United States Court of Appeals
For the Eighth Circuit

No. 15-1316

United States of America

Plaintiff - Appellee

v.

Eric-Arnaud Benjamin Briere DE L'Isle

Defendant - Appellant

Appeal from United States District Court
for the District of Nebraska - Lincoln

Submitted: November 20, 2015
Filed: June 8, 2016

Before RILEY, Chief Judge, BEAM and KELLY, Circuit Judges.

BEAM, Circuit Judge.

Eric-Arnaud Benjamin Briere DE L'Isle appeals the district court's[1] denial of his motion to suppress information discovered by law enforcement after officers seized credit, debit, and gift cards from DE L'Isle's vehicle and scanned the cards'

[1]The Honorable John M. Gerrard, United States District Judge for the District of Nebraska.

magnetic strips. Despite DE L'Isle's untimely motion to suppress, the district court examined the merits of the motion and concluded that reading the magnetic strip on the back of a credit, debit, or gift card was not a search within the meaning of the Fourth Amendment. For the reasons discussed below, we affirm.

I. BACKGROUND

On June 20, 2014, Sergeant Michael Vance stopped DE L'Isle for following too closely to a semi-tractor trailer. When the officer approached DE L'Isle's car, he smelled burnt marijuana and saw air fresheners inside the car. DE L'Isle accompanied Sergeant Vance to his police cruiser where DE L'Isle was given a warning citation for following too closely. Sergeant Vance then deployed his canine, which alerted to the presence of controlled substances inside the vehicle. When Sergeant Vance began searching the vehicle, DE L'Isle approached him and told him he could not search the vehicle. After a brief struggle between DE L'Isle and Sergeant Vance, DE L'Isle was handcuffed and placed into the backseat of the police cruiser.

Sergeant Vance and two other officers completed the search. No narcotics were found, but they seized a large stack of credit, debit, and gift cards located in a duffle bag in the trunk of DE L'Isle's car. DE L'Isle was subsequently arrested for assault and resisting arrest. United States Secret Service agents then scanned the seized cards and discovered that the magnetic strips on the back of the cards either contained no account information or contained stolen American Express credit card information. Ten of the cards were American Express credit cards with DE L'Isle's name on the front. The magnetic strips on the back of these ten cards, however, were "empty"; there was no information at all in the magnetic strips. At least one card, card 23, was a Parker's PumpPal Club gas debit card, and card 25 was a Quik Trip prepaid card. The magnetic strips on the back of these cards had account information linked to legitimate American Express credit card accounts. Cards 31 through 47 were American Express gift cards. The magnetic strips on these cards contained credit card

information from legitimate American Express customers. Cards 48 through 58 were Visa debit cards, Visa gift cards, and a Mastercard. The account information encoded on the magnetic strips of these cards also corresponded to American Express credit accounts. Card 59 was a Subway gift card with American Express credit card information encoded in the magnetic strip. However, none of the American Express account information on any of the cards was DE L'Isle's. In fact, he had no existing accounts with American Express.

As a result, DE L'Isle was charged with possession of fifteen or more counterfeit and unauthorized access devices, in violation of 18 U.S.C. §§ 1029(a)(3) and (c)(1)(A)(i). He pled not guilty, and on July 31, 2014, the magistrate judge filed a progression order requiring that pretrial motions be filed on or before August 29, 2014. On October 23, 2014, De L'Isle filed a motion to suppress asking the district court to suppress any evidence discovered when law enforcement scanned the magnetic strips on the seized cards. He argued that the search of the information in the magnetic strips of the cards was done without a warrant or a warrant exception and thus violated his Fourth Amendment right to be free from unreasonable searches. The district court noted that his motion was untimely. However, the court considered the merits of the motion and held that "based on the law," DE L'Isle's motion lacked merit.[2] Thus, the district court denied the motion to suppress without a hearing, ultimately holding that "reading the magnetic strip on the back of a credit, debit, or gift card is not a 'search' for Fourth Amendment purposes."

