads/ [https://perma.cc/8DZV-VVFX] (describing Fourth Amendment originalism). Under this approach, the Fourth Amendment was thought to be violated only when the government physically trespassed

the traditional approach to Fourth Amendment search determinations risked rendering certain privacy interests unprotected.[42] In response to this risk, in 1967, in *Katz v. United States,* the U.S. Supreme Court set forth a more "pragmatic" approach.[43]

In *Katz*, the Court held that the government's act of wiretapping a public telephone booth was a Fourth Amendment search.[44] In so holding, the Court eschewed an application of the physical trespass approach in favor of an approach that considered an individual's expectation of privacy in the object or item being searched.[45] Justice Harlan articulated what has come to be known as the *Katz* standard in his concurrence, stating that a Fourth Amendment search occurs when a person has a reasonable expectation of privacy in the

---

against a person or tangible property without a warrant. *See Jones*, 565 U.S. at 404–05 (describing a trespass-based approach to Fourth Amendment search determinations); Porter, *supra* note 32, at 1787 (describing the trespass-based origins of Fourth Amendment search determinations).

[42] *See Jones*, 565 U.S. at 421–22 (Alito, J., concurring) (discussing critiques to the trespass-based approach); *Kyllo*, 533 U.S. at 33–35 (holding that the government's use of thermal imaging on a house to determine if there were people inside constituted a search under the Fourth Amendment because, although there was no physical trespass, to hold otherwise would "leave the [suspect] at the mercy of advancing technology"); *Katz*, 389 U.S. at 358–59 (noting that although electronic surveillance did not involve physical trespass, there was still an unreasonable search under the Fourth Amendment); *see also Turner*, 839 F.3d at 434 (describing how the majority of Fourth Amendment violations involving technology do not involve a physical trespass).

[43] *See Jones*, 565 U.S. at 405–06 (explaining the Supreme Court's break from the traditional "property-based approach" to Fourth Amendment search determinations); Porter, *supra* note 32, at 1787–88 (describing the Supreme Court's evolution from the trespass-based approach to Fourth Amendment search determinations); Rosenthal, *supra* note 41 (describing the "pragmatic" approach to the Fourth Amendment taken by the Court in *Katz v. United States*).

[44] *Katz*, 389 U.S. at 358–59. Although the act of wiretapping a public phone booth may not have constituted a search under the traditional trespass-based theory, the *Katz* Court expanded Fourth Amendment protections to cover searches that may not involve a "physical intrusion" on a person or place. *Id.* at 353; *see also Jones*, 565 U.S. at 421–22 (Alito, J., concurring) (explaining that *Katz* abandoned the "old approach" by disposing of the requirement of a physical trespass to find the Fourth Amendment had been infringed). As justification for doing so, the *Katz* Court reasoned that the traditional approach, as articulated in 1928 in *Olmstead v. United States* and in 1942 in *Goldman v. United States*, had been "so eroded by our subsequent decisions" that they could "no longer be regarded as controlling." *Katz*, 389 U.S. at 353 (citing Goldman v. United States, 316 U.S. 129, 134–36 (1942) and *Olmstead*, 277 U.S. at 457, 464, 466).

[45] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see Jones*, 565 U.S. at 421–22 (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)) (acknowledging that the Fourth Amendment can be violated when a government search "violates a person's 'reasonable expectation of privacy'"); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 21 (2015) (describing Fourth Amendment search determinations under the *Katz* standard); Potapchuk, *supra* note 21, at 1412–13 (discussing the *Katz* standard). The new approach set forth in *Katz* did not abolish the trespass-based approach to search determinations. *See Jones*, 565 U.S. at 409 (finding that "the *Katz* reasonable-expectation-of-privacy test has been *added to, but not substituted for,* the common-law trespassory test") (emphasis added). Courts remain free to apply either test depending on the circumstances of the case. *See id.* at 409–11; *see also* LAFAVE, *supra* note 32, at § 2.1(e) (noting that the trespass theory is an "alternate theory" to the *Katz* expectation-of-privacy test).

object or item being searched.[46] Accordingly, an analysis under the *Katz* standard requires both subjective and objective inquiries into an individual's expectation of privacy.[47]

Under the *Katz* standard, an individual must first demonstrate that he or she had an actual—i.e. subjective—expectation of privacy in the object or item that has been searched.[48] A reviewing court must then determine if the individual's subjective expectation of privacy was reasonable under an objective standard.[49] This objective standard requires the expectation of privacy to be one that "society is prepared to recognize as reasonable."[50] If both of these prongs are met, the governmental conduct constitutes a Fourth Amendment search.[51]

B. In the Interest of Clarity: Limitations on When an Individual May Claim a Reasonable Expectation of Privacy

The objective prong of the *Katz* analysis tasks courts with ultimately deciding what is and is not reasonable in light of societal expectations of privacy.[52] Though far from a mechanical or scientific analysis, the U.S. Supreme

---

[46] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also Turner*, 839 F.3d at 434 (articulating the *Katz* standard); *DE L'Isle*, 825 F.3d at 431 (same). Applying this analysis to the case before the *Katz* Court, Justice Harlan concluded that an individual would have had a reasonable expectation of privacy upon entering a phone booth to make a phone call. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring) ("[O]ne who occupies [a public telephone booth] . . . shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that his conversation is not being intercepted.") (citations omitted).

[47] *See Katz*, 389 U.S. at 361–62; *DE L'Isle*, 825 F.3d at 432 (acknowledging that the *Katz* analysis requires proof of both a "subjective" and "objective" expectation of privacy); Huff v. Spaw, 794 F.3d 543, 549 (6th Cir. 2015) (noting that "[c]ourts generally refer to *Katz*'s reasonable-expectation test as having a subjective part and an objective part").

[48] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *DE L'Isle*, 825 F.3d at 432; Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113 (2015). In many cases, reviewing courts will either assume that this prong is met or avoid the subjective prong analysis altogether. *See, e.g.*, *DE L'Isle*, 825 F.3d at 432 (assuming the existence of an actual expectation of privacy in order to address the second prong of the *Katz* analysis); *Bah*, 794 F.3d at 630 n.9 (assuming the existence of an actual expectation of privacy for purposes of the appeal despite noting reservations about whether such an expectation existed); *see also* LAFAVE, *supra* note 32, at § 2.1(c) (explaining that courts rarely address the subjective prong of the *Katz* analysis); Kerr, *supra*, at 130–32 (arguing that the subjective prong of the *Katz* standard is a "phantom doctrine" due to the fact that courts rarely address or apply it).

[49] *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *DE L'Isle*, 825 F.3d at 432.

[50] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (finding that "the [subjective] expectation [must] be one that society is prepared to recognize as 'reasonable.'").

[51] *Id.*

[52] *See* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 250 (1993) (arguing that the objective prong of the *Katz* analysis "implicitly encourages decision makers to define fundamental constitutional values by referring to contemporary social values, goals, and attitudes"). The true objectiveness of this standard, however, has been questioned. *See* Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (raising concerns that under the *Katz* standard, there is a risk that judges will input their own subjective views of reasonableness).

Court has nevertheless identified several instances where an individual is precluded from claiming a reasonable expectation of privacy.[53] These include, *inter alia*, purported expectations of privacy in objects, items, or information that: (1) have been exposed to the public; (2) are contraband; or (3) are voluntarily disclosed to third parties.[54] In each instance, the Court has concluded that society does not recognize a reasonable expectation of privacy.[55]

First, courts preclude individuals from claiming a reasonable expectation of privacy in objects, items, or information that have been exposed to the public.[56] For example, the U.S. Supreme Court has held that an individual may not claim a reasonable expectation of privacy in what is exposed to public view, what is contained in a garbage can that is placed on a public street, or even their location while driving on a public roadway.[57] In the Court's view, once an individual exposes something to the public, he or she cannot reasonably expect that it will remain private.[58]

Second, courts rarely recognize a reasonable expectation of privacy in objects, items, or information considered to be contraband.[59] Accordingly, governmental conduct that will "*only*" reveal the presence of contraband, rather than the presence of lawful activity, is not considered to be a Fourth Amend-

---

[53] *See infra* notes 56–73 and accompanying text (describing instances when an individual may not claim a reasonable expectation of privacy in objects or information).

[54] *See* Illinois v. Caballes, 543 U.S. 405, 408–10 (2005) (addressing contraband); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (addressing information voluntarily disclosed to third parties); *Katz*, 389 U.S. at 351 (addressing information exposed to the public).

[55] *Caballes*, 543 U.S. at 408–10; *Smith*, 442 U.S. at 743–42; *Katz*, 389 U.S. at 351.

[56] *Katz*, 389 U.S. at 351 (finding 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"); David Reichbach, *The Home Not the Homeless: What the Fourth Amendment Has Historically Protected and Where the Law Is Going After* Jones, 47 U.S.F. L. REV. 377, 385–88 (2012) (describing cases holding that an individual is precluded from claiming a reasonable expectation of privacy in objects, items, or information exposed to the public).

[57] *See* Florida v. Riley, 488 U.S. 445, 449–50 (1989) (holding that aerial surveillance of an individual's backyard was not a Fourth Amendment search because it was exposed to the public's vantage point); California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that there is no reasonable expectation of privacy in objects or items in a garbage can on a public street); Oliver v. United States, 466 U.S. 170, 180–81 (1984) (holding that there is no reasonable expectation of privacy in "open fields" because they are exposed to the public); *Knotts*, 460 U.S. at 281–82 (holding that an individual has no reasonable expectation of privacy in their location while traveling on public roads); *see also* LAFAVE, *supra* note 32, at § 2.2 (noting that an individual may not claim a reasonable expectation of privacy in anything that "a law enforcement officer is able to detect [] by utilization of one or more of his senses while lawfully present at the vantage point where those senses are used").