[2]Pursuant to Federal Rule of Criminal Procedure 12(c)(1), the magistrate judge issued a progression order requiring all pretrial motions be filed on or before August 29, 2014. DE L'Isle did not file his motion to suppress until October 23, 2014. Thus, the district court would not have abused its discretion if it had denied the motion solely on the basis of untimeliness. United States v. Salgado-Campos, 442 F.3d 684, 686 (8th Cir. 2006) ("If a party fails to file a pretrial motion before that deadline, the party waives that issue.").

At trial, United States Secret Service Agent Nicholas Wadding testified about credit card theft and identity theft. He explained that nearly all plastic cards have three tracks, or lines, of information on the magnetic strip. The first line has the account number, the second line has the credit card holder's name, and the third line, which is discretionary, may have a frequent flier number or some specific identifier.[3] According to Peter Grimm, an American Express fraud investigator, the magnetic strip also generally contains the card's expiration date. The information contained in the magnetic strip should match the information on the front of the card. A card is said to be "re-encoded" when the magnetic strip information is rewritten.

The ten American Express cards confiscated from De L'Isle's vehicle all had his name on the front of the cards with different account numbers, but the cards had no information on the magnetic strips. Grimm testified that it is significant that a card has a blank magnetic strip because that means it is counterfeit. All American Express cards are issued with account information contained in the magnetic strip. It is also significant that the magnetic strips on the Parker's PumpPal Club gas debit card, Quik Trip prepaid card, American Express gift cards, Visa debit and gift cards, Mastercard debit card, and Subway gift card all contained legitimate American Express customer account information. American Express would never encode credit card holder information on the back of these types of cards. If a gift card has been re-encoded with account information that was not originally there, it is a counterfeit card. DE L'Isle testified that he bought the cards from an unknown person and believed they were legitimate. On October 29, 2014, the jury returned a guilty verdict, and DE L'Isle was sentenced to fifteen months in prison and three years of supervised release. He was also ordered to pay over $4,700 in restitution and over $12,700 in court costs.

[3]Here, none of the cards in question had any information in the third discretionary line of the magnetic strip.

DE L'Isle now appeals the district court's denial of his motion to suppress. He does not challenge the traffic stop or the seizure of the cards. DE L'Isle disputes only the district court's narrow holding that he had no Fourth Amendment privacy interest in the information contained in the magnetic strips on the credit, debit, and gift cards seized from his vehicle.

II. DISCUSSION

When reviewing a district court's denial of a motion to suppress, "this [c]ourt reviews factual findings for clear error, and questions of constitutional law *de novo*." United States v. Smith, 715 F.3d 1110, 1114 (8th Cir. 2013) (quoting United States v. Hollins, 685 F.3d 703, 705 (8th Cir. 2012)). In regard to factual determinations, this court "give[s] 'due weight' to the inferences of the district court and law enforcement officials." United States v. Robbins, 682 F.3d 1111, 1115 (8th Cir. 2012) (quoting United States v. Replogle, 301 F.3d 937, 938 (8th Cir. 2002)). Also, "[w]e may affirm the district court's denial of a motion to suppress on any ground the record supports." United States v. Anderson, 688 F.3d 339, 343 (8th Cir. 2012) (quoting United States v. Pratt, 355 F.3d 1119, 1121 (8th Cir. 2004)).

DE L'Isle argues that reading the magnetic strips on the back of the cards was a search in violation of his Fourth Amendment rights because the strip contains information about the account. According to DE L'Isle, this is the type of information that the Supreme Court would consider a legitimate privacy interest. Given the facts of this case, we disagree.

The Fourth Amendment gives people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)), cert. denied, Riley v. California, 136 S. Ct. 506 (2015). A

search is reasonable if the officer has a valid search warrant or if the search fits within a specific warrant exception. Id. It is clear that a physical intrusion or trespass by a government official constitutes a search within the meaning of the Fourth Amendment. United States v. Jones, 132 S. Ct. 945, 949 (2012). However, "a violation [can also] occur[] when government officers violate a person's 'reasonable expectation of privacy.'" Id. at 950 (quoting Katz v. United States, 389 U.S. 347, 360 (1967)). For this type of violation, the claimant must show both "an actual (subjective) expectation of privacy, and . . . that the expectation [is] one that society is prepared to recognize as 'reasonable.'" Katz, 389 U.S. at 361. Thus, "[o]fficial conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." Illinois v. Caballes, 543 U.S. 405, 408 (2005) (quoting United States v. Jacobsen, 466 U.S. 109, 123 (1984)).

First, scanning the magnetic strips on the cards was not a physical intrusion into a protected area prohibited by the Fourth Amendment. See Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013). The magnetic strip on the back of a debit or credit card is a type of "external electronic storage device, [that] is designed simply to record the same information that is embossed on the front of the card." United States v. Medina, No. 09-20717-CR, 2009 WL 3669636, at *10 (S.D. Fla. 2009). Accordingly, the information embossed on the front of the card and recorded in the magnetic strip will only be different if the card has been tampered with. Id. Credit card readers reveal whether the information in the magnetic strip on the back of the card matches the information on the front. Id. The process of using a credit card reader "is analogous to using an ultraviolet light to detect whether a treasury bill is authentic, . . . [which is not a] . . . 'search.'" Id. Thus, because "sliding a card through a scanner to read virtual data does not involve physically invading a person's" space or property, there was no Fourth Amendment violation under the original trespass theory of the Fourth Amendment. United States v. Alabi, 943 F. Supp. 2d 1201, 1265 (D.N.M. 2013).

Second, DE L'Isle failed to show that he had a reasonable expectation of privacy under Katz, which requires a showing of both a subjective expectation of privacy and an objective expectation of privacy that society recognizes as reasonable. Katz, 389 U.S. at 361. Although DE L'Isle claims he had an actual, subjective privacy interest in the cards, he is unable to make that case.[4] As to the ten American Express credit cards, he could not have had an expectation of privacy simply because his name was embossed on the front of the cards. He also could not have had a subjective expectation of privacy in any of the other cards because the purpose of a credit, debit, or gift card is to enable the holder of the card to make purchases, and to accomplish this, the holder must transfer information from the card to the seller, which negates an expressed privacy interest. Medina, 2009 WL 3669636, at *11. Information is transferred to the seller "by manually inputting the information on the front of the card or swiping the card through a machine that reads the magnetic strip on the back." Id. 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." Id.

---

[4]The dissent in its footnote 7, citing a very small portion of the district court's footnote 2, apparently seeks to formulate a case-wide factual dispute sufficient to convert this appeal into a quest for an advisory opinion dealing with a laundry list of issues barely, if at all, in dispute. The operative language leading into the district court's footnote is as follows: "[E]ven assuming that the defendant could show a subjective expectation of privacy in the magnetically-encoded information on the cards–that expectation is not one that society is prepared to accept as legitimate." While the validity, or not, of a defendant's subjective expectation of privacy may be a question of fact, whether such expectation is one that society is prepared to reasonably accept as legitimate is a question of law. United States v. Douglas, 744 F.3d 1065, 1069 (8th Cir. 2014).

The district court unequivocally said it was not a reasonable, legitimate expectancy. Accordingly, no question of fact survives in support of the dissent's quest for an advisory opinion on the numerous listed issues.

Even if DE L'Isle had an actual, subjective expectation of privacy in the information found in the magnetic strips on the cards, this alleged privacy interest is not one society is prepared to endorse. In the normal course, all of the information found in the magnetic strips on American Express credit cards is identical to the information in plain view on the front of the cards. "Society is not prepared to recognize as legitimate an asserted privacy interest in information in plain view that any member of the public may see." Alabi, 943 F. Supp. 2d at 1276. Even less convincing is the situation in this case where the magnetic strips on the American Express credit cards were empty. If society does not recognize a privacy interest in readily visible information, DE L'Isle certainly cannot assert a privacy interest in information that is nonexistent.