[58] *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

[59] *Caballes*, 543 U.S. at 408–10 (noting that contraband "cannot be deemed 'legitimate'" for Fourth Amendment purposes and thus is not protected); United States v. Jacobsen, 466 U.S. 109, 137 (1984); *Place*, 462 U.S. at 707.

ment search.[60] The U.S. Supreme Court addressed this notion in 2005 in *Illinois v. Caballes*.[61] In *Caballes*, the Court held that a Fourth Amendment search did not occur when a police dog's sniff of the trunk of a vehicle revealed the presence of narcotics.[62] The *Caballes* Court concluded that because the police dog had been trained specifically to identify the presence of drugs, its sniff of the vehicle would reveal only contraband and nothing else.[63] In the Court's view, "governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'"[64] The Court emphasized the uniqueness of such governmental conduct, however, by characterizing dog sniffs as "*sui generis*"—Latin for unique.[65] In the Court's view, because the governmental conduct could not possibly reveal lawful activity, is was not a Fourth Amendment search.[66]

The third preclusion has come to be known as the third-party doctrine, and is perhaps the most notorious.[67] The third-party doctrine, broadly speak-

---

[60] *Caballes*, 543 U.S. at 408–10 (holding that a police dog's sniff of a vehicle is not a Fourth Amendment search because the sniff would only reveal the presence of contraband); *see Jacobsen*, 466 U.S. at 137 (holding that a chemical test that will only reveal whether the tested substance was contraband "compromises no legitimate privacy interest" because the test would not disclose a "'private' fact"); *Place*, 462 U.S. at 707 (noting that a dog sniff of luggage "discloses only the presence or absence of narcotics, a contraband item[,]" and thus is not a search under the Fourth Amendment). *But see* Florida v. Jardines, 569 U.S. 1, 10–11 (2013) (declining to apply the *Katz* standard and holding that a dog sniff of a home was a Fourth Amendment search under the trespass-based approach to Fourth Amendment search determinations).

[61] *Caballes*, 543 U.S. at 407.

[62] *Id.* at 408–10.

[63] *Id.* at 409. Given the specialized nature of a dog's ability to alert only to contraband, the Court characterized this type of preclusion as "s*ui generis*." *Id.*

[64] *Id.* at 408 (quoting *Jacobsen*, 466 U.S. at 123). Notably, the *Caballes* Court distinguished its case from the Court's 2001 decision in *Kyllo v. United States*. *Id.* at 409–10. In *Kyllo*, the Court held that law enforcement's use of thermal technology to reveal the presence of heat lamps used to grow marijuana constituted a search under the Fourth Amendment. 533 U.S. at 38–40. The *Caballes* Court concluded that because the type of search in *Kyllo* could have revealed the presence of "lawful activity" in the home, the individual whose home was searched had a reasonable expectation that his or her "lawful activity w[ould] remain private." *Caballes*, 543 U.S. at 409–10. The disputed search in *Caballes*, the Court held, was distinguishable because the dog's sniff could not have revealed lawful activity. *Id.* at 410.

[65] *Caballes*, 543 U.S. at 409. This characterization came from the Court's description of dog sniffs in 1983 in *United States v. Place*. 462 U.S. at 707. Critical to the *Place* Court's characterization of a dog sniff as *"sui generis*" was the fact that there was no risk of an intrusive search that would reveal perfectly legal materials. *Id.* Although the Court felt comfortable in concluding that no search had occurred, it stressed that the circumstances leading to this determination were rare. *Id.* (finding that "we are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure").

[66] *Caballes*, 543 U.S. at 409.

[67] *See Smith*, 442 U.S. at 743–44 (discussing the third-party doctrine); United States v. Miller, 425 U.S. 435, 443 (1976) (same); *see also* Porter, *supra* note 32, at 1788–90 (discussing the history of the third-party doctrine). In some instances, however, courts will apply the third-party doctrine to the subjective prong of the *Katz* analysis. *See, e.g.*, *DE L'Isle*, 825 F.3d at 432 (holding that one cannot have a subjective expectation of privacy in information that is voluntarily disclosed to third parties);

ing, dictates that an individual may not claim a reasonable expectation of privacy in information that has been voluntarily disclosed to third parties.[68] The U.S. Supreme Court clearly articulated the doctrine in its 1979 decision in *Smith v. Maryland*.[69] In *Smith*, law enforcement officers placed a pen register at the offices of Smith's telephone company to record the telephone numbers that Smith dialed.[70] The government later used these recorded telephone numbers as evidence against Smith.[71] The *Smith* Court held that the government's conduct did not amount to a Fourth Amendment search because Smith could not claim a reasonable expectation of privacy in telephone numbers that he dialed.[72] In the Court's view, by dialing the numbers, Smith voluntarily disclosed them to a third party (the telephone company) and assumed the risk that the numbers would later be turned over to law enforcement.[73]

Criticism of the third-party doctrine, however, has been levied since its inception.[74] In his dissent in *Smith*, Justice Marshall argued, in part, that the voluntary disclosure of information for one purpose should not militate against a later expectation of privacy in the same information.[75] In Justice Marshall's

---

Bah, 794 F.3d at 630 n.9 (concluding that a larger factual record could have allowed the court to determine that there was no subjective expectation of privacy); *Alabi*, 943 F. Supp. 2d at 1274–75 (noting that courts have found that a "person's disclosure of something in which the person asserts he or she has a reasonable expectation of privacy precludes finding the manifestation of such a subjective belief").

[68] *See Smith*, 442 U.S. at 743–44 (discussing the third-party doctrine); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563, 566–70 (2009) (describing the third-party doctrine and its origins).

[69] *See* Porter, *supra* note 32, at 1789 (noting that *Smith* "named and further refined the third-party doctrine"). The articulation of the third-party doctrine in *Smith* was the culmination of several U.S. Supreme Court holdings that stood for the same proposition: that an individual may not claim a reasonable expectation of privacy in information voluntarily disclosed to third parties. *See* Kerr, *supra* note 68, at 567–70 (describing the origins of the third-party doctrine); *see, e.g.*, *Miller*, 425 U.S. at 443 (holding there is no reasonable expectation of privacy in information voluntarily disclosed to a bank); United States v. White, 401 U.S. 745, 752 (1971) (holding there is no reasonable expectation of privacy in information disclosed to a companion who later turned that information over to the government); Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that no Fourth Amendment search occurred when the defendant disclosed incriminating information to an informant).

[70] *Smith*, 442 U.S. at 737.

[71] *Id.* (noting that the telephone numbers were used to convict Smith by confirming that he was the one who had called the victim shortly after robbing her).

[72] *Id.* at 744–46; Porter, *supra* note 32, at 1789–90 (discussing the holding of *Smith*).

[73] *See Smith*, 442 U.S. at 744–46; Porter, *supra* note 32, at 1789–90 (discussing the holding of *Smith*).

[74] *See* State v. Tate, 849 N.W.2d 798, 827 (Wis. 2014) (describing historical criticism of the third-party doctrine); Kerr, *supra* note 68, at 570–73 (discussing critiques of the third-party doctrine); *see, e.g.*, *Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring) (criticizing the third-party doctrine's current construction and application); United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) (noting that "[a] *per se* rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy") (emphasis added); Porter, *supra* note 32, at 1806–10 (arguing that the third-party doctrine should be "reformed").

[75] *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

view, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[76] These early concerns have not abated since *Smith* was decided.[77] Contemporary criticism points to the fact that, in light of the economic and technological realities of today, individuals are regularly forced to disclose private information to third parties as a matter of course.[78] Nevertheless, rather than adapt to these realities, federal courts seemingly remain steadfast in their rigid application of the third-party doctrine.[79]

C. Get "Smart": The Supreme Court Weighs in on Privacy Interests in Smart Phones

As discussed *supra*, after a court has determined that a Fourth Amendment search has occurred, the court must then determine if the search was reasonable.[80] In June 2014, in *Riley v. California*, the U.S. Supreme Court held that the government's act of opening a lawfully arrested individual's cell phone without a warrant to access the data and information stored therein was unreasonable.[81]

---

[76] *Id.*

[77] *See* Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 261 (2015) (arguing that "[t]he third-party doctrine has become the Fourth Amendment's supervillain"); Kerr, *supra* note 68, at 563 n.5 "The third-party doctrine is the Fourth Amendment rule scholars love to hate . . . . A list of every article or book that has criticized the doctrine would make [for] the world's longest law review footnote.").

[78] *See, e.g.*, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (arguing that the third-party doctrine 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"); *Tate*, 849 N.W.2d at 827 ("In the modern world, in which we regularly disclose information to third parties as part of everyday life, the third-party doctrine is ailing as a principle of law."); Bambauer, *supra* note 77, at 216 (discussing how "[c]omputing power and the accretion of third-party records" complicate Fourth Amendment search determinations); Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1495 (2015) (criticizing the application of the third-party doctrine because "[i]n an increasingly connected world, choosing not to provide personal information via credit cards, cell phones, the Internet, and other media through a corporate third-party intermediary is not a viable option"); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 673 (2013) (arguing that "[t]he danger of the [third-party] doctrine is even more apparent today" because of the prevalence of information "transmitted to third-party Internet service providers, search engines, email servers, and others"); Porter, *supra* note 32, at 1803–10 (discussing privacy concerns over an individual's cell-site location data and arguing that the third-party doctrine should be "reformed" to account for privacy interests created by advances in technology).

[79] *See* Porter, *supra* note 32, at 1790 (discussing how the application of the third-party doctrine has not changed since *Smith*).

[80] *See* Kerr, *supra* note 31, at 316–19 (describing the sequential approach to Fourth Amendment search determinations); Lucier, *supra* note 23, at 1811 (describing how courts adjudicate Fourth Amendment disputes); *supra* notes 30–32 and accompanying text (describing the reasonableness requirement of the Fourth Amendment.