When the information contained in the magnetic strip differs from the information on the front of the card, there is another possible issue that diminishes DE L'Isle's purported privacy interest. According to Agent Wadding, the only reason a person re-encodes the magnetic strip on the back of a card is to "mask that they have a card number." Society is even less likely to recognize as reasonable DE L'Isle's "subjective expectation of privacy in the information stored on [the] credit and debit cards' magnetic strips [when] the evidence shows [that it] would only be different from the information embossed on the outside of the card if the intent is to engage in a crime." Id. at 1287. American Express credit cards with no information in the magnetic strips, and debit and gift cards that have been re-encoded with new information in the magnetic strips, are counterfeit cards. The evidence strongly suggests that DE L'Isle intended to engage in credit card fraud and identity theft. "[G]overnmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'" Caballes, 543 U.S. at 408 (quoting Jacobsen, 466 U.S. at 123). Thus, because scanning the magnetic strips 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.

There may be an instance, with facts different from this case, where a court reasonably finds a legitimate privacy interest in information contained in the magnetic strip of a credit, debit, or gift card. In such a case, a motion to suppress may well be proper to further explicate the nature and character of privacy interests, if any, that may reside within the confines of these magnetic strips. However, here, where all of the information in the magnetic strip should have been identical to the information in plain view on the front of the card, and where the cards were lawfully possessed by law enforcement officers and established to be counterfeit, we cannot conclude that DE L'Isle had a privacy interest warranting further investigation into potential Fourth Amendment protections.

III. CONCLUSION

The judgment of the district court is affirmed.

KELLY, Circuit Judge, dissenting.

This appeal presents a narrow legal issue: Does scanning the magnetic stripe on the back of a credit or debit card to access the data stored on it implicate the protections of the Fourth Amendment? In my view, answering this question requires further factual development, and I would remand the case to the district court to hold an evidentiary hearing.[5]

[5]I recognize the difficult position in which the district court found itself, faced with a motion to suppress almost on the eve of trial. The district court would have been within its rights to deny the motion as untimely. In a commendable effort to grant the defendant a full opportunity to present his defense, the district court instead excused the delinquency of the motion and decided it on the merits. Although I recognize that the district court's decision not to hold an evidentiary hearing is reviewed deferentially, United States v. Hill, 750 F.3d 982, 986 (8th Cir. 2014), I believe an evidentiary hearing is necessary to resolve this case.

A Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. Kyllo v. United States, 533 U.S. 27, 31–33 (2001). The district court, while expressing some skepticism on whether Briere[6] had a subjective expectation of privacy in the contents of the cards, said that it would "give the defendant the benefit of the (minimal) doubt." United States v. Briere de L'Isle, No. 4:14-CR-3089, 2014 WL 5431349, at *3 n.2 (D. Neb. Oct. 24, 2014).[7] The sole remaining question, then, is whether an expectation of privacy in the contents of the magnetic stripes on one's credit and debit cards is reasonable.

In my view, the answer to this question depends on whether there are significant technological barriers to an individual rewriting information on the magnetic stripe of their cards, and I would remand the case to the district court to develop evidence on this point. If the information on the magnetic stripe can be modified without much difficulty, the cardholder may indeed have a reasonable expectation of privacy in the contents of the stripe, based on the straightforward principle that law enforcement conducts a Fourth Amendment "search" when it reads the contents of rewritable

[6]I abbreviate Eric-Arnaud Benjamin Briere de L'Isle's name as Briere, the short form that he used on a number of the cards, and that the government used in its brief and the affidavit attached to the criminal complaint.