[81] *Riley*, 134 S. Ct. at 2485; William Clark, Note, *Protecting the Privacies of Digital Life:* Riley v. California*, the Fourth Amendment's Particularity Requirement, and Search Protocols for Cellphone Search Warrants*, 56 B.C. L. REV. 1981, 1996 (2015) (discussing the *Riley* decision). The *Riley* Court did not address whether the government's conduct amounted to a Fourth Amendment search. Potapchuk, *supra* note 21, at 1413 n.58 (explaining that the sole question before the *Riley* Court was

In *Riley*, the government arrested the petitioner after a routine traffic stop resulted in the discovery of drugs, firearms, and materials evidencing gang activity.[82] The government lawfully seized the petitioner's cell phone during the arrest and later searched it without a warrant.[83] On appeal, the Court was tasked with deciding whether or not the warrantless search was reasonable by way of falling within the search incident to a lawful arrest exception to the warrant requirement.[84] The Court held that, although searches incident to an arrest generally do not require a warrant, this "categorical exception" should not apply to the "digital contents" contained within "physical objects," such as cell phones, and therefore held the warrantless search to be unreasonable.[85]

Central to the Court's holding was the conclusion that the digital data contained within a cell phone does not implicate the twin dangers that the search incident to arrest exception seeks to guard against.[86] First, the digital data itself poses no physical danger to law enforcement at the time of the arrest.[87] Second,

---

whether or not the government's search of the cell phone fell within the search incident to arrest warrant exception). Indeed, it seems that it was conceded that the government's conduct was a Fourth Amendment search. *See Turner*, 839 F. 3d at 434 n.2 (explaining that there was "no dispute" among the parties that by examining the contents of the phone, the government committed a search under the Fourth Amendment).

[82] *Riley*, 134 S. Ct. at 2480. *Riley* decided two cases that had been consolidated for appeal. *Id.* at 2473. The other case had a similar factual record, as the respondent, Wurie, had his cell phone seized and searched. *Id.* at 2481. Information contained in the cell phone was then used to secure a search warrant for an apartment that contained evidence of Wurie's involvement in a drug distribution scheme. *Id.*

[83] *Id.* at 2480. The trial court denied the petitioner's motion to suppress the information taken from the cell phone and the California Court of Appeals affirmed, holding that accessing the contents of the cell phone fell within the "search incident to arrest" warrant exception. *Id.* at 2481. Riley subsequently appealed. *Id.*

[84] *Id.* at 2482.

[85] *Id.* at 2484–85. The Court thoroughly summarized its precedent with respect to searches incident to an arrest. *See id.* at 2482–84. The Court explained that in 1969, in *Chimel v. California*, the Court concluded that searches incident to a lawful arrest were reasonable if a given search was necessary to remove objects that may pose a danger to the arresting officer's safety. *Id.* at 2482 (citing Chimel v. California, 395 U.S. 752, 762–63 (1969)). The *Chimel* Court further concluded that searches incident to an arrest were allowable when they would aid in preventing the "concealment or destruction" of evidence. *Id.* (quoting *Chimel*, 395 U.S. at 762–63). The *Riley* Court next discussed the Court's decisions in 1973 in *United States v. Robinson* and in 1991 in *United States v. Chadwick* which held that a search incident to an arrest may be reasonable with respect to "personal property . . . immediately associated with the person of the arrestee" even though there is no danger of loss of evidence or harm to the arresting officer. *Id.* at 2483–84 (citing United States v. Chadwick, 433 U.S. 1, 15 (1977)).

[86] *See id.* at 2485–88 (concluding that digital data does not implicate the policy concerns behind the search incident to arrest exception to the warrant requirement). The *Chimel* Court concluded that the search incident to arrest exception was necessary to protect arresting police officers and preserve the evidence that may be found upon an arrest. *See Chimel*, 395 U.S. at 762–63.

[87] *Riley*, 134 S. Ct. at 2485–86. The Court explained that digital data "cannot itself be used as a weapon to harm an arresting officer." *Id.* at 2485. The Court juxtaposed the digital contents of a cell phone with the cigarette pack confiscated and searched in *Robinson*, concluding that because the arresting officer could not have known whether the physical objects contained in the cigarette pack

there is minimal risk that an arrestee will be able to "conceal or destroy" evidence within the digital data once the cell phone has been confiscated.[88] Additionally, the Court found that the modern cell phone's substantial storage capability and the sensitive personal information typically contained therein creates a privacy interest that far outweighs any perceived government interest in searching the cell phone.[89] The Court therefore held that that the warrantless search of the cell phone was unreasonable.[90]

Because the *Riley* Court tailored the holding to the propriety of warrantless cell phone searches, it therefore left open the constitutionality of warrantless searches of other types of physical objects capable of storing digital data.[91] In July 2015, in *United States v. Bah*, the U.S. Court of Appeals for the Sixth Circuit held that the government's act of scanning the magnetic stripe of a card to access the data contained therein is not a Fourth Amendment search.[92] In so doing, the Sixth Circuit became the first circuit to address this issue.[93] Soon after, the Eighth Circuit, in June 2016 in *United States v. DE L'Isle*, the Fifth Circuit, in October 2016 in *United States v. Turner*, and the First Circuit, in May 2017 in *United States v. Hillaire*, followed the Sixth Circuit's lead and similarly held that scanning a card is not a Fourth Amendment search.[94]

II. THE CARD CONUNDRUM: WARRANTLESS SEARCHES OF DIGITAL STORAGE DEVICES POST-*RILEY*

The U.S. Courts of Appeals for the First, Fifth, Sixth, and Eighth Circuits uniformly concluded that swiping the magnetic stripe of a card is not a search

---

could have been harmful, it was reasonable to search the contents of the pack. *Id.*; *see* United States v. Robinson, 414 U.S. 218, 236 (1973). Not so in the case of a cell phone, the *Riley* Court held, as the digital data within the cell phone posed no physical harm to the arresting officers because they "knew exactly what they would find therein: data." 134 S. Ct. at 2485 (quoting United States v. Wurie, 728 F. 3d 1, 10 (1st Cir. 2013)).

[88] *Riley*, 134 S. Ct. at 2486–88.

[89] *Id.* at 2488–91.

[90] *Id.* at 2493.

[91] *See id.* (tailoring the holding to warrantless searches of cell phones); Katharine Saphner, Note, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1705–06 (2016) (discussing post-*Riley* decisions that have sought to determine the authority of conducting warrantless searches of digital storage devices).

[92] *Bah*, 794 F.3d at 621; *see* Orin Kerr, Opinion, *Is Credit Card Skimming a Fourth Amendment Search?*, WASH. POST (July 29, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/07/29/is-credit-card-skimming-a-fourth-amendment-search/?tid=a_inl&utm_term=.10220e449428 [https://perma.cc/T6U8-DFQK] (describing the *Bah* case).

[93] *Bah*, 794 F.3d at 631–32.

[94] *Hillaire*, 857 F.3d at 130; *Turner*, 839 F.3d at 434; *DE L'Isle*, 825 F.3d at 431–33. DE L'Isle's subsequent motion for a rehearing *en banc* was denied. United States v. DE L'Isle, No. 15-01316, slip op. at 1 (8th Cir. July 22, 2016).

within the meaning of the Fourth Amendment.[95] In order to reach their respective conclusions, each court applied the analysis set forth by the U.S. Supreme Court in 1967, in *Katz v. United States*.[96] In each case, the court found that the appellants were categorically precluded from claiming a reasonable expectation of privacy in the information encoded on the magnetic stripes of the cards.[97] Moreover, the Fifth and Sixth Circuits concluded that the U.S. Supreme Court's 2014 decision in *Riley* v. *California* further supported the finding that an individual does not have a reasonable expectation of privacy in the information encoded on cards.[98] Section A examines the *Bah*, *DE L'Isle*, and *Turner* courts' application of the *Katz* analysis.[99] Section B examines the *Bah* and *Turner* courts' consideration of the *Riley* decision.[100]

A. Not So Great Expectations: The Data Encoded on Cards Fails the Katz *Standard*

In adjudicating the appellants' claims, the *Bah*, *DE L'Isle*, and *Turner* courts each had to make the threshold determination of whether or not the government's conduct constituted a search under the Fourth Amendment.[101] To do this, the courts applied the analysis set forth in *Katz*.[102] Subsection 1 examines the Sixth Circuit's application of the *Katz* standard in 2015 in *United States v. Bah*.[103] Subsection 2 examines the Eighth Circuit's application of the *Katz* standard in 2016 in *United States v. DE L'Isle*.[104] Subsection 3 examines the Fifth Circuit's application of the *Katz* standard in 2016 in *United States v. Turner*.[105]

---

[95] United States v. Hillaire, 857 F.3d 128, 130 (1st Cir. 2017); United States v. Turner, 839 F.3d 429, 435 (5th Cir. 2016); United States v. DE L'Isle, 825 F.3d 426, 431–33 (8th Cir. 2016); United States v. Bah, 794 F.3d 617, 630 (6th Cir. 2015), *cert. denied sub nom.* Harvey v. United States, 136 S. Ct. 561 (2015).

[96] *See Hillaire*, 857 F.3d at 130 (applying *Katz v. United States* analysis); *Turner*, 839 F.3d at 434–35 (same); *DE L'Isle*, 825 F.3d at 431–33 (same); *Bah*, 794 F.3d at 630–32 (same).

[97] *See Turner*, 839 F.3d at 434–35; *DE L'Isle*, 825 F.3d at 431–33; *Bah*, 794 F.3d at 630–32.

[98] *Turner*, 839 F.3d at 434; *Bah*, 794 F.3d at 632–33.

[99] *See infra* notes 101–137 and accompanying text. As mentioned *supra*, the U.S. Court of Appeals for the First Circuit's decision in *United States v. Hillaire* will not be analyzed in this Part. *See supra* note 19.

[100] *See infra* notes 138–150 and accompanying text.

[101] *Turner*, 839 F.3d at 434; *DE L'Isle*, 825 F.3d at 431–33; *Bah*, 794 F.3d at 630.