[7]The court holds, on the contrary, that Briere did not have a subjective expectation of privacy in the contents of the magnetic stripes. But "whether [Briere] had a subjective expectation of privacy is a question of fact, which this court reviews for clear error." United States v. Long, 797 F.3d 558, 564–65 (8th Cir. 2015) (quotation marks omitted). To the extent the district court's statement, quoted above, represents a factual finding that Briere had a subjective expectation of privacy in the contents of the magnetic stripe, it was not clearly erroneous; to the extent the district court made no finding on this point, there is no clear record to justify appellate factfinding in the first instance. What the court calls "the purpose of a credit, debit, or gift card" (presumably meaning the purpose the issuing institution intended for the card), ante at 7, does not bear on Briere's own subjective beliefs about the card.

digital storage media. See United States v. James, 353 F.3d 606, 613 (8th Cir. 2003) (holding that accessing CDs given by defendant to a friend violated Fourth Amendment). That principle is implicit in the fact that both this court and the Supreme Court have consistently required searches of storage devices like hard drives and CDs to be justified either by a warrant or an applicable exception to the warrant requirement. See, e.g., Riley v. California, 134 S. Ct. 2473, 2482 (2014) (search incident to lawful arrest); United States v. Makeeff, — F.3d —, 2016 WL 1720234, at *6 (8th Cir. Apr. 29, 2016) (per curiam) (probationary search); United States v. Beckmann, 786 F.3d 672, 677–78 (8th Cir. 2015) (consent); United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008) (warrant). The principle is also suggested by the Supreme Court's judgment in Walter v. United States, 447 U.S. 649 (1980), that federal agents violated the Fourth Amendment by viewing reels of defendants' 8-millimeter films without a warrant, despite the fact that the agents had come into possession of the films lawfully. If a magnetic stripe card is a digital storage device, albeit one whose storage capacity is limited, see United States v. Bah, 794 F.3d 617, 633 (6th Cir. 2015) (noting that according to defendant magnetic stripes could hold 79 alphanumeric characters and 147 numbers), reading the data on it is a Fourth Amendment search. Accessing the data on the stripe would simply be a special case of the general rule that reading a digital storage device constitutes a Fourth Amendment search.

In coming to the opposite conclusion, the court relies in large part on the fact that "[i]n the normal course" the information on the magnetic stripe is identical to the information embossed on the front of the card and there can be no reasonable expectation of privacy in information that is in plain view. Ante at 8. It also points out that the magnetic stripes on the cards seized from Briere contained only zeroes or stolen credit card information, and concludes that Briere could not have had an expectation of privacy in nonexistent or fraudulent information.

The problem with this approach is 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. And the results of a search cannot be used to justify its legality. See United States v. Jacobsen, 466 U.S. 109, 114 & n.9 (1984) (collecting cases); United States v. Di Re, 332 U.S. 581, 595 (1948) ("We have had frequent occasion to point out that a search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success."). If a search could be justified by what it yields, the exclusionary rule would have no effect:

> Obviously the word "legitimate" in the phrase "legitimate expectation of privacy" is being used in a special sense. . . . The cases must be analyzed on the hypothesis that no illegal activity is occurring or contemplated. The illegality comes to light only through [the search] whose validity is the very point at issue. Otherwise Fourth Amendment analysis would be pointless, because motions to suppress are never made in the first place unless evidence of criminality has been seized.

United States v. Little, 735 F.2d 1049, 1052 (8th Cir.) (R. Arnold, J.), modified on reh'g on other grounds sub nom. United States v. Sager, 743 F.2d 1261 (8th Cir. 1984). If a law enforcement officer opened a briefcase to find it empty or full of contraband, that officer conducted a Fourth Amendment search no less than if the briefcase contained legitimate papers. See United States v. Ross, 456 U.S. 798, 822–23 (1982) ("[T]he Fourth Amendment provides protection to the owner of every container that conceals its contents from plain view."); United States v. Knight, 306 F.3d 534, 536 (8th Cir. 2002).

If information on the magnetic stripe can be modified by the cardholder, it is obviously possible (though perhaps not common) to rewrite that information in a lawful manner. It would not be illegal, for example, for a cardholder to rewrite the

data on the magnetic stripe of a card she had no more use for to "MYBANKACCOUNTPASSWORDIS78911Y783," so that she could recover her password in the event she forgot it. This fact distinguishes the present case from Illinois v. Caballes, which held that canine drug-detection sniffs are not Fourth Amendment searches, because they reveal either nothing at all or the presence of illegal drugs. 543 U.S. 405, 409 (2005) (explaining that "a canine sniff by a well-trained narcotics-detection dog [is] '*sui generis*' because it 'discloses only the presence or absence of narcotics, a contraband item.'" (quoting United States v. Place, 462 U.S. 696, 707 (1983))). If there is no technological barrier to either the card issuer or the card holder placing arbitrary and potentially private (and innocent) data on the card, the same dichotomy does not apply to magnetic stripes.

It may well be the case that few people rewrite the information on the magnetic stripes of their cards for innocent purposes, though no evidence was developed on this point at the district court.[8] But that does not change the result under the Fourth Amendment. This court has held that individuals have a reasonable expectation of privacy even in so-called single-purpose containers, "those rare containers" whose "distinctive configuration . . . proclaims [their] content." United States v. Banks, 514 F.3d 769, 774 (8th Cir. 2008) (second alteration in original) (quoting Texas v. Brown, 460 U.S. 730, 750–51 (1983) (Stevens, J., concurring in the judgment), and Robbins v. California, 453 U.S. 420, 427 (1981), overruled on other grounds by United States v. Ross, 456 U.S. 798 (1982)). The examples of single-purpose containers given in Banks – cereal boxes, guitar bags, gun cases, and the like – make it clear that the

[8]The court cites trial testimony from United States Secret Service Agent Nicholas Wadding, ante at 8, but Wadding was explaining why someone would re-encode the magnetic stripe on a gift card with an unrelated credit card number, not how common it is to re-encode magnetic stripes for lawful purposes. It is unclear how the latter question could be answered solely on the basis of law enforcement experience of the sort Wadding possessed; it would likely require a survey or similar investigation.

category includes containers that could (but usually do not) contain items other than what might be inferred from the container itself. See 514 F.3d at 774; United States v. Meada, 408 F.3d 14, 24 (1st Cir. 2005); see also United States v. Soto, 988 F.2d 1548, 1553–54 (10th Cir. 1993) (holding defendant had reasonable expectation of privacy in secret compartment of car even though "secret compartments are most often used to conceal narcotics, weapons, or large amounts of cash"). Just as there is a reasonable expectation of privacy in the contents of cereal boxes, despite the fact that most people store nothing more than cereal in them, the Fourth Amendment applies to the contents of magnetic stripes, despite the likelihood that most people don't change or modify in any way the account information stored there by default.[9]

Although the stakes may appear small at this stage, technological progress has a way of ensuring that they do not remain so. The Supreme Court has instructed that "the rule we adopt must take account of more sophisticated systems that are already in use or in development." Kyllo, 533 U.S. at 36. What advances are likely to be made in this area is a topic that deserves further factual development by the district court, especially because the available evidence suggests that the amount of information storable on a credit card will not long be numbered in the dozens of characters. Already many newly-issued credit cards in the United States contain chips that have a storage capacity much greater than that of the old magnetic stripes. See Rachel Abrams, Chip Cards Will Require Users to Dip Rather Than Swipe, N.Y. Times (Sept. 28, 2015), http://nyti.ms/1Vn2wdm; EMVCo, About EMV, https://www.emvco.com/about_emv.aspx [https://perma.cc/4VL6-TF4T] (last visited

[9]It is true that the expectation of privacy in single-purpose containers is a diminished one that permits warrantless searches upon a showing of probable cause to seize the container. Banks, 514 F.3d at 774. This "single-purpose container exception" to the warrant requirement, however, does not apply here because to the extent probable cause existed to seize the cards found in Briere's trunk, it was probable cause to believe that the magnetic stripes did *not* contain what the "container" implied, namely, the account information embossed on the front of the card.

May 31, 2016) (website of creator of chip card standard noting they store "considerably more information than magnetic stripe cards"). As cards are able to store more information, the privacy interests they implicate increase. If higher-capacity cards are in our future, with the ability for the cardholder to modify what they store for their own private use, any line we could attempt to draw between the cards at issue in this case and those of the future would necessarily be arbitrary.

Because I think that resolution of Briere's motion requires more factual development, I would remand this case to the district court for that purpose. For this reason, I respectfully dissent.