[102] *Turner*, 839 F.3d at 434–35 (applying the *Katz* analysis); *DE L'Isle*, 825 F.3d at 431–33 (same); *Bah*, 794 F.3d at 630–32 (same).

[103] *See infra* notes 106–123 and accompanying text.

[104] *See infra* notes 124–132 and accompanying text.

[105] *See infra* notes 133–137 and accompanying text.

1. *United States v. Bah*

In *United States v. Bah*, law enforcement arrested the driver of a car, Bah, for driving with a suspended license.[106] Following the arrest, the government searched the vehicle.[107] Approximately seventy cards were discovered and then seized.[108] Law enforcement brought the seized cards back to the police station and—without a warrant—scanned them through the station's magnetic card reader to determine if the electronic account information encoded on the magnetic stripes matched the account numbers embossed on the face of each corresponding card.[109] The scans revealed that the encoded information did not match the information embossed on the cards.[110] The cards were therefore determined to be fraudulent and Bah was charged and convicted.[111]

Before trial, Bah moved to suppress the evidence from the station's magnetic card reader.[112] Bah argued that the warrantless scans of these cards violated his Fourth Amendment right against unreasonable searches.[113] After the district court denied Bah's motion, Bah entered a conditional guilty plea and the trial judge sentenced him to ten months in prison.[114] On appeal, the Sixth Circuit concluded that, under *Katz*, the government's scans of the suspected fraudulent cards were not Fourth Amendment searches.[115]

---

[106] *Bah*, 794 F.3d at 622.

[107] *Id.* Bah's passenger, Allen Harvey, was not placed under arrest at the scene, but nonetheless was escorted back to the police station for questioning. *Id.* After a search of Harvey's wallet, several credit cards were found. *Id.* After the cards were deemed to be fraudulent, Harvey was arrested. *Id.*

[108] *Id.*

[109] *Id.* at 623. As the court in *Bah*, as well as subsequent courts, explained, upon scanning the magnetic stripe of a credit, debit, or gift card (collectively, "cards") in a magnetic card reader, a number of different types of information will appear. *Id.* This information includes the card's "account number, bank identification number . . . the card expiration date, the three digit 'CSC' code, and the cardholder's first and last name." *Id.; see Turner*, 839 F.3d at 435–36 (describing electronic information contained within the magnetic stripe of gift cards); *DE L'Isle*, 825 F.3d at 430 (describing electronic information contained within the magnetic stripe of gift cards). Typically, a card that contains electronic information that is different from the information embossed on the face of the card indicates that the card is fraudulent. *Turner*, 839 F.3d at 436.

[110] *Bah*, 794 F.3d at 623.

[111] *Id.* Bah and his passenger, Harvey, were charged with the "production, use, or trafficking in counterfeit access devices." *Id.* at 624.

[112] *Id.*

[113] *Id.*

[114] *Id.* at 625. The magistrate judge made the initial ruling on Bah's motion and found that there was no search within the meaning of the Fourth Amendment. *Id.* The district court then adopted the magistrate's findings. *Id.*

[115] *Id.* at 630. Consistent with *Jones*, the *Bah* court concluded that the scanning of the cards did not constitute a search under the trespass-based approach to Fourth Amendment search determinations because they did not involve a "physical intrusion of a constitutionally protected area." *See id.*; *see also supra* note 45 (discussing how *Katz* did not replace the "trespass-based" approach to Fourth Amendment determinations but rather supplemented it). In making this determination, the *Bah* court reasoned that because the confiscated cards were lawfully possessed by law enforcement, there could not have been a physical trespass. *See Bah*, 794 F.3d at 630 (citing United States v. Alabi, 943 F.

The *Bah* court began the two-pronged *Katz* analysis by first addressing the subjective inquiry.[116] Consistent with the practice of many other courts, however, the *Bah* court assumed the subjective prong was satisfied for the purposes of addressing the next prong of the *Katz* analysis.[117]

The court then analyzed the objective prong and concluded that Bah's expectation of privacy was unreasonable because it was not one that "society is prepared to consider reasonable."[118] Critical to the court's holding was its conclusion that individuals are precluded from claiming a reasonable expectation of privacy in contraband and in objects, items, or information exposed to the public.[119] In the court's view, regardless of whether the card was authentic or not, Bah retained no privacy interest in the information encoded on it.[120] The court reasoned that if the cards were authentic, the information encoded on the magnetic stripes would be no different from the information embossed on the cards themselves—information that is typically exposed to the public upon making purchases and readily visible to law enforcement upon seizure.[121] Conversely, if the information encoded on the magnetic stripe was different, the information could be considered contraband.[122] In either case, the court concluded, Bah would not be able to claim a legitimate privacy interest in the encoded information.[123]

2. *United States v. DE L'Isle*

Similarly, in June 2016, in *United States v. DE L'Isle*, the Eighth Circuit held that warrantless scans of magnetic stripes of cards are not searches under the Fourth Amendment.[124] Unlike the *Bah* court, however, the *DE L'Isle* court

---

Supp. 2d 1201, 1265 (D.N.M. 2013)). The court then went on to apply the *Katz* analysis. *See id.* at 630–34.

[116] *Bah*, 794 F.3d at 630.

[117] *Id.* The court noted, however, that this assumption was not intended to imply that Bah had a strong argument in support of the subjective prong of the *Katz* analysis. *See id.* at 630 n.9 (noting that Bah's claim to have had a subjective expectation of privacy in the information encoded on the magnetic stripe of the seized cards "is far from clear").

[118] *Id.* at 630.

[119] *Id.* at 632.

[120] *See id.* ("The question presented here lies at 'an intersection . . . between the principle that there is no legitimate privacy interest in already known information, and . . . no legitimate privacy interest in contraband.'") (quoting United States v. DE L'Isle, No. 4:14-CR-3089, 2014 WL 5431349, at *3 (D. Neb. Oct. 24, 2014)).

[121] *Id.* at 631–32.

[122] *Id.* at 632.

[123] *Id.* at 631–32.

[124] *DE L'Isle*, 825 F.3d at 429–30. *DE L'Isle* involved a routine traffic stop that eventually led to the discovery of a large number of cards in the trunk of DE L'Isle's vehicle. *Id.* at 429. The cards were turned over to the U.S. Secret Service for examination and, after scanning the cards without a warrant, many were identified as having been re-encoded with stolen account information. *Id.* Scans of some of the confiscated cards revealed that their magnetic stripes were "blank." *Id.* In other words, the scans of the

did not merely assume that the appellant had a subjective expectation of privacy in encoded information under *Katz*, but rather scrutinized that claim specifically. [125] It reasoned that because the use of a card necessarily requires the voluntary transfer of the account information encoded on the magnetic stripe to cashiers and the like, no subjective expectation of privacy in that content could be claimed. [126] In effect, the court concluded that the third-party doctrine precluded DE L'Isle from claiming an expectation of privacy in the encoded information. [127]

Next, the *DE L'Isle* court addressed the objective prong of the *Katz* analysis and held that even assuming that DE L'Isle could claim a subjective expectation of privacy, such an expectation would be unreasonable because it is not one that "society is prepared to endorse." [128] In this respect, the court's analysis largely mirrored the analysis employed by the Sixth Circuit in *Bah*. [129] The *DE L'Isle* court concluded that there is no reasonable expectation of privacy in the encoded information, reasoning that if the cards were authentic, the information encoded on the magnetic stripe would have mirrored the information embossed on the card and thus would be exposed to the public. [130] Alternatively, if the encoded information was different from the information embossed on the card, the information would be considered contraband. [131] Under either analysis, the court

---

cards turned up no account information at all, thereby indicating that the cards were fraudulent and were capable of later becoming encoded with stolen account information. *Id.* at 430. DE L'Isle promptly moved to suppress the evidence of the card readings under the theory that the warrantless scans violated his Fourth Amendment right against unreasonable searches. *Id.* at 429–30. The district court denied the motion and held that the scans were not searches under the Fourth Amendment. *Id.* After being convicted at trial, DE L'Isle appealed to the Eighth Circuit. *Id.* at 430. Unlike *Bah*, however, *DE L'Isle* was decided over a dissent. *See id.* at 433–37 (Kelly, J., dissenting) (arguing that the case should be remanded for further "factual development" to be able to make an appropriate determination on whether DE L'Isle had a reasonable expectation of privacy).

[125] *Id.* at 432 (majority opinion) (assessing whether DE L'Isle had a subjective expectation of privacy). Prior to addressing the *Katz* standard, the *DE L'Isle* court first disposed of the theory that scanning a card to reveal the encoded account information would be considered a search under the trespass-based approach to Fourth Amendment search determinations. *Id.* at 431–32. The court found this argument unavailing, reasoning that scanning a credit card "'does not involve physically invading a person's' space or property." *Id.* at 431 (quoting United States v. Medina, 09-20717-CR, 2009 WL 3669636, at *10 (S.D. Fla. Oct. 24, 2009).

[126] *Id.* at 432.

[127] *See id.* (quoting *Medina*, 2009 WL 3669636, at *10) ("When the holder uses the card[,] he 'knowingly disclose[s] the information on the magnetic strip of his credit card to a third party and cannot claim a reasonable expectation of privacy in it.'").

[128] *Id.*

[129] *Id.*; *Bah*, 794 F.3d at 631–32.

[130] *See DE L'Isle*, 825 F.3d at 432 (holding that individuals cannot reasonably expect privacy in information that is put into "plain view" such that "any member of the public may see" it).

[131] *See id.* at 432–33 ("[G]overnmental conduct that *only* reveals the presence of contraband 'compromises no legitimate privacy interest.'") (quoting Illinois v. Caballes, 543 U.S. 405, 408 (2005)).

held that DE L'Isle could not have had a reasonable expectation of privacy in the encoded information.[132]

3. *United States v. Turner*

Several months after the *DE L'Isle* decision, in October 2016, the Fifth Circuit, in *United States v. Turner*, followed the Sixth and Eighth Circuits by holding that the government's scans of the magnetic stripes of confiscated gift cards were not searches within the meaning of the Fourth Amendment.[133] Similar to the *Bah* court, the *Turner* court did not address the issue of whether or not Turner had manifested a subjective expectation of privacy in the information encoded on the gift cards.[134] Rather, the court rested its holding on the conclusion that Turner failed to meet the objective prong of the *Katz* analysis.[135] Central to the court's conclusion was the fact that the functional purpose of gift cards was to be swiped by third parties.[136] The court reasoned that because information encoded on the magnetic stripe of a gift card is regularly disclosed to third parties at the time of a purchase, the third-party doctrine precluded Turner from exercising a reasonable expectation of privacy in the information.[137]

---

[132] *Id.* at 433. The majority ruled over a dissent. *Id*. at 433– 35 (Kelly, J., dissenting). The dissenting justice dissented on the grounds that the case needed further factual development before a determination of a reasonable expectation of privacy under *Katz* could be made. *Id.* at 433. The dissent focused on the fact that a credit card may be appropriately described as a "digital storage device," which the U.S. Supreme Court has held to require a warrant before searching. *Id.* at 434 (citing Riley v. California, 134 S. Ct. 2473, 2482 (2014), United States v. Makeeff, 820 F.3d 995, 1002–03 (8th Cir. 2016), United States v. Beckmann, 786 F.3d 672, 677–78 (8th Cir. 2015), and United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008)). The dissent took further issue with the majority's reasoning that no privacy interest exists in information that constitutes illegal conduct. *Id.* at 434–35. The dissent argued that this reasoning was flawed because the illegality of the card is only revealed once the card has been scanned by law enforcement. *Id.* at 434 (citing United States v. Jacobsen, 466 U.S. 109, 114 n.9 (1984) and United States v. Di Re, 332 U.S. 581, 595 (1948)).

[133] *Turner*, 839 F.3d at 433–37. As with *Bah* and *DE L'Isle*, *Turner* involved a suspect who was arrested following a routine traffic violation. *See id.* at 431 (involving a vehicle pulled over for a faulty license plate light); *DE L'Isle*, 825 F.3d at 429 (involving vehicle pulled over for tailgating); *Bah*, 794 F.3d at 621 (involving a vehicle pulled over for speeding). After the vehicle was pulled over, the police officer determined that the passenger of the vehicle—Turner—had an outstanding arrest warrant. *Turner*, 839 F.3d at 431. Law enforcement placed Turner in the police car and a subsequent search of the vehicle revealed the presence of a bag containing approximately 100 gift cards. *Id.* The cards were eventually turned over to the U.S. Secret Service and scanned without a warrant to determine their authenticity. *Id.* at 431–32. Following the scans, approximately forty of the cards were deemed fraudulent. *Id.* at 432. Turner moved to suppress this evidence by arguing that the scans of the cards constituted unreasonable searches in violation of the Fourth Amendment. *Id.* The district court denied Turner's motion and held that the scans were not Fourth Amendment searches. *Id.* Turner entered a conditional guilty plea and appealed to the Fifth Circuit. *Id.*

[134] *Turner*, 839 F.3d at 435–36.

[135] *Id.* at 436.

[136] *See id.* (finding that "the raison d'être of gift cards means that third party cashiers will often be doing the same swiping that law enforcement did here").

[137] *Id.*

B. No Comparison: The Bah *and* Turner *Courts' Consideration of* Riley v. California

In addition to performing the *Katz* analysis, the *Bah* and *Turner* courts each addressed the petitioners' respective arguments that scans of cards should require a warrant under the U.S. Supreme Court's 2014 ruling in *Riley v. California*.[138] Critical to each court's analysis was a discussion of whether the information encoded on a magnetic stripe is sufficiently private or personal enough in nature to create a privacy interest similar to the privacy interest in cellphones recognized in *Riley*.[139]

The *Bah* court distinguished the case before it from *Riley* by focusing on the difference in storage capacity between a magnetic stripe of a card and a cell phone.[140] To highlight this difference, the court summarized the technical aspects of a magnetic stripe.[141] The court explained that a magnetic stripe of a card contains three lines of data, each containing 79 alphanumeric characters, 40 numeric characters, and 107 numeric characters, respectively.[142] Additionally, the court emphasized that the data actually encoded on a card typically matches the information embossed on the front of the card.[143] Thus, in the court's view, such information is not of such a "highly personal" character that one would seek to keep private.[144] In contrast, the court noted, modern cellphones are capable of storing large swaths of private and sensitive information in a variety of formats far exceeding the capabilities of a magnetic stripe.[145] Accordingly, the court concluded that the limited data storage capacity of the magnetic stripe was insufficient to create a privacy interest similar to other digital storage devices such as cell phones or computers.[146] The court therefore held that the *Riley* decision did not allow individuals to claim a reasonable expectation of privacy in the information encoded on a magnetic stripe.[147]

---

[138] *Id.*; *Bah*, 794 F.3d at 631. The *DE L'Isle* court did not address this argument. *See generally DE L'Isle*, 825 F.3d at 430–33 (failing to discuss any relevance of the *Riley* decision). The dissent, however, did address the pertinence of *Riley* to the case before it. *See id.* at 434–35 (Kelly, J., dissenting) (discussing how courts have previously held that a warrant must be obtained before searching digital storage devices).

[139] *See Turner*, 839 F.3d at 434–35; *Bah*, 794 F.3d at 632–33.

[140] *See Bah*, 794 F.3d at 633 ("The storage capacity of the magnetic strip of a credit, debit or gift card pales in comparison to that of a computer hard drive, cell phone, or even audiocassette.").

[141] *Id.*

[142] *Id. But see Alabi*, 943 F. Supp. 2d at 1211 (describing credit and debit cards as only containing "two tracks of stored data").

[143] *Bah*, 794 F.3d at 631.

[144] *Id.* at 633.

[145] *Id.* at 632–33 ("The storage capacity of the magnetic strip of a credit, debit or gift card pales in comparison to that of a . . . cell phone . . . .").

[146] *Id.* at 633.

[147] *Id.* The court explained, however, that their holding was "limited in scope" and is not intended to reach new types of cards with greater storage capacity that may be developed in the future. *Id.* at

Similarly, the Fifth Circuit, in *Turner*, held that although *Riley* established a warrant requirement for lawfully seized digital storage devices like cell phones, it does not apply to digital storage devices with the minimal storage capacity of the magnetic stripe of a gift card.[148] The *Turner* court emphasized the lack of personal information contained within the magnetic stripe of the card, concluding that the three data strips of electronic data—first and last name of the card holder, CSC code, bank identification number, and card number—were not nearly as personal or private as the information contained within a cell phone.[149] Because the information revealed in a scan is minimally invasive, as compared to a search of a cell phone, the court held that individuals cannot claim a reasonable expectation of privacy in the information encoded on a magnetic stripe of a lawfully seized card.[150]

III. Let's Be Reasonable: Scans of Cards Are Fourth Amendment Searches

Collectively, the *Bah*, *DE L'Isle*, and *Turner* courts rested their conclusions that a scan of the magnetic stripe of a lawfully seized card is not a Fourth Amendment search on two main grounds.[151] First, the three courts held that the categorical preclusions to claiming a reasonable expectation of privacy applied to the information encoded on magnetic stripes.[152] Second, the *Bah* and *Turner* courts held that, under the U.S. Supreme Court's 2014 holding in *Riley*, the minimal storage capability of the cards could not give rise to a reasonable expectation of privacy in their contents.[153] Section A argues that the courts erred in holding that the petitioners were precluded from claiming a reasonable expectation of privacy in the information encoded on the cards' magnetic stripes.[154] Section B argues that the *Riley* decision should have played no part in the courts' determination of whether or not scanning a card is a Fourth Amendment search.[155]

631. The *DE L'Isle* and *Turner* courts made similar qualifications. *Turner*, 839 F.3d at 436–37; *DE L'Isle*, 825 F.3d at 433.

[148] *Turner*, 839 F.3d at 434–35.

[149] *Id.* at 435–36; *see supra* notes 7–8 and accompanying text (describing the digital content contained on magnetic stripes of cards).

[150] *Turner*, 839 F.3d at 435–36.

[151] United States v. Turner, 839 F.3d 429, 434–36 (5th Cir. 2016); United States v. DE L'Isle, 825 F.3d 426, 431–33 (8th Cir. 2016); United States v. Bah, 794 F.3d 617, 630–33 (6th Cir. 2015), *cert. denied sub nom.* Harvey v. United States, 136 S. Ct. 561 (2015). As with Part II of this Note, the First Circuit's decision in *Hillaire* will not be analyzed in Part III due to its reliance on the reasoning of the *Bah* and *DE L'Isle* courts. *See supra* notes 19, 99.

[152] *Turner*, 839 F.3d at 434–36; *DE L'Isle*, 825 F.3d at 431–33; *Bah*, 794 F.3d at 630–33.

[153] *Turner*, 839 F.3d at 435–36; *Bah*, 794 F.3d at 632–33.

[154] *See infra* notes 156–196 and accompanying text.

[155] *See infra* notes 197–213 and accompanying text.

A. The Preclusions

The *Bah*, *DE L'Isle*, and *Turner* courts held that the categorical preclusions to claiming a reasonable expectation of privacy applied to the information encoded on magnetic stripes.[156] Each court found that because the cards were either exposed to the public or voluntarily disclosed to third parties, the appellants could not have had a reasonable expectation of privacy in the information.[157] Further, the *Bah* and *DE L'Isle* courts held that in the event that the encoded information is different from the information embossed on the cards, one could not claim a reasonable expectation of privacy in the information because it would constitute contraband.[158] Subsection 1 argues that the exposure of the physical cards to the public does not preclude an individual from claiming a reasonable expectation of privacy in the information encoded on magnetic stripes.[159] Subsection 2 argues that the courts' application of *Caballes* is misplaced.[160] Subsection 3 argues that the third-party doctrine should not apply to the information encoded on magnetic stripes.[161]

1. Public Exposure

The *Bah* and *DE L'Isle* courts each implicitly held that because the cards were exposed to the public, the appellants could not have claimed a reasonable expectation of privacy in the encoded information.[162] Indeed, although the cards themselves may have been taken out of a wallet or bag and been exposed to the public, the exposure of the cards themselves does not, in and of itself, justify a search of their contents.[163] The contents of a card are similar to the contents of other physical items—such as a suitcase.[164] In either instance, the contents of the container, whether physical or digital, are not visible to the na-

---

[156] *Turner*, 839 F.3d at 434–36; *DE L'Isle*, 825 F.3d at 431–33; *Bah*, 794 F.3d at 630–33.

[157] *Turner*, 839 F.3d at 434–36; *DE L'Isle*, 825 F.3d at 431–33; *Bah*, 794 F.3d at 630–33.

[158] *DE L'Isle*, 825 F.3d at 432–33; *Bah*, 794 F.3d at 632.

[159] *See infra* notes 162–166 and accompanying text.

[160] *See infra* notes 167–180 and accompanying text.

[161] *See infra* notes 181–196 and accompanying text.

[162] *See DE L'Isle*, 825 F.3d at 432 (quoting United States v. Alabi, 943 F. Supp. 2d 1201, 1276 (D.N.M. 2013) (finding that "[s]ociety is not prepared to recognize as legitimate an asserted privacy interest in information in plain view that any member of the public may see"); *Bah*, 794 F.3d at 630–33.

[163] *See* United States v. Ross, 456 U.S. 798, 822–23 (1982) (noting that "the Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view[,]" and then describing instances where a warrantless search of a container's contents may be reasonable); LAFAVE, *supra* note 32, at § 2.2(a) (noting that "the mere fact that [a] container itself is in plain view provides no basis for a warrantless seizure and search of it").

[164] *See* Bond v. United States, 529 U.S. 334, 339 (2000) (holding that a bag exposed to the public on a public bus could not be searched without a warrant); United States v. Rivera-Padilla, 365 F. App'x 343, 345 (3d Cir. 2010) (holding that a warrantless search of a closed wallet was unreasonable).

ked eye and cannot be known until the government acts in some way to expose them.[165] Further, because the magnetic stripes are rewritable, the fact that certain information is embossed on the card provides no guarantee of what information is actually encoded on the magnetic stripe.[166]

2. Contraband

The *Bah* and *DE L'Isle* courts further held that an individual does not have a reasonable expectation of privacy in encoded information when it differs from the information embossed on the front and back of the corresponding card.[167] In the courts' view, when the sets of information differ, the encoded information must be contraband.[168] In support of this conclusion, the courts cited the U.S. Supreme Court's decision in *Illinois v. Caballes* that held that a police dog's sniff of a vehicle was not a Fourth Amendment search because the sniff could only have resulted in the identification of contraband.[169]

In *Caballes*, the police dog performing the sniff was trained specifically to identify the presence of contraband.[170] This specific training ensured that the police dog would not erroneously trigger a search that would reveal legal activity.[171] Because dog sniffs would not reveal the presence of lawful activity, the Court characterized them as "*sui generis*" and held that they were not Fourth Amendment searches.[172]

---

[165] *See Bond*, 529 U.S. at 336 (describing how the contents of the bag would not be revealed until it was searched by law enforcement); *Rivera-Padilla*, 365 F. App'x at 346 (describing how incriminating evidence was not discovered in the wallet until it was opened and searched by law enforcement); *see also DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (noting that "it is only possible to determine whether the information on the magnetic stripe is blank or matches the information embossed on the front of the card by scanning the magnetic stripe to determine its contents").

[166] *See DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (noting that a magnetic stripe may be re-encoded to store any kind of information).

[167] *Id.* at 432–33; *Bah*, 794 F.3d at 632.

[168] *See DE L'Isle*, 825 F.3d at 433 (finding that "because scanning the magnetic strips [sic] on the cards was the government's way of revealing DE L'Isle's possession of contraband, the counterfeit cards, there was no violation of a legitimate privacy interest and accordingly, no search within the meaning of the Fourth Amendment"); *Bah*, 794 F.3d at 632 (quoting *Alabi*, 943 F. Supp. 2d at 1273) (noting that "either the information disclosed is the same information on the outside of the credit and debit cards, or is information about a different account, used to commit credit card fraud").

[169] *DE L'Isle*, 825 F.3d at 433; *Bah*, 794 F.3d at 632; *see also* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005).

[170] *See Caballes*, 543 U.S. at 409.

[171] *See id.* (finding that "[a]lthough respondent argues that the error rates, particularly the existence of false positives, call into question the premise that drug-detection dogs alert only to contraband, the record contains no evidence or findings that support his argument").

[172] *Id.* Emphasizing that individuals have a reasonable expectation of privacy in the presence of lawful activity, the *Caballes* Court distinguished the case before it from its 2001 decision in *Kyllo v. United States*. *Id.* at 409–10. The *Kyllo* Court held that law enforcement's use of thermal technology to reveal the presence of heat lamps used to grow marijuana constituted a search under the Fourth Amendment. Kyllo v. United States, 533 U.S. 27, 31–32 (2001). The *Caballes* Court concluded that

Relying on *Caballes*, the *Bah* and *DE L'Isle* courts concluded that individuals do not have a reasonable expectation of privacy in the information encoded on a magnetic stripe when the information is different from what is embossed on the front and back of the card.[173] The courts' premise that encoded information is contraband whenever it differs from the embossed information is flawed, however, and their reliance on *Caballes* is therefore misplaced.[174]

Unlike the *sui generis* nature of a dog sniff, a scan of the magnetic stripe of a card may very well reveal the presence of lawful activity.[175] Magnetic stripes are capable of being re-encoded with any type of information.[176] Depending on how the stripe is re-encoded, the scan could reveal re-encoded information distinct from the information embossed on the card that was nonetheless not contraband.[177] Regardless of the likelihood that an individual would re-encode a magnetic stripe with anything other than stolen account information, exactly what information is encoded on a magnetic stripe is not known to the government unless and until the card is scanned.[178] At the time of the scan the government does not know what information will be revealed.[179] This

---

because the search in *Kyllo* could have revealed the presence of "lawful activity" in the home, the individual whose home was searched had a reasonable expectation that his or her "lawful activity w[ould] remain private." *Caballes*, 543 U.S. at 409–10. The disputed search in *Caballes*, however, was distinguishable because the dog's sniff could not have revealed lawful activity. *Id.* at 410.

[173] *See DE L'Isle*, 825 F.3d at 432–33 (quoting *Caballes*, 543 U.S. at 408) (finding that "governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest'"); *Bah*, 794 F.3d at 632.

[174] *See DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (distinguishing the *DE L'Isle* majority opinion from *Caballes*); Kerr, *supra* note 92 (arguing that *Caballes* should not apply to cases dealing with scans of credit or debit cards); *see also Caballes*, 543 U.S. at 410–13 (Souter, J., dissenting) (dissenting on the grounds that it is not conclusive that police dogs can perform sniffs without creating false positive results).

[175] *See DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (discussing how a magnetic stripe may be re-encoded to potentially include non-incriminating information); Kerr, *supra* note 92 (providing examples of how a magnetic stripe may be re-encoded to contain information that is neither identical to the information embossed on the card nor contraband).

[176] *See DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (discussing how a magnetic stripe may be re-encoded to store any information); Kerr, *supra* note 92 (providing examples of how a magnetic stripe may be re-encoded with information that is not contraband).

[177] Kerr, *supra* note 92 (noting that scanning a card can "reveal[] non-contraband data that could be anything. The magstripe is just a small electronic storage device that can be programmed, within its technical parameters, to contain any information the encoder wants it to contain . . . . [I]t's still information that could say anything").

[178] *See Turner*, 839 F.3d at 431–35 (describing how cards are revealed to be fraudulent only upon scanning them); *Alabi*, 943 F. Supp. 2d at 1211–12; *see also DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (arguing that scans are Fourth Amendment searches even if there is only a small likelihood that the stripes would be rewritten with information that was neither stolen account information nor the information embossed on the cards); Kerr, *supra* note 92 (explaining that "[scanning cards] reveals non-contraband data that could be anything").

[179] *See DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (arguing that "it is only possible to determine whether the information on the magnetic stripe is blank or matches the information embossed on the front of the card by scanning the magnetic stripe to determine its contents"); Kerr, *supra* note

type of search is exactly what the Fourth Amendment seeks to prevent and *Caballes* is therefore inapplicable to the scans of cards.[180]

3. Third-Party Doctrine

The *Bah*, *DE L'Isle*, and *Turner* courts each implicitly held that the third-party doctrine precludes an individual from claiming a reasonable expectation of privacy in the information encoded on the magnetic stripes of cards.[181] The courts concluded that because cards—and by operation, the encoded information—are regularly disclosed to third party merchants at the time of a purchase, the card holder is precluded from claiming a reasonable expectation of privacy in the encoded information.[182]

As a threshold matter, it is not clear in any of the cases if the seized cards had ever been used by the appellants and thus it is not clear if the encoded information had ever actually been voluntarily disclosed to a third party.[183] The courts nevertheless applied the third-party doctrine, reasoning that there is no reasonable expectation of privacy in the encoded information because the purpose of such cards necessarily requires that they be turned over to third party merchants in order to complete transactions.[184] The third-party doctrine cannot apply, however, when no disclosure to third parties has definitively been made.[185] That the cards were *intended* to be used and that their encoded infor-

---

92 (arguing that *Caballes* cannot apply to cases of scans of credit or debit cards); *see also Caballes*, 543 U.S. 410–13 (Souter, J., dissenting) (arguing that a police dog's sniff was a Fourth Amendment search because "[t]he infallible dog . . . is a creature of legal fiction[,]" and the government therefore could not guarantee that lawful activity would not be revealed from a sniff that resulted in a "false positive").

[180] Kerr, *supra* note 92 (arguing that "[t]he police can't know [what information will be revealed] until they [scan] the card, and that means *Caballes* can't apply"); *see* United States v. Jacobsen, 466 U.S. 109, 114, 114 n.9 (1984) (holding that a warrantless search is not made reasonable by discovering contraband, and citing to several cases holding the same); *DE L'Isle*, 825 F.3d at 435 (Kelly, J., dissenting) (arguing that "the results of a search cannot be used to justify its legality").

[181] *Turner*, 839 F.3d at 436; *DE L'Isle*, 825 F.3d at 432; *Bah*, 794 F.3d at 630–32. Although only the *Turner* court referred to the third-party doctrine by name, the *Bah* and *DE L'Isle* courts each cited to portions of district court opinions that discussed the third-party doctrine at length. *See Turner*, 839 F.3d at 436; *DE L'Isle*, 825 F.3d at 432; *Bah*, 794 F.3d at 630–31.

[182] *Turner*, 839 F.3d at 436; *DE L'Isle*, 825 F.3d at 432; *Bah*, 794 F.3d at 630–32.

[183] *Turner*, 839 F.3d at 431–34; *DE L'Isle*, 825 F.3d at 432; *Bah*, 794 F.3d at 621–26. The *Bah* court expressly noted the lack of direct evidence on this point. *Bah*, 794 F.3d at 630 n.9.

[184] *See Turner*, 839 F.3d at 436 (finding that "the raison d'être of gift cards means that third party cashiers will often be doing the same swiping that law enforcement did here"); *DE L'Isle*, 825 F.3d at 432 (quoting United States v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *10 (S.D. Fla. Oct. 24, 2009) (finding that "[w]hen the holder uses the card he 'knowingly disclose[s] the information on the magnetic strip of his credit card to a third party and cannot claim a reasonable expectation of privacy in it.'"); *Bah*, 794 F.3d at 632.

[185] S*ee* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding that "a person has no legitimate expectation of privacy in information he *voluntarily turns over* to third parties") (emphasis added); United States v. Miller, 425 U.S. 435, 443 (1976) (finding that "[t]he Fourth Amendment does not

mation was therefore *intended* to be disclosed to third parties is of no consequence.[186]

Even assuming that these cards were used, however, the third-party doctrine should not apply to the information encoded on the magnetic stripes of cards.[187] As with cell phones and other technological devices, the ubiquity of credit and debit card use today necessarily means that millions of Americans are regularly forced to use them in day-to-day life.[188] This necessity in turn requires individuals to hand over their card—and therefore the encoded account information—to third parties on a near daily basis.[189] At the same time

---

prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities"); Kerr, *supra* note 68, at 563 (noting that the third-party doctrine involves a disclosure of information to third parties); *see also* Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-Up*, 110 NW. U. L. REV. ONLINE 61, 75 (2015), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1231&context=nulr_online [https://perma.cc/4RPP-C58X] (arguing that the third-party doctrine does not apply in a hypothetical situation where no disclosure has been made by the individual claiming a reasonable expectation of privacy); Kerr, *supra* note 92 (arguing that "the fact that the [encoded] information . . . might in the future be disclosed [] does not eliminate Fourth Amendment protection").

[186] *See Smith*, 442 U.S at 743–44 (noting that information is "turn[ed] over" when the third-party doctrine applies); *Miller*, 425 U.S. at 443 (noting that information has been "revealed" to third parties when the third-party doctrine applies); Orin Kerr, Opinion, *Fifth Circuit Rules on Whether Scanning the Magnetic Stripe on a Card Is a Search*, WASH. POST (Oct. 16, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/16/fifth-circuit-rules-on-whether-scanning-magnetic-stripe-on-a-card-is-a-search/?utm_term=.985820e6f87a [https://perma.cc/CC86-6Y8E] (arguing that expectation of privacy is not waived unless disclosure occurs).

[187] *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (criticizing the third-party doctrine on the grounds that individuals regularly turn over information to third parties in day-to-day life); *Constitutional Law—State Action—Ninth Circuit Rejects Due Process Limit on Credit Card Fees*, 128 HARV. L. REV. 751, 757 (2014) (citing Late Fee & Over-Limit Fee Litig., 741 F.3d 1022, 1028 (9th Cir. 2014) (Reinhardt, J., concurring) (describing credit cards as a "practical necessit[y] of modern life"); Joseph W. Jerome, *Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, 52 (2013) https://www.stanfordlawreview.org/online/privacy-and-big-data-buying-and-selling-privacy/ [https://perma.cc/AG7X-FB34] (describing credit cards as a "necessity[y] of modern life").

[188] *See* State v. Tate, 849 N.W.2d 798, 827 (Wis. 2014) (finding that "[i]n the modern world . . . we regularly disclose information to third parties as part of everyday life"); Jamie Gonzales-Garcia, *Credit Card Ownership Statistics*, CREDITCARDS.COM (Oct. 25, 2016), https://www.creditcards.com/credit-card-news/ownership-statistics.php [https://perma.cc/Y2AD-K68L] (discussing 2015 statistics indicating that at least 70% of consumers own at least one credit card); *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (observing that cell phones are so commonplace in American society that they have become "essential" to modern life); *Constitutional Law—State Action—Ninth Circuit Rejects Due Process Limit on Credit Card Fees*, *supra* note 187, at 757 (citing *Late Fee & Over-Limit Fee Litig.*, 741 F.3d at 1028 (Reinhardt, J., concurring)) (describing credit cards as a "practical necessit[y] of modern life"); Jerome, *supra* note 187, at 52 (describing credit cards as a "necessit[y] of modern life"); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1736 (2006) (noting that individuals regularly disclose "a trove of information about [them]selves to third parties on a daily basis").

[189] *See* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 435 (2013) ("We now live in a world of ubiquitous third party information . . . . More and more people, and in more and more places, pay in an identified and

that these individuals are forced to disclose their card information to third party merchants in order to participate in today's economy, they are simultaneously advised by their banks, lending companies, and even the government, that the information contained on and within their cards is highly sensitive information that should be closely guarded.[190]

This paradox highlights the fact that the third-party doctrine, as it is currently applied, is "ill suited for the digital age."[191] Indeed, the type of information encoded on the magnetic stripe seems intuitively to be exactly the type of information that society would reasonably expect to remain private.[192] Societal expectations of privacy are drastically different than in 1979 when the U.S. Supreme Court decided *Smith v. Maryland* and, accordingly, courts should adapt their understanding.[193] Although until recently the third-party doctrine had not been directly before the Supreme Court in decades, there are indications that the Supreme Court may soon opt in favor of a more narrow applica-

---

recorded manner."); Gonzales-Garcia, *supra* note 188 (discussing 2015 statistics indicating that at least 70% of consumers own at least one credit card).

[190] *See, e.g.*, *Checking & Savings Account Security from Bank of America*, BANK OF AMERICA (2017), https://www.bankofamerica.com/privacy/accounts-cards/credit-debit-card-security.go [https://perma.cc/G8QZ-A7PB] (discussing security of debit and credit card account information and suggesting steps to maintain the privacy of the information); *Protecting Against Credit Card Fraud*, FED. TRADE COMM'N (July 2012), https://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud [https://perma.cc/AW7A-8WA7] (describing steps to take to ensure that credit and debit card account information remains protected).

[191] *See Jones*, 565 U.S. at 417–18 (2012) (Sotomayor, J., concurring). Citing the fact that modern technology has led to an increased need to disclose personal and private information to third parties in everyday life, Justice Sotomayor argued that she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *See id.* at 418.

[192] Byrd v. Aaron's Inc., 784 F.3d 154, 159 n.1 (3d Cir. 2015) (characterizing credit and debit card numbers as "personal information"); Slot Speaker Techs., Inc. v. Apple, Inc., No. 13-CV-01161-HSG(DMR), 2017 WL 386345, at *4 (N.D. Cal. Jan. 27, 2017) (ordering excerpts of a filed brief to be sealed because it disclosed "private information . . . such as credit card numbers"); Guarisma v. Microsoft Corp., No. 15-24326-CIV, 2016 WL 4017196, at *4 (S.D. Fla. July 26, 2016) (citing Creative Hosp. Ventures, Inc. v. U.S. Liab. Ins. Co, 655 F. Supp. 2d 1316, 1333 (S.D. Fla. 2009)) (characterizing credit card numbers as "private financial information"); Chapman v. Krutonog, No. CIV. 08-00579 HG-LEK, 2010 WL 727577, at *5 (D. Haw. Feb. 26, 2010) (recognizing the existence of "a privacy interest in financial information such as . . . credit card numbers"); State v. Mank, No. CAAP-16-0000342, 2017 WL 432898, at *3 (Haw. Ct. App. Mar. 13, 2017) (finding that "an individual also has a significant privacy interest in protecting against the unauthorized possession of his or her credit card number").

[193] *See, e.g.*, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 698 (2014) (describing that the courts are out of touch with "society's current expectations of privacy"); Henderson, *supra* note 189, at 453–54 (describing that, in response to the third-party doctrine, state legislatures passed laws in the "1960s, 1970s, and 1980s" to guard against warrantless searches of banking and telephone records because "reasonable persons did expect privacy"); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 333–36 (2008) (describing a study that found respondents believed that the government's access to data disclosed to third parties, such as "credit card records[,]" "email addresses sent to and received from[,]" and "bank records[,]" would be more intrusive than a "search of a car[,]" a "patdown[,]" or a "roadblock").

tion.[194] The economic and technological realties of the day should not work to frustrate an individual's Fourth Amendment protections.[195] Instead, as they have for other aspects of Fourth Amendment considerations, the courts should adapt the application of the third-party doctrine in light of today's technology.[196]

B. Riley*'s (Ir)Relevancy to Cards*

In holding that the minimal storage capability of the cards could not give rise to a reasonable expectation of privacy in their contents, the *Bah* and *Turner* courts distinguished the privacy interests at stake in cell phones from the privacy interests at stake in cards.[197] The *Bah* and *Turner* courts' consideration of the *Riley* holding, however, is misplaced.[198]

The threshold issue before the *Bah* and *Turner* courts was whether or not scanning the magnetic stripes of cards was, in fact, *a search* under the Fourth

---

[194] *See* Transcript of Oral Argument at 3, Carpenter v. United States, (No. 16-402) (addressing whether the act of obtaining a cell phone user's cell-site location data without a warrant violates the Fourth Amendment); *see also*, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (noting that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); Henderson, *supra* note 189, 438–42 (collecting Supreme Court cases that have addressed Fourth Amendment search determinations over the last twenty years and arguing that they indicate the Court's tendency to "sh[y] away from applying a strong third party doctrine"). Although the *Carpenter* case will address cell-site location data, the Court has an opportunity to re-work the application of the third-party doctrine in light of modern technological advances. Transcript of Oral Argument at 16, Carpenter v. United States, (No. 16-402). During the oral argument in *Carpenter*, Justice Alito acknowledged that "new technology is raising very serious privacy concerns" and noted that an issue in the case is "how much of existing [third-party doctrine] precedent [the petitioner] wants us to overrule or declare obsolete." *Id.* Moreover, the difficulty of applying the third-party doctrine in the modern-day was noted by Justice Breyer. *Id.* at 17–22 ("[T]he law is at the moment [that] third-party information [belongs to the] third-party, with a few exceptions, but it may be that here another exception should exist for the reason that the technology, since the time [the original third-party doctrine] cases [were decided] has changed dramatically . . . .").

[195] *See Kyllo*, 533 U.S. at 33–35 (adapting Fourth Amendment jurisprudence so as to not "leave the [suspect] at the mercy of advancing technology"); *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (arguing that an individual retains a reasonable expectation of privacy in bank records because their disclosure is not "volitional," but rather necessary to "participate in the economic life of contemporary society"); Katz v. United States, 389 U.S. 347, 358–59 (1967) (adapting Fourth Amendment jurisprudence to account for advancements in technology).

[196] *See Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring) (arguing for a reform of the third-party doctrine due to the prevalence with which individuals disclose personal information to third parties in today's world).

[197] *See Turner*, 839 F.3d at 435–36; *Bah*, 794 F.3d at 632–36; *see also supra* notes 140–150 and accompanying text (describing *Bah* and *Turner* courts' discussions of privacy interests arising in cards as compared to privacy interests arising in cell phones).

[198] *See* Arizona v. Hicks, 480 U.S. 321, 324–25 (1987); *see also* Kerr, *supra* note 186 (arguing that Fourth Amendment searches do not require that the search reveal substantial amounts of personal information); Kerr, *supra* note 92 (arguing that scans of cards should be considered Fourth Amendment searches based on the U.S. Supreme Court's holding in *Hicks*).

Amendment.[199] Conversely, it was conceded in *Riley* that the government had committed a Fourth Amendment search when it accessed the contents of the lawfully seized cell phone.[200] Instead, the dispositive question before the *Riley* Court was whether or not the *search was reasonable*.[201] Reasoning that the modern cell phone's substantial storage capability and tendency to contain sensitive personal information created a privacy interest that far outweighed the government's purported interest in searching the cell phone, the *Riley* Court held that the warrantless search was unreasonable.[202]

It appears, however, that the *Bah* and *Turner* courts applied *Riley*'s reasoning on the reasonability of the Fourth Amendment search at issue to their respective determinations on whether scanning a card is a Fourth Amendment search.[203] The courts concluded that the lack of storage capacity and personal information contained in a card precluded an individual from claiming a reasonable expectation of privacy in the encoded information.[204]

The *Bah* and *Turner* courts' conclusion that a card's lack of storage capacity and personal information militates against a finding that a Fourth Amendment search occurred is belied by previous court holdings.[205] Indeed, the U.S. Supreme Court has held that government action may constitute a Fourth Amendment search even if the object or item being searched does not store anything overly personal or private.[206] Instead, the Court has scrutinized the

---

[199] *See Turner*, 839 F.3d at 431; *Bah*, 794 F.3d at 621.

[200] *Turner*, 839 F.3d at 434 n.2 (finding that "[t]here was no dispute in *Riley* that reviewing the contents of a cell phone involved a search").

[201] *See id.* ("At issue was only whether such a search was permissible without a warrant when conducted during an arrest."). As discussed *supra*, when adjudicating a Fourth Amendment dispute, a court must first determine whether or not the government's conduct was a search within the meaning of the Fourth Amendment. *See* Lucier, *supra* note 23, at 1811 (noting that "[a]s a threshold question, courts must first determine whether a 'search' or 'seizure' occurred"). If the conduct is deemed to have been a Fourth Amendment search, the question then turns to whether or not the search was reasonable. *Id.*

[202] Riley v. California, 134 S. Ct. 2473, 2488–91 (2014).

[203] *See Turner*, 839 F.3d at 434–35; *Bah*, 794 F.3d at 632–33.

[204] *See Turner*, 839 F.3d at 434–35; *Bah*, 794 F.3d at 632–33.

[205] *See Hicks*, 480 U.S. at 324–25 (holding that moving a turntable to read its serial number was a search under the Fourth Amendment); Kerr, *supra* note 186 (arguing that Fourth Amendment searches do not require that the search reveal substantial amounts of personal information); *see also* Bond v. United States, 529 U.S. 334, 339 (2000) (holding that law enforcement committed a Fourth Amendment search when they felt the outside of a bag stowed on a public bus in "an exploratory manner[,]" even though such a search would not reveal overly personal information because the bag was never opened); United States v. Makeeff, 820 F.3d 995, 1002–03 (8th Cir. 2016) (holding a search of a USB drive to be a Fourth Amendment search); United States v. James, 353 F.3d 606, 613 (8th Cir. 2003) (holding a warrantless search of rewritable CDs to be a Fourth Amendment search and thus required to fit within an exception to the warrant requirement in order to be admissible).

[206] *See Hicks*, 480 U.S. at 324–25 (holding a search that revealed only a serial number to be a Fourth Amendment search); Kerr, *supra* note 186 (arguing that "the kind or amount of information obtained is irrelevant. The Fourth Amendment protects all 'effects' from searches, and there is no *de minimis* doctrine where breaking in just to get a few small things does not constitute a search").

government's means of attaining the underlying contents of an item.[207] As prominent Fourth Amendment scholar Orin Kerr has previously argued, one such example transpired in 1987, in *Arizona v. Hicks*, when the U.S. Supreme Court held that a Fourth Amendment search occurred when a law enforcement officer moved a turntable to record its serial number.[208] Although the turntable itself was in plain view, the serial number was not.[209] In holding that a Fourth Amendment search occurred, Justice Scalia, writing for the majority, held that "[i]t matters not that the search uncovered nothing of any great personal value to respondent . . . . A search is a search."[210]

Similarly, as Professor Kerr points out, neither the amount nor the nature of the information stored within the magnetic stripe of a card are dispositive of whether or not the appellants could claim a reasonable expectation of privacy.[211] The law enforcement officers in *Bah* and *Turner* "t[ook] action" that "exposed to view concealed portions" of the seized cards and thus "produce[d] a new invasion of [the appellants'] privacy."[212] Regardless of the likelihood that the scans would reveal the information to be identical to the information embossed on the card, the act of scanning the cards was "more than trivial for purposes of the Fourth Amendment," and the *Bah* and *Turner* courts should therefore have held that scanning the cards were Fourth Amendment searches.[213]

---

[207] *See, e.g.*, *Bond*, 529 U.S. at 339 (holding that feeling the outside of a bag was a Fourth Amendment search); *Hicks*, 480 U.S. at 324–325 (holding that slightly moving a turntable was a Fourth Amendment search).

[208] Kerr, *supra* note 92 (arguing that scans of cards should be considered Fourth Amendment searches based on the U.S. Supreme Court's holding in *Hicks*); *see Hicks*, 480 U.S. at 324–325.

[209] *Hicks*, 480 U.S. at 325.

[210] *Id.*

[211] *See id.* at 324–25; Kerr, *supra* note 186 (arguing that "the kind or amount of information obtained is irrelevant"); *see also DE L'Isle*, 825 F.3d at 436 (Kelly, J., dissenting) (noting that courts have held that the search of certain containers, such as cereal boxes or guitar bags, are Fourth Amendment searches irrespective of the fact that such searches were unlikely to reveal anything of great value); United States v. Haqq, 278 F.3d 44, 50 (2d Cir. 2002) (finding that "because the Supreme Court in *Hicks* held that the search of the stereo equipment was unlawful, it necessarily also found . . . that the defendant had a legitimate expectation of privacy in that equipment").

[212] *See Hicks*, 480 U.S. at 325 (finding that "taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of respondent's privacy unjustified by the exigent circumstance that validated the entry").

[213] *See id.* (concluding that although looking at the turntable did not require a warrant, moving the turn table was "much more than trivial for the purposes of the Fourth Amendment"); Kerr, *supra* note 92 (arguing that scans of cards should be considered Fourth Amendment searches).

Conclusion

Scanning the magnetic stripes of cards to access the information encoded therein should be considered a search within the meaning of the Fourth Amendment. The U.S. Courts of Appeals' collective refusal to recognize this sets an arbitrary precedent that encourages future courts to scrutinize merely the amount and nature of information being searched. Such a prioritization contravenes the purpose of the Fourth Amendment, as the Founders sought to protect individuals from the methods by which the government searched, regardless of what it was that they were searching for. In an era of continual technological advancement, such an arbitrary focus will undoubtedly threaten legitimate expectations of privacy. This includes the expectation of privacy in the encoded information of cards. The government should therefore be required to act reasonably when scanning the magnetic stripes of cards. After all, "[a] search is a search," regardless of what it may reveal.

John A. LeBlanc